
Stream:	Internet Engineering Task Force (IETF)		
RFC:	9788		
Updates:	8551		
Category:	Standards Track		
Published:	May 2025		
ISSN:	2070-1721		
Authors:	D. K. Gillmor <i>American Civil Liberties Union</i>	B. Hoeneisen <i>pEp Project</i>	A. Melnikov <i>Isode Ltd</i>

RFC 9788

Header Protection for Cryptographically Protected Email

Abstract

S/MIME version 3.1 introduced a mechanism to provide end-to-end cryptographic protection of email message headers. However, few implementations generate messages using this mechanism, and several legacy implementations have revealed rendering or security issues when handling such a message.

This document updates the S/MIME specification (RFC 8551) to offer a different mechanism that provides the same cryptographic protections but with fewer downsides when handled by legacy clients. Furthermore, it offers more explicit usability, privacy, and security guidance for clients when generating or handling email messages with cryptographic protection of message headers.

The Header Protection scheme defined here is also applicable to messages with PGP/MIME (Pretty Good Privacy with MIME) cryptographic protections.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <https://www.rfc-editor.org/info/rfc9788>.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	8
1.1. Update to RFC 8551	8
1.1.1. Problems with RFC 8551 Header Protection	8
1.2. Risks of Header Protection for Legacy MUA Recipients	9
1.3. Motivation	10
1.3.1. Backward Compatibility	10
1.3.2. Deliverability	11
1.4. Other Protocols to Protect Email Header Fields	11
1.5. Applicability to PGP/MIME	12
1.6. Requirements Language	12
1.7. Terms	12
1.8. Document Scope	13
1.8.1. In Scope	14
1.8.2. Out of Scope	14
1.9. Example	14
2. Internet Message Format Extensions	16
2.1. Content-Type Parameters	16
2.1.1. Content-Type Parameter: hp	17
2.1.2. Content-Type Parameter: hp-legacy-display	17

2.2. HP-Outer Header Field	18
2.2.1. HP-Outer Header Field Definition	19
3. Header Confidentiality Policy	19
3.1. HCP Definition	20
3.1.1. HCP Avoids Changing addr-spec of From Header Field	21
3.2. Initial Registered HCPs	21
3.2.1. Baseline Header Confidentiality Policy	21
3.2.2. Shy Header Confidentiality Policy	22
3.2.3. No Header Confidentiality Policy	22
3.3. Default Header Confidentiality Policy	22
3.4. HCP Evolution	23
3.4.1. Offering More Ambitious Header Confidentiality	23
3.4.2. Expert Guidance for Registering Header Confidentiality Policies	23
4. Receiving Guidance	24
4.1. Identifying That a Message Has Header Protection	25
4.2. Extracting Protected and Unprotected ("Outer") Header Fields	25
4.2.1. HeaderSetsFromMessage	25
4.3. Updating the Cryptographic Summary	26
4.3.1. HeaderFieldProtection	26
4.4. Handling Mismatch of From Header Fields	27
4.4.1. Definitions	27
4.4.2. Warning for From Header Field Mismatch	28
4.4.3. From Header Field Rendering	28
4.4.4. Handling the Protected From Header Field When Responding	29
4.4.5. Matching addr-specs	29
4.5. Rendering a Message with Header Protection	29
4.5.1. Example Signed-Only Message	29
4.5.2. Example Signed-and-Encrypted Message	30
4.5.3. Do Not Render Legacy Display Elements	31

4.6. Implicitly Rendered Header Fields	32
4.7. Handling Undecryptable Messages	32
4.8. Guidance for Automated Message Handling	33
4.8.1. Only Interpret Protected Header Fields	33
4.8.2. Ignore Legacy Display Elements	34
4.9. Affordances for Debugging and Troubleshooting	34
4.10. Handling RFC8551HP Messages (Backward Compatibility)	35
4.10.1. Identifying an RFC8551HP Message	35
4.10.2. Rendering or Responding to an RFC8551HP Message	36
4.11. Rendering Other Schemes	36
5. Sending Guidance	36
5.1. Composing a Cryptographically Protected Message Without Header Protection	37
5.1.1. ComposeNoHeaderProtection	37
5.2. Composing a Message with Header Protection	37
5.2.1. Compose	38
5.2.2. Adding a Legacy Display Element to a text/plain Part	40
5.2.3. Adding a Legacy Display Element to a text/html Part	40
5.2.4. Only Add a Legacy Display Element to Main Body Parts	42
5.2.5. Do Not Add a Legacy Display Element to Other Content-Types	42
6. Replying and Forwarding Guidance	42
6.1. Avoid Leaking Encrypted Header Fields in Replies and Forwards	42
6.1.1. ReferenceHCP	43
6.2. Avoid Misdirected Replies	45
7. Unprotected Header Fields Added in Transit	45
7.1. Mailing List Header Fields: List-* and Archived-At	46
8. Email Ecosystem Evolution	46
8.1. Dropping Legacy Display Elements	46
8.2. More Ambitious Default Header Confidentiality Policy	47
8.3. Deprecation of Messages Without Header Protection	48

9. Usability Considerations	48
9.1. Mixed Protections Within a Message Are Hard to Understand	48
9.2. Users Should Not Have to Choose a Header Confidentiality Policy	49
10. Security Considerations	49
10.1. From Address Spoofing	50
10.1.1. From Rendering Reasoning	51
10.2. Avoid Cryptographic Summary Confusion from the hp Parameter	52
10.3. Caution About Composing with Legacy Display Elements	53
10.4. Plaintext Attacks	54
11. Privacy Considerations	54
11.1. Leaks When Replying	54
11.2. Encrypted Header Fields Are Not Always Private	54
11.2.1. Encrypted Header Fields Can Leak Unwanted Information to the Recipient	55
11.2.2. Encrypted Header Fields Can Be Inferred from External or Internal Metadata	55
11.2.3. Encrypted Header Fields May Not Be Fully Masked by HCP	55
11.3. A Naive Recipient May Overestimate the Cryptographic Status of a Header Field in an Encrypted Message	56
11.4. Privacy and Deliverability Risks with Bcc and Encrypted Messages	56
12. IANA Considerations	57
12.1. Registration of the HP-Outer Header Field	57
12.2. Reference Update for the Content-Type Header Field	57
12.3. New Mail Header Confidentiality Policies Registry	58
13. References	59
13.1. Normative References	59
13.2. Informative References	60
Appendix A. Table of Pseudocode Listings	62
Appendix B. Possible Problems with Legacy MUAs	62
B.1. Problems Viewing Messages in a List View	63
B.2. Problems When Rendering a Message	63
B.3. Problems When Replying to a Message	63

Appendix C. Test Vectors	64
C.1. Baseline Messages	64
C.1.1. No Cryptographic Protections over a Simple Message	64
C.1.2. S/MIME Signed-Only signedData over a Simple Message, No Header Protection	65
C.1.3. S/MIME Signed-Only multipart/signed over a Simple Message, No Header Protection	67
C.1.4. S/MIME Signed and Encrypted over a Simple Message, No Header Protection	69
C.1.5. No Cryptographic Protections over a Complex Message	73
C.1.6. S/MIME Signed-Only signedData over a Complex Message, No Header Protection	74
C.1.7. S/MIME Signed-Only multipart/signed over a Complex Message, No Header Protection	77
C.1.8. S/MIME Signed and Encrypted over a Complex Message, No Header Protection	80
C.2. Signed-Only Messages	85
C.2.1. S/MIME Signed-Only signedData over a Simple Message, Header Protection	85
C.2.2. S/MIME Signed-Only multipart/signed over a Simple Message, Header Protection	87
C.2.3. S/MIME Signed-Only signedData over a Complex Message, Header Protection	89
C.2.4. S/MIME Signed-Only multipart/signed over a Complex Message, Header Protection	93
C.2.5. S/MIME Signed-Only signedData over a Complex Message, Legacy RFC 8551 Header Protection	95
C.2.6. S/MIME Signed-Only multipart/signed over a Complex Message, Legacy RFC 8551 Header Protection	99
C.3. Signed-and-Encrypted Messages	101
C.3.1. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_baseline	101
C.3.2. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)	106
C.3.3. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy	111
C.3.4. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)	116
C.3.5. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline	121
C.3.6. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)	126

C.3.7. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy	132
C.3.8. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)	137
C.3.9. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline	142
C.3.10. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)	149
C.3.11. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy	156
C.3.12. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)	162
C.3.13. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline	170
C.3.14. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)	177
C.3.15. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy	184
C.3.16. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)	191
C.3.17. S/MIME Signed and Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline	199
Appendix D. Composition Examples	205
D.1. New Message Composition	205
D.1.1. Unprotected Message	206
D.1.2. Encrypted with hcp_baseline and Legacy Display	207
D.2. Composing a Reply	208
D.2.1. Unprotected Message	210
D.2.2. Encrypted with hcp_no_confidentiality and Legacy Display	211
Appendix E. Rendering Examples	214
E.1. Example text/plain Cryptographic Payload with Legacy Display Elements	214
E.2. Example text/html Cryptographic Payload with Legacy Display Elements	215
Appendix F. Other Header Protection Schemes	216
F.1. Original RFC 8551 Header Protection	216

F.2. Pretty Easy Privacy (pEp)	216
F.3. Autocrypt Protected Headers	217
Acknowledgements	217
Index	218
Authors' Addresses	219

1. Introduction

Privacy and security issues regarding email Header Protection in S/MIME and PGP/MIME have been identified for some time. Most current implementations of cryptographically protected email protect only the Body of the message, which leaves significant room for attacks against otherwise-protected messages. For example, lack of Header Protection allows an attacker to substitute the message subject and/or author.

This document describes how to cryptographically protect message headers and provides guidance for the implementer of a Mail User Agent (MUA) that generates, interprets, and replies to such a message. It uses the term "Legacy MUA" to refer to an MUA that does not implement this specification. This document takes particular care to ensure that messages interact reasonably well with Legacy MUAs.

1.1. Update to RFC 8551

An older scheme for Header Protection was specified in S/MIME 3.1 [RFC8551], which involves wrapping a `message/rfc822` MIME object with a Cryptographic Envelope around the message to protect it. This document refers to that scheme as "RFC 8551 Header Protection", or "[RFC8551HP](#)". Substantial testing has shown that [RFC8551HP](#) does not interact well with some Legacy MUAs (see [Section 1.1.1](#)).

This specification supersedes [RFC8551HP](#), effectively replacing the final two paragraphs of [Section 3.1](#) of [RFC8551].

In this specification, all Header Fields gain end-to-end cryptographic integrity and authenticity by being copied directly into the Cryptographic Payload without using an intervening `message/rfc822` MIME object. In an encrypted message, some Header Fields can also be made confidential by removing or obscuring them from the Outer Header Section.

This specification also offers substantial security, privacy, and usability guidance for sending and receiving MUAs that was not considered in [RFC8551].

1.1.1. Problems with RFC 8551 Header Protection

Several Legacy MUAs have difficulty rendering a message that uses [RFC8551HP](#). These problems can appear on signed-only messages, as well as signed-and-encrypted messages.

In some cases, some MUAs cannot render `message/rfc822` message subparts at all, which is in violation of baseline MIME requirements as defined in [Section 2](#) of [\[RFC2049\]](#). A message using [RFC8551HP](#) is unreadable by any recipient using such an MUA.

In other cases, the user sees an attachment suggesting a forwarded email message that -- in fact -- contains the protected email message that should be rendered directly. In most of these cases, the user can click on the attachment to view the protected message.

However, viewing the protected message as an attachment in isolation may strip it of any security indications, leaving the user unable to assess the cryptographic properties of the message. Worse, for encrypted messages, interacting with the protected message in isolation may leak contents of the cleartext, for example, if the reply is not also encrypted.

Furthermore, [RFC8551HP](#) lacks any discussion of the following points, all of which are provided in this specification:

- Which Header Fields should be given end-to-end cryptographic integrity and authenticity protections (this specification mandates protection of all Header Fields that the sending MUA knows about).
- How to securely indicate the sender's intent to offer Header Protection and encryption, which lets a receiving MUA detect messages whose cryptographic properties may have been modified in transit (see [Section 2.1.1](#)).
- Which Header Fields should be given end-to-end cryptographic confidentiality protections in an encrypted message and how (see [Section 3](#)).
- How to securely indicate the sender's choices about which Header Fields were made confidential, which lets a receiving MUA reply or forward an encrypted message safely without accidentally leaking confidential material (see [Section 2.2](#)).

These stumbling blocks with Legacy MUAs, missing mechanisms, and missing guidance create a strong disincentive for existing MUAs to generate messages using [RFC8551HP](#). Because few messages have been produced, there has been little incentive for those MUAs capable of upgrading to bother interpreting them better.

In contrast, the mechanisms defined here are safe to adopt and produce messages with very few problems for Legacy MUAs. And [Section 4.10](#) provides useful guidance for rendering and replying to [RFC8551HP](#) messages.

1.2. Risks of Header Protection for Legacy MUA Recipients

Producing a signed-only message using this specification is risk free. Such a message will render in the same way on any Legacy MUA as a Legacy Signed Message (that is, a signed message without Header Protection). An MUA conformant to this specification that encounters such a message will be able to gain the benefits of end-to-end cryptographic integrity and authenticity for all Header Fields.

An encrypted message produced according to this specification that has some User-Facing Header Fields removed or obscured may not render as desired in a Legacy MUA. In particular, those Header Fields that were made confidential will not be visible to the user of a Legacy MUA. For example, if the Subject Header Field outside the Cryptographic Envelope is replaced with [. . .], a Legacy MUA will render the [. . .] anywhere the Subject is normally seen. This is the only risk of producing an encrypted message according to this specification.

A workaround "Legacy Display" mechanism is provided in this specification (see [Section 2.1.2](#)). Legacy MUAs will render "Legacy Display Elements" to the user, albeit not in the same location that the Header Fields would normally be rendered.

Alternately, if the sender of an encrypted message is particularly concerned about the experience of a recipient using a Legacy MUA, and they are willing to accept leaking the User-Facing Header Fields, they can simply adopt the No [Header Confidentiality Policy](#) (see [Section 3.2.3](#)). A signed-and-encrypted message composed using the No [Header Confidentiality Policy](#) offers no usability risk for a reader using a Legacy MUA and retains end-to-end cryptographic integrity and authenticity properties for all Header Fields for any reader using a conformant MUA. Of course, such a message has the same (non-existent) confidentiality properties for all Header Fields as a Legacy Encrypted Message (that is, an encrypted message made without Header Protection).

1.3. Motivation

Ordinary Users generally do not understand the distinction between email message Body and Header Section. When an email message has cryptographic protections that cover the message Body but not the Header Fields, several attacks become possible.

For example, a Legacy Signed Message has a signature that covers the Body but not the Header Fields. An attacker can therefore modify the Header Fields (including Subject) without invalidating the signature. Since most readers consider a message Body in the context of the message's Subject, the meaning of the message itself could change drastically (under the attacker's control) while still retaining the same cryptographic indicators of integrity and authenticity.

In another example, a Legacy Encrypted Message has its Body effectively hidden from an adversary that snoops on the message. But if the Header Fields are not also encrypted, significant information about the message (such as the message Subject) will leak to the inspecting adversary.

However, if the sending and receiving MUAs ensure that cryptographic protections cover the message Header Section as well as the message Body, these attacks are defeated.

1.3.1. Backward Compatibility

If the sending MUA is unwilling to generate such a fully protected message due to the potential for rendering, usability, deliverability, or security issues, these defenses cannot be realized.

The sender cannot know what MUA (or MUAs) the recipient will use to handle the message. Thus, an outbound message format that is backward compatible with as many legacy implementations as possible is a more effective vehicle for providing the whole-message cryptographic protections described above.

This document aims for backward compatibility with Legacy MUAs to the extent possible. In some cases, like when a user-visible Header Field like the Subject is cryptographically hidden, a Legacy MUA will not be able to render or reply to the message exactly the same way as a conformant MUA would. But accommodations are described here that ensure a rough semantic equivalence for a Legacy MUA even in these cases.

1.3.2. Deliverability

A message with perfect cryptographic protections that cannot be delivered is less useful than a message with imperfect cryptographic protections that can be delivered. Senders want their messages to reach the intended recipients.

Given the current state of the Internet mail ecosystem, encrypted messages in particular cannot shield all of their Header Fields from visibility and still be guaranteed delivery to their intended recipient.

This document accounts for this concern by providing a mechanism ([Section 3](#)) that prioritizes initial deliverability (at the cost of some header leakage) while facilitating future message variants that shield more header metadata from casual inspection.

1.4. Other Protocols to Protect Email Header Fields

A separate pair of protocols also provides some cryptographic protection for the email message header integrity: DomainKeys Identified Mail (DKIM) [[RFC6376](#)], as used in combination with Domain-based Message Authentication, Reporting, and Conformance (DMARC) [[RFC7489](#)]. This pair of protocols provides a domain-based reputation mechanism that can be used to mitigate some forms of unsolicited email (spam).

However, the DKIM+DMARC suite provides cryptographic protection at a different scope, as it is usually applied by and evaluated by a mail transport agent (MTA). DKIM+DMARC typically provide MTA-to-MTA protection, whereas this specification provides MUA-to-MUA protection. This is because DKIM+DMARC are typically applied to messages by (and interpreted by) MTAs, whereas the mechanisms in this document are typically applied and interpreted by MUAs.

A receiving MUA that relies on DKIM+DMARC for sender authenticity should note [Section 10.1](#).

Furthermore, the DKIM+DMARC suite only provides cryptographic integrity and authentication, not encryption. So cryptographic confidentiality is not available from that suite.

The DKIM+DMARC suite can be used on any message, including messages formed as defined in this document. There should be no conflict between DKIM+DMARC and the specification here.

Though not strictly email, similar protections have been in use on Usenet for the signing and verification of message Header Fields for years. See [\[PGPCONTROL\]](#) and [\[PGPVERIFY-FORMAT\]](#) for more details. Like DKIM, these Usenet control protections offer only integrity and authentication, not confidentiality.

1.5. Applicability to PGP/MIME

This document specifies end-to-end cryptographic protections for email messages in reference to S/MIME [\[RFC8551\]](#).

Comparable end-to-end cryptographic protections can also be provided by PGP/MIME [\[RFC3156\]](#).

The mechanisms in this document should be applicable in the PGP/MIME protections as well as S/MIME protections, but analysis and implementation in this document focuses on S/MIME.

To the extent that any divergence from the mechanism defined here is necessary for PGP/MIME, that divergence is out of scope for this document.

1.6. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [\[RFC2119\]](#) [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

1.7. Terms

The following terms are defined for the scope of this document:

S/MIME: Secure/Multipurpose Internet Mail Extensions (see [\[RFC8551\]](#))

PGP/MIME: Pretty Good Privacy with MIME (see [\[RFC3156\]](#))

Message: An email message consisting of Header Fields (collectively called "the Header Section of the message") optionally followed by a message Body; see [\[RFC5322\]](#).

Note: To avoid ambiguity, this document avoids using the terms "Header" or "Headers" in isolation, but instead always uses "Header Field" to refer to the individual field and "Header Section" to refer to the entire collection.

Header Field: A Header Field includes a field name, followed by a colon (":"), followed by a field Body (value), and is terminated by CRLF; see [Section 2.2](#) of [\[RFC5322\]](#) for more details.

Header Section: The Header Section is a sequence of lines of characters with special syntax as defined in [\[RFC5322\]](#). The Header Section of a message contains the Header Fields associated with the message itself. The Header Section of a MIME part (that is, a subpart of a message) typically contains Header Fields associated with that particular MIME part.

Outer Header Section: The unprotected Header Section that MTAs and MUAs unaware of Header Protection treat as the Header Section of the Message.

Body: The Body is the part of a message that follows the Header Section and is separated from the Header Section by an empty line (that is, a line with nothing preceding the CRLF); see [\[RFC5322\]](#). It is the (bottom) section of a message containing the payload of a message. Typically, the Body consists of a (possibly multipart) MIME [\[RFC2045\]](#) construct.

Header Protection (HP): The cryptographic protection of email Header Sections (or parts of it) by means of signatures and/or encryption.

Legacy MUA: An MUA that does not understand Header Protection as defined in this document. A Legacy Non-Crypto MUA is incapable of doing any end-to-end cryptographic operations. A Legacy Crypto MUA is capable of doing cryptographic operations but does not understand or generate messages with Header Protection.

Legacy Signed Message: An email message that was signed by a Legacy MUA and therefore has no cryptographic authenticity or integrity protections on its Header Fields.

Legacy Encrypted Message: An email message that was signed and encrypted by a Legacy MUA and therefore has no cryptographic authenticity, integrity, or confidentiality protections on any of its Header Fields.

Header Confidentiality Policy (HCP): A functional specification of which Header Fields should be removed or obscured when composing an encrypted message with Header Protection. An HCP is considered more "conservative" when it removes or obscures fewer Header Fields. When it removes or obscures more Header Fields, it is more "ambitious". See [Section 3](#).

Ordinary User: A user of an MUA who follows a simple and minimal experience, focused on sending and receiving emails. A user who opts into advanced configuration, expert mode, or the like is not an "Ordinary User".

Additionally, Cryptographic Layer, Cryptographic Payload, Cryptographic Envelope, Cryptographic Summary, Structural Header Fields, Non-Structural Header Fields, Main Body Part, User-Facing Header Fields, and MUA are all used as defined in [\[RFC9787\]](#).

The policies "Specification Required" and "IETF Review" that appear in this document when used to describe namespace allocation are to be interpreted as described in [\[RFC8126\]](#).

1.8. Document Scope

This document describes sensible, simple behavior for a program that generates an email message with standard end-to-end cryptographic protections, following the guidance in [\[RFC9787\]](#). An implementation conformant to this document will produce messages that have cryptographic protection that covers the message's Header Fields as well as its Body.

1.8.1. In Scope

This document also describes sensible, simple behavior for a program that interprets such a message in a way that can take advantage of these protections covering the Header Fields as well as the Body.

The message generation guidance aims to minimize negative interactions with any Legacy receiving MUA while providing actionable cryptographic properties for modern receiving MUAs.

In particular, this document focuses on two standard types of cryptographic protection that cover the entire message:

- a cleartext message with a single signature and
- an encrypted message that contains a single cryptographic signature.

1.8.2. Out of Scope

The message composition guidance in this document (in [Section 5.2](#)) aims to provide minimal disruption for any Legacy MUA that receives such a message. However, by definition, a Legacy MUA does not implement any of the guidance here. Therefore, the document does not attempt to provide guidance for Legacy MUAs directly.

Furthermore, this document does not explicitly contemplate other variants of cryptographic message protections, including any of these:

- encrypted-only message (without a cryptographic signature; see [Section 5.3](#) of [RFC9787])
- triple-wrapped message
- signed message with multiple signatures
- encrypted message with a cryptographic signature outside the encryption

All such messages are out of scope of this document.

1.9. Example

This section gives an overview by providing an example of how MIME messages with Header Protection look.

Consider the following MIME message:

```
A └─ application/pkcs7-mime; smime-type="enveloped-data"
   ↓ (decrypts to)
B └─ application/pkcs7-mime; smime-type="signed-data"
   ↓ (unwraps to)
C └─ multipart/alternative; hp="cipher"
D   └─ text/plain; hp-legacy-display="1"
E   └─ text/html; hp-legacy-display="1"
```

Observe that:

- Nodes A and B are collectively called the Cryptographic Envelope. Node C (including its subnodes D and E) is called the Cryptographic Payload [RFC9787].
- Node A contains the traditional unprotected ("outer") Header Fields. Node C contains the protected ("inner") Header Fields.
- The presence of the hp attribute (see [Section 2.1.1](#)) on the Content-Type of node C allows the receiver to know that the sender applied Header Protection. Its value allows the receiver to distinguish whether the sender intended for the message to be confidential (hp="cipher") or not (hp="clear"), since encryption may have been added in transit (see [Section 10.2](#)).

The "outer" Header Section on node A looks as follows:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: [...]
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: application/pkcs7-mime; smime-type="enveloped-data"
MIME-Version: 1.0
```

The "inner" Header Section on node C looks as follows:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Keywords: Contract, Urgent
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: multipart/alternative; hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:08:43 -0500
HP-Outer: From: Bob <bob@example.net>
HP-Outer: To: Alice <alice@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <20230111T210843Z.1234@lhp.example>
```

Observe that:

- Between node C and node A, some Header Fields are copied as is (Date, From, To, Message-ID), some are obscured (Subject), and some are removed (Keywords).
- The HP-Outer Header Fields (see [Section 2.2](#)) of node C contain a protected copy of the Header Fields in node A. The copy allows the receiver to recompute for which Header Fields the sender provided confidentiality by removing or obscuring them.
- The copying/removing/obscuring and the HP-Outer only apply to Non-Structural Header Fields, not to Structural Header Fields like Content-Type or MIME-Version (see [Section 1.1](#) of [RFC9787]).

- If the sender intends no confidentiality and doesn't encrypt the message, it doesn't remove or obscure Header Fields. All Non-Structural Header Fields are copied as is. No HP-Outer Header Fields are present.

Node D looks as follows:

```
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";  
  
Subject: Handling the Jones contract  
Keywords: Contract, Urgent  
  
Please review and approve or decline by Thursday, it's critical!  
  
Thanks,  
Bob  
  
--  
Bob Gonzalez  
ACME, Inc.
```

Observe that:

- The sender adds the removed and obscured User-Facing Header Fields (see [Section 1.1.2 of \[RFC9787\]](#)) to the main Body (note the empty line after the Content-Type). This is called the Legacy Display Element. It allows a user with a Legacy MUA that doesn't implement this document to understand the message, since the Header Fields will be shown as part of the main Body.
- The `hp-legacy-display="1"` attribute (see [Section 2.1.2](#)) indicates that the sender added a Legacy Display Element. This allows receivers that implement this document to recognize the Legacy Display Element and distinguish it from user-added content. The receiver then hides the Legacy Display Element and doesn't display it to the user.
- `hp-legacy-display` is added to the node to which it applies, not on any outer nodes (e.g., not to node C).

For more examples, see Appendices [D](#) and [E](#).

2. Internet Message Format Extensions

This section describes relevant, backward-compatible extensions to the Internet Message Format [\[RFC5322\]](#). Subsequent sections offer concrete guidance for an MUA to make use of these mechanisms, including policy decisions and recommended pseudocode.

2.1. Content-Type Parameters

This document introduces two parameters for the Content-Type Header Field, which have distinct semantics and use cases.

2.1.1. Content-Type Parameter: hp

This specification defines a parameter for the Content-Type Header Field named hp (for Header Protection). This parameter is only relevant on the Content-Type Header Field at the root of the Cryptographic Payload. The presence of this parameter at the root of the Cryptographic Payload indicates that the sender intends for this message to have end-to-end cryptographic protections for the Header Fields.

The parameter's defined values describe the sender's cryptographic intent when producing the message:

hp Value	Authenticity	Integrity	Confidentiality	Description
"clear"	yes	yes	no	This message has been signed by the sender, with Header Protection.
"cipher"	yes	yes	yes	This message has been signed by the sender, with Header Protection, and is encrypted to the recipients.

Table 1: hp Parameter for Content-Type Header Field

A sending implementation **MUST NOT** produce a Cryptographic Payload with parameter hp="cipher" for an unencrypted message (that is, where none of the Cryptographic Layers in the Cryptographic Envelope of the message provide encryption). Likewise, if a sending implementation is sending an encrypted message with Header Protection, it **MUST** emit an hp="cipher" parameter, regardless of which Header Fields were made confidential.

Note that hp="cipher" indicates that the message itself has been encrypted by the sender to the recipients but makes no assertions about which Header Fields have been removed or obscured. This can be derived from the Cryptographic Payload itself (see [Section 4.2](#)).

A receiving implementation **MUST NOT** mistake the presence of an hp="cipher" parameter in the Cryptographic Payload for the actual presence of a Cryptographic Layer that provides encryption.

2.1.2. Content-Type Parameter: hp-legacy-display

This specification also defines an hp-legacy-display parameter for the Content-Type Header Field. The only defined value for this parameter is 1.

This parameter is only relevant on a leaf MIME node of Content-Type text/html or text/plain within a well-formed message with end-to-end cryptographic protections. Its presence indicates that the MIME node it is attached to contains a decorative "Legacy Display Element". The Legacy Display Element itself is used for backward-compatible visibility of any removed or obscured User-Facing Header Field in a Legacy MUA.

Such a Legacy Display Element need not be rendered to the user of an MUA that implements this specification, because the MUA already knows the correct Header Field information and can render it to the user in the appropriate part of the MUA's user interface rather than in the Body of the message.

See [Section 5.2.2](#) for how to insert a Legacy Display Element into a `text/plain` Main Body Part. See [Section 5.2.3](#) for how to insert a Legacy Display Element into a `text/html` Main Body Part. See [Section 4.5.3](#) for how to avoid rendering a Legacy Display Element.

2.2. HP-Outer Header Field

This document also specifies a new Header Field: `HP-Outer`.

This Header Field is used only in the Header Section of the Cryptographic Payload of an encrypted message. It is not relevant for signed-only messages. It documents, with the same cryptographic guarantees shared by the rest of the message, the sender's choices about Header Field confidentiality. It does so by embedding a copy within the Cryptographic Envelope of every Non-Structural Header Field that the sender put outside the Cryptographic Envelope. This Header Field enables the MUA receiving the encrypted message to reliably identify whether the sending MUA intended to make a Header Field confidential (see [Section 11.3](#)).

The `HP-Outer` Header Fields in a message's Cryptographic Payload are useful for ensuring that any confidential Header Field will not be automatically leaked in the clear if the user replies to or forwards the message. They may also be useful for an MUA that indicates the confidentiality status of any given Header Field to the user.

An implementation that composes encrypted email **MUST** include a copy of all Non-Structural Header Fields deliberately exposed to the outside of the Cryptographic Envelope using a series of `HP-Outer` Header Fields within the Cryptographic Payload. These `HP-Outer` MIME Header Fields should only ever appear directly within the Header Section of the Cryptographic Payload of a Cryptographic Envelope offering confidentiality. They **MUST** be ignored for the purposes of evaluating the message's Header Protection if they appear in other places.

Each instance of `HP-Outer` contains a Non-Structural Header Field name and the value that this Header Field was set in within the outer (unprotected) Header Section. The `HP-Outer` Header Field can appear multiple times in the Header Section of a Cryptographic Payload.

If a Non-Structural Header Field named `Z` is present in Header Section of the Cryptographic Payload but doesn't appear in an `HP-Outer` Header Field value at all, then the sender is effectively asserting that every instance of `Z` was made confidential by removal from the Outer Header Section. Specifically, it means that no Header Field `Z` was included on the outside of the message's Cryptographic Envelope by the sender at the time the message was injected into the mail system.

See [Section 5.2](#) for how to insert HP-Outer Header Fields into an encrypted message. See [Section 4.3](#) for how to determine the end-to-end confidentiality of a given Header Field from an encrypted message with Header Protection using HP-Outer. See [Section 6.1](#) for how an MUA can safely reply to (or forward) an encrypted message without leaking confidential Header Fields by default.

2.2.1. HP-Outer Header Field Definition

The syntax of this Header Field is defined using the following ABNF [[RFC5234](#)], where field-name, WSP, VCHAR, and FWS are defined in [[RFC5322](#)]:

```
hp-outer      = "HP-Outer:" [FWS] field-name ": "  
                hp-outer-value CRLF  
  
hp-outer-value = (*( [FWS] VCHAR ) *WSP)
```

Note that hp-outer-value is the same as unstructured from [Section 3.2.5](#) of [[RFC5322](#)] but without the obsolete obs-unstruct option.

3. Header Confidentiality Policy

An MUA composing an encrypted message according to this specification may make any given Header Field confidential by removing it from the Header Section outside the Cryptographic Envelope or by obscuring it by rewriting it to a different value in that Outer Header Section. The composing MUA faces a choice for any new message: Which Header Fields should be made confidential, and how?

This section defines the "[Header Confidentiality Policy](#)" (or [HCP](#)) as a well-defined abstraction to encourage MUA developers to consider, document, and share reasonable policies across the community. It establishes a registry of known HCPs, defines a small number of simple HCPs in that registry, and makes a recommendation for a reasonable default.

Note that such a policy is only needed when the end-to-end protections include encryption (confidentiality). No comparable policy is needed for other end-to-end cryptographic protections (integrity and authenticity), as they are simply uniformly applied so that all Header Fields known by the sender have these protections.

This asymmetry is a consequence of complexities in existing message delivery systems, some of which may reject, drop, or delay messages where all Header Fields are removed from the top-level MIME object.

Note that no representation of the [HCP](#) itself ever appears "on the wire". However, the consumer of the encrypted message can see the decisions that were made by the sender's [HCP](#) via the HP-Outer Header Fields (see [Section 2.2](#)).

3.1. HCP Definition

In this document, we represent that [Header Confidentiality Policy](#) as a function `hcp`:

- `hcp(name, val_in) -> val_out`: This function takes a Non-Structural Header Field identified by name with the initial value `val_in` as arguments and returns a replacement Header Field value `val_out`. If `val_out` is the special value `null`, it means that the Header Field in question should be removed from the set of Header Fields visible outside the Cryptographic Envelope.

In the pseudocode descriptions of various choices of [HCP](#) in this document, any comparison with the name input is done case-insensitively. This is appropriate for Header Field names, as described in [\[RFC5322\]](#).

Note that `hcp` is only applied to Non-Structural Header Fields. When composing a message, Structural Header Fields are dealt with separately, as described in [Section 5.2](#).

As an example, an MUA that obscures the Subject Header Field by replacing it with the literal string "[...]" hides all Cc'ed recipients and does not offer confidentiality to any other Header Fields that would be represented as (in pseudocode):

```
hcp_example_hide_cc(name, val_in) -> val_out:
  if lower(name) is 'subject':
    return '[...]'
  else if lower(name) is 'cc':
    return null
  else:
    return val_in
```

For alignment with common practice as well as the ABNF in [Section 2.2.1](#) for HP-Outer, `val_out` **MUST** be one of the following:

- identical to `val_in`,
- the special value `null` (meaning that the Header Field will be removed from the outside of the message), or
- a sequence of whitespace (that is, space or tab) and printable 7-bit, clean ASCII characters (of course, non-ASCII text can be encoded as ASCII using the encoded-word construct from [\[RFC2047\]](#))

The [HCP](#) can compute `val_out` using any technique describable in pseudocode, such as copying a fixed string or invocations of other pseudocode functions. If it alters the value, it **MUST NOT** include control or NUL characters in `val_out`. `val_out` **SHOULD** match the expected ABNF for the Header Field identified by name.

3.1.1. HCP Avoids Changing addr-spec of From Header Field

The From Header Field should also be treated specially by the [HCP](#) to enable defense against possible email address spoofing (see [Section 10.1](#)). In particular, for `hcp("From", val_in)`, the `addr-spec` of `val_in` and the `addr-spec` of `val_out` **SHOULD** match according to [Section 4.4.5](#), unless the sending MUA has additional knowledge coordinated with the receiving MUA about more subtle `addr-spec` equivalence or certificate validity.

3.2. Initial Registered HCPs

This document formally defines three Header Confidentiality Policies with known and reasonably well-understood characteristics as a way to compare and contrast different possible behavioral choices for a composing MUA. These definitions are not meant to preclude the creation of other HCPs.

The purpose of the registry of HCPs is to facilitate [HCP](#) evolution and interoperability discussion among MUA developers and MTA operators.

(The example hypothetical [HCP](#), `hcp_example_hide_cc`, described in [Section 3.1](#) above is deliberately not formally registered, as it has not been evaluated in practice.)

3.2.1. Baseline Header Confidentiality Policy

The most conservative recommended [Header Confidentiality Policy](#) only provides confidentiality for Informational Fields, as defined in [Section 3.6.5](#) of [\[RFC5322\]](#). These fields are "only human-readable content" and thus their content should not be relevant to transport agents. Since most Internet messages today do have a Subject Header Field, and some filtering engines might object to a message without a Subject, this policy is conservative and merely obscures that Header Field by replacing it with a fixed string `[...]`. By contrast, Comments and Keywords Header Fields are comparatively rare, so these fields are removed entirely from the Outer Header Section.

```
hcp_baseline(name, val_in) → val_out:
  if lower(name) is 'subject':
    return '[...]'
  else if lower(name) is in ['comments', 'keywords']:
    return null
  else:
    return val_in
```

`hcp_baseline` is the recommended default [HCP](#) for a new implementation, as it provides meaningful confidentiality protections and is unlikely to cause deliverability or usability problems.

3.2.2. Shy Header Confidentiality Policy

Alternately, a slightly more ambitious (and therefore more privacy-preserving) [Header Confidentiality Policy](#) might avoid leaking human-interpretable data that MTAs generally don't care about. The additional protected data isn't related to message routing or transport but might reveal sensitive information about the sender or their relationship to the recipients. This "shy" [HCP](#) builds on `hcp_baseline` but also:

- avoids revealing the `display-name` of each identified email address and
- avoids leaking the sender's locally configured time zone in the Date Header Field.

```
hcp_shy(name, val_in) → val_out:
  if lower(name) is 'from':
    if val_in is an RFC 5322 mailbox:
      return the RFC 5322 addr-spec part of val_in
  if lower(name) in ['to', 'cc']:
    if val_in is an RFC 5322 mailbox-list:
      let val_out be an empty mailbox-list
      for each mailbox in val_in:
        append the RFC 5322 addr-spec part of mailbox to val_out
      return val_out
  if lower(name) is 'date':
    if val_in is an RFC 5322 date-time:
      return the UTC form of val_in
  else if lower(name) is 'subject':
    return ' [...]'
  else if lower(name) is in ['comments', 'keywords']:
    return null
  return val_in
```

`hcp_shy` requires more sophisticated parsing and Header Field manipulation and is not recommended as a default [HCP](#) for new implementations.

3.2.3. No Header Confidentiality Policy

Legacy MUAs can be conceptualized as offering a "No Header Confidentiality" Policy, which offers no confidentiality protection to any Header Field:

```
hcp_no_confidentiality(name, val_in) → val_out:
  return val_in
```

A conformant MUA that is not modified by local policy or configuration **MUST NOT** use `hcp_no_confidentiality` by default.

3.3. Default Header Confidentiality Policy

An MUA **MUST** have a default [Header Confidentiality Policy](#) that offers confidentiality for the Subject Header Field at least. Local policy and configuration may alter this default, but the MUA **SHOULD NOT** require the user to select an [HCP](#).

hcp_baseline provides confidentiality for the Subject Header Field by replacing it with the literal string "[...]". It also provides confidentiality for the other less common Informational Header Fields (Comments and Keywords) by removing them entirely from the Outer Header Section. This is a sensible default because most users treat the Informational Fields of a message (particularly the Subject) the same way that they treat the Body, and they are surprised to find that the Subject of an encrypted message is visible.

3.4. HCP Evolution

This document does not mandate any particular [Header Confidentiality Policy](#), though it offers guidance for MUA implementers in selecting one in [Section 3.3](#). Future documents may recommend or mandate such a policy for an MUA with specific needs. Such a recommendation might be motivated by descriptions of metadata-derived attacks, stem from research about message deliverability, or describe new signaling mechanisms, but these topics are out of scope for this document.

3.4.1. Offering More Ambitious Header Confidentiality

An MUA **MAY** offer even more ambitious confidentiality for Header Fields of an encrypted message than defined in [Section 3.2.2](#). For example, it might implement an [HCP](#) that removes the To and Cc Header Fields entirely, relying on the SMTP envelope to ensure proper routing. Or it might remove References and In-Reply-To so that message threading is not visible to any MTA. Any more ambitious choice might result in deliverability, rendering, or usability issues for the relevant messages, so testing and documentation will be valuable to get this right.

The authors of this document hope that implementers with deployment experience will document their chosen [Header Confidentiality Policy](#) and the rationale behind their choice.

3.4.2. Expert Guidance for Registering Header Confidentiality Policies

There is no formal syntax specified for the [Header Confidentiality Policy](#), but any attempt to specify an [HCP](#) for inclusion in the registry needs to provide:

- a stable reference document clearly indicating the distinct name for the proposed [HCP](#),
- pseudocode that other implementers can clearly and unambiguously interpret,
- a clear explanation of why this [HCP](#) is different from all other registered HCPs, and
- any relevant considerations related to deployment of the [HCP](#) (for example, known or expected deliverability, rendering, or privacy challenges and possible mitigations).

When the proposed [HCP](#) produces any non-null output for a given Header Field name, val_out **SHOULD** match the expected ABNF for that Header Field. If the proposed [HCP](#) does not match the expected ABNF for that Header Field, the documentation should explicitly identify the relevant circumstances and provide a justification for the deviation.

An entry should not be marked as "Recommended" unless it has been shown to offer confidentiality or privacy improvements over the status quo and have minimal or mitigable negative impact on messages to which it is applied, considering factors such as message deliverability and security. Only one entry in the table (hcp_baseline) is initially marked as "Recommended". In the future, more than one entry may be marked as "Recommended".

4. Receiving Guidance

An MUA that receives a cryptographically protected email will render it for the user.

The receiving MUA will render the message Body, render a selected subset of Header Fields, and provide a summary of the cryptographic properties of the message (as described in [Section 3](#) of [\[RFC9787\]](#)).

Most MUAs only render a subset of Header Fields by default. For example, most MUAs render the From, To, Cc, Date, and Subject Header Fields to the user, but few render Message-Id or Received.

An MUA that knows how to handle a message with Header Protection makes the following four changes to its behavior when rendering a message:

- If the MUA detects that an incoming message has protected Header Fields:
 - For a Header Field that is present in the protected Header Section, the MUA **SHOULD** render the protected value and ignore any unprotected counterparts that may be present (with a special exception for the From Header Field (see [Section 4.4](#))).
 - For a Header Field that is present only in the unprotected Header Section, the MUA **SHOULD NOT** render that value. If it does render the value, the MUA **SHOULD** indicate that the rendered value is unprotected. For an exception to this, see [Section 7](#) for a discussion of some specific Header Fields that are known to be added in transit and therefore are not expected to have end-to-end cryptographic protections.
- The MUA **SHOULD** include information in the message's Cryptographic Summary to indicate the types of protection that applied to each rendered Header Field (if any).
- If any Legacy Display Elements are present in the Body of the message, it does not render them.
- When replying to a message with confidential Header Fields, the replying MUA avoids leaking any Header Fields that were confidential in the original into the cleartext of the reply. It does this even if its own [Header Confidentiality Policy](#) would not have treated those Header Fields as confidential. See [Section 6](#) for more details.

Note that an MUA that handles a message with Header Protection does *not* need to render any new Header Fields that it did not render before.

4.1. Identifying That a Message Has Header Protection

An incoming message can be identified as having Header Protection using the following test:

- The Cryptographic Payload has parameter `hp` set to `"clear"` or `"cipher"`. See [Section 4.5](#) for rendering guidance.

When consuming a message, an MUA **MUST** ignore the `hp` parameter to `Content-Type` when it encounters it anywhere other than the root of the message's Cryptographic Payload.

4.2. Extracting Protected and Unprotected ("Outer") Header Fields

When a message is encrypted and uses Header Protection, an MUA extracts a list of protected Header Fields (names and values), as well as a list of Header Fields that were added by the original message sender in unprotected form to the outside of the message's Cryptographic Envelope.

The following algorithm takes reference message `refmsg` as input, which is encrypted with Header Protection as described in this document (that is, the Cryptographic Envelope includes a Cryptographic Layer that provides encryption, and the `hp` parameter for the `Content-Type` Header Field of the Cryptographic Payload is `cipher`). It produces as output a pair of lists of `(h, v)` Header Fields.

4.2.1. HeaderSetsFromMessage

Method signature:

`HeaderSetsFromMessage(refmsg) -> (refouter, refprotected)`

Procedure:

1. Let `refheaders` be the list of `(h, v)` protected Header Fields found in the root of the Cryptographic Payload.
2. Let `refouter` be an empty list of Header Field names and values.
3. Let `refprotected` be an empty list of Header Field names and values.
4. For each `(h, v)` in `refheaders`:
 - i. If `h` is `HP-Outer`:
 - a. Split `v` into `(h1, v1)` on the first colon (`:`), followed by any amount of whitespace.
 - b. Append `(h1, v1)` to `refouter`.
 - ii. Else:
 - a. Append `(h, v)` to `refprotected`.
5. Return `refouter, refprotected`.

Note that this algorithm is independent of the unprotected Header Fields. It derives its output only from the normal Header Fields and the HP-Outer Header Fields, both contained inside the Cryptographic Payload.

4.3. Updating the Cryptographic Summary

Regardless of whether a cryptographically protected message has protected Header Fields, the Cryptographic Summary of the message should be modified to indicate what protections the Header Fields have. This field-by-field status is complex and isn't necessarily intended to be presented in full to the user. Rather, it represents the state of the message internally within the MUA and may be used to influence behavior like replying to the message (see [Section 6.1](#)).

Each Header Field individually has exactly one of the following protection states:

- **unprotected** (has no Header Protection)
- **signed-only** (bound into the same validated signature as the enclosing message, but also visible in transit)
- **encrypted-only** (only appears within the Cryptographic Payload; the corresponding external Header Field was either removed or obscured)
- **signed-and-encrypted** (same as encrypted-only, but additionally is under a validated signature)

If the message does not have Header Protection (as determined by [Section 4.1](#)), then all of the Header Fields are by definition **unprotected**.

If the message has Header Protection, an MUA **SHOULD** use the following algorithm to compute the protection state of a protected Header Field (*h*, *v*) (that is, an element of *refprotected* from [Section 4.2](#)):

4.3.1. HeaderFieldProtection

Method signature:

HeaderFieldProtection(msg, *h*, *v*) -> protection_state

Procedure:

1. Let *ct* be the Content-Type of the root of the Cryptographic Payload of *msg*.
2. Compute (*refouter*, *refprotected*) from [HeaderSetsFromMessage\(msg\)](#).
3. If (*h*, *v*) is not in *refprotected*:
 - i. Abort, *v* is not a valid value for Header Field *h*.
4. Let *is_sig_valid* be false.
5. If the message is signed:
 - i. Let *is_sig_valid* be the result of validating the signature.

6. If the message is encrypted, and if `ct` has a parameter `hp="cipher"`, and if (h, v) is not in `refouter`:
 - i. Return signed-and-encrypted if `is_sig_valid`, otherwise return encrypted-only.
7. Return signed-only if `is_sig_valid`, otherwise return unprotected.

Note that:

- This algorithm is independent of the unprotected Header Fields. It derives the protection state only from (h, v) and the set of HP-Outer Header Fields, both of which are inside the Cryptographic Envelope.
- If the signature fails validation, the MUA lowers the affected state to unprotected or encrypted-only without any additional warning to the user, as specified by [Section 3.1](#) of [\[RFC9787\]](#).
- Data from signed-and-encrypted and encrypted-only Header Fields may still not be fully private (see [Section 11.2](#)).
- Encryption may have been added in transit to an originally signed-only message. Thus, only consider Header Fields to be confidential if the sender indicates it with the `hp="cipher"` parameter.
- The protection state of a Header Field may be weaker than that of the message Body. For example, a message Body can be signed-and-encrypted, but a Header Field that is copied unmodified to the unprotected Header Section is signed-only.

If the message has Header Protection, Header Fields that are not in `refprotected` (e.g., because they were added in transit) are unprotected.

Rendering the cryptographic status of each Header Field is likely to be complex and messy -- users may not understand it. It is beyond the scope of this document to suggest any specific graphical affordances or user experience. Future work should include examples of successful rendering of this information.

4.4. Handling Mismatch of From Header Fields

End-to-end (MUA-to-MUA) Header Protection is good for authenticity, integrity, and confidentiality, but it potentially introduces new issues when an MUA depends on its MTA to authenticate parts of the Header Section. The latter is typically the case in modern email systems.

In particular, when an MUA depends on its MTA to ensure that the email address in the (unprotected) From Header Field is authentic, but the MUA renders the email address of the protected From Header Field that differs from the address visible to the MTA, this could create a risk of sender address spoofing (see [Section 10.1](#)). This potential risk applies to signed-only messages as well as signed-and-encrypted messages.

4.4.1. Definitions

4.4.1.1. From Header Field Mismatch

"From Header Field Mismatch" is defined as follows:

The addr-spec of the inner From Header Field doesn't match the addr-spec of the outer From Header Field (see [Section 4.4.5](#)).

Note: The unprotected From Header Field used in this comparison is the actual outer Header Field (as seen by the MTA), not the value indicated by any potential inner HP-Outer.

4.4.1.2. No Valid and Correctly Bound Signature

"No Valid and Correctly Bound Signature" is defined as follows:

There is no valid signature made by a certificate for which the MUA has a valid binding to the protected From address. This includes:

- the message has no signature
- the message has a broken signature
- the message has a valid signature, but the receiving MUA does not see any valid binding between the signing certificate and the addr-spec of the inner From Header Field

Note: There are many possible ways that an MUA could choose to validate a certificate-to-address binding. For example, the MUA could ensure the certificate is issued by one of a set of trusted certification authorities, it could rely on the user to do a manual out-of-band comparison, it could rely on a DNSSEC signal ([[RFC7929](#)] or [[RFC8162](#)]), and so on. It is beyond the scope of this document to describe all possible ways an MUA might validate the certificate-to-address binding or to choose among them.

4.4.2. Warning for From Header Field Mismatch

To mitigate the above described risk of sender address spoofing, an MUA **SHOULD** warn the user whenever both of the following conditions are met:

- From Header Field Mismatch (as defined in [Section 4.4.1.1](#)) and
- No Valid and Correctly Bound Signature (as defined in [Section 4.4.1.2](#))

This warning should be comparable to the MUA's warning about messages that are likely spam or phishing, and it **SHOULD** show both of the non-matching From Header Fields.

4.4.3. From Header Field Rendering

Furthermore, a receiving MUA that depends on its MTA to authenticate the unprotected (outer) From Header Field **SHOULD** render the outer From Header Field (as an exception to the guidance in the beginning of [Section 4](#)) if both of the following conditions are met:

- From Header Field Mismatch (as defined in [Section 4.4.1.1](#)) and
- No Valid and Correctly Bound Signature (as defined in [Section 4.4.1.2](#))

An MUA **MAY** apply a local preference to render a different display name (e.g., from an address book).

See [Section 10.1.1](#) for a detailed explanation of this rendering guidance.

4.4.4. Handling the Protected From Header Field When Responding

When responding to a message, an MUA has different ways to populate the recipients of the new message. Depending on whether it is a Reply, a Reply All, or a Forward, an MUA may populate the composer view using a combination of the referenced message's From, To, Cc, Reply-To, or Mail-Followup-To Header Fields or any other signals.

When responding to a message with Header Protection, an MUA **MUST** only use the protected Header Fields when populating the recipients of the new message.

This avoids compromise of message confidentiality when a man-in-the-middle (MITM) attacker modifies the unprotected From address of an encrypted message, attempting to learn the contents through a misdirected reply. Note that with the rendering guidance above, a MITM attacker can cause the unprotected From Header Field to be displayed. Thus, when responding, the populated To address may differ from the rendered From address. However, this change in addresses should not cause more user confusion than the address change caused by a Reply-To in a Legacy Message does.

4.4.5. Matching addr-specs

When generating (Section 3.1.1) or consuming (Section 4.4) a protected From Header Field, the MUA considers the equivalence of two different addr-spec values.

First, the MUA **MUST** check whether the domain part of an addr-spec being compared contains a U-label [RFC5890]. If it does, it **MUST** be converted to the A-label form as described in [RFC5891]. We call a domain converted in this way (or the original domain if it didn't contain any U-label) "the ASCII version of the domain part". Second, the MUA **MUST** compare the ASCII version of the domain part of the two addr-specs by standard DNS comparison: Assume ASCII text and compare alphabetic characters case-insensitively, as described in Section 3.1 of [RFC1035]. If the domain parts match, then the two local-parts are matched against each other. The simplest and most common comparison for the local-part is also an ASCII-based, case-insensitive match. If the MUA has special knowledge about the domain and, when composing, it can reasonably expect the receiving MUAs to have the same information, it **MAY** match the local-part using a more sophisticated and inclusive matching algorithm.

It is beyond the scope of this document to recommend a more sophisticated and inclusive matching algorithm.

4.5. Rendering a Message with Header Protection

When the Cryptographic Payload's Content-Type has the parameter hp set to "clear" or "cipher", the values of the protected Header Fields are drawn from the Header Fields of the Cryptographic Payload, and the Body that is rendered is the Cryptographic Payload itself.

4.5.1. Example Signed-Only Message

Consider a message with this structure, where the MUA is able to validate the cryptographic signature:

```

A └─ application/pkcs7-mime; smime-type="signed-data"
   ↓ (unwraps to)
B └─ multipart/alternative [Cryptographic Payload + Rendered Body]
C └─ text/plain
D └─ text/html

```

The message Body should be rendered the same way as this message:

```

B └─ multipart/alternative
C └─ text/plain
D └─ text/html

```

The MUA should render Header Fields taken from part B.

Its Cryptographic Summary should indicate that the message was signed and all rendered Header Fields were included in the signature.

Because this message is signed-only, none of its parts will have a Legacy Display Element.

The MUA should ignore Header Fields from part A for the purposes of rendering.

4.5.2. Example Signed-and-Encrypted Message

Consider a message with this structure, where the MUA is able to validate the cryptographic signature:

```

E └─ application/pkcs7-mime; smime-type="enveloped-data"
   ↓ (decrypts to)
F └─ application/pkcs7-mime; smime-type="signed-data"
   ↓ (unwraps to)
G └─ multipart/alternative [Cryptographic Payload + Rendered Body]
H └─ text/plain
I └─ text/html

```

The message Body should be rendered the same way as this message:

```

G └─ multipart/alternative
H └─ text/plain
I └─ text/html

```

It should render Header Fields taken from part G.

Its Cryptographic Summary should indicate that the message is signed-and-encrypted.

When rendering the Cryptographic Status of a Header Field and when composing a reply, each Header Field found in G should be considered against all HP-Outer Header Fields found in G. If an HP-Outer Header Field that matches both the name and value is found, the Header Field's

Cryptographic Status is just signed-only, even though the message itself is signed-and-encrypted. If no matching HP-Outer Header Field is found, the Header Field's Cryptographic Status is signed-and-encrypted, like the rest of the message.

If any of the User-Facing Header Fields are removed or obscured, the composer of this message may have placed Legacy Display Elements in parts H and I.

The MUA should ignore Header Fields from part E for the purposes of rendering.

4.5.3. Do Not Render Legacy Display Elements

As described in [Section 2.1.2](#), a message with cryptographic confidentiality protection **MAY** include Legacy Display Elements for backward compatibility with Legacy MUAs. These Legacy Display Elements are strictly decorative and unambiguously identifiable and will be discarded by compliant implementations.

The receiving MUA **MUST** completely avoid rendering the identified Legacy Display Elements to the user, since it is aware of Header Protection and can render the actual protected Header Fields.

If a text/html or text/plain part within the Cryptographic Envelope is identified as containing Legacy Display Elements, those elements **MUST** be hidden when rendering and **MUST** be dropped when generating a draft reply or inline forwarded message. Whenever a Message or MIME subtree is exported, downloaded, or otherwise further processed, if there is no need to retain a valid cryptographic signature, the implementer **MAY** drop the Legacy Display Elements.

4.5.3.1. Identifying a Part with Legacy Display Elements

A receiving MUA acting on a message that contains an encrypting Cryptographic Layer identifies a MIME subpart within the Cryptographic Payload as containing Legacy Display Elements based on the Content-Type of the subpart. The subpart's Content-Type:

- contains a parameter hp-legacy-display with value set to 1 and
- is either text/html (see [Section 4.5.3.3](#)) or text/plain (see [Section 4.5.3.2](#)).

Note that the term "subpart" above is used in the general sense: If the Cryptographic Payload is a single part, that part itself may contain a Legacy Display Element if it is marked with the hp-legacy-display="1" parameter.

4.5.3.2. Omitting Legacy Display Elements from text/plain

If a text/plain part within the Cryptographic Payload has the Content-Type parameter hp-legacy-display="1", it should be processed before rendering in the following fashion:

- Discard the leading lines of the Body part up to and including the first entirely blank line.

Note that implementing this strategy is dependent on the charset used by the MIME part.

See [Appendix E.1](#) for an example.

4.5.3.3. Omitting Legacy Display Elements from text/html

If a text/html part within the Cryptographic Payload has the Content-Type parameter `hp-legacy-display="1"`, it should be processed before rendering in the following fashion:

- If any element of the HTML `<body>` is a `<div>` with class attribute `header-protection-legacy-display`, that entire element should be omitted.

This cleanup could be done, for example, as a custom rule in the MUA's HTML sanitizer, if one exists. Another implementation strategy for an HTML-capable MUA would be to add an entry to the [\[CSS\]](#) style sheet for such a part:

```
body div.header-protection-legacy-display { display: none; }
```

4.6. Implicitly Rendered Header Fields

While the From, To, Cc, Subject, and Date Header Fields are often explicitly rendered to the user, some Header Fields do affect message display without being explicitly rendered.

For example, the Message-Id, References, and In-Reply-To Header Fields may collectively be used to place a message in a "thread" or series of messages.

In another example, [Section 6.2](#) notes that the value of the Reply-To Header Field can influence the draft reply message. So while the user may never see the Reply-To Header Field directly, it is implicitly "rendered" when the user interacts with the message by replying to it.

An MUA that depends on any implicitly rendered Header Field in a message with Header Protection **MUST** use the value from the protected Header Field and **SHOULD NOT** use any value found outside the cryptographic protection unless it is known to be a Header Field added in transit, as specified in [Section 7](#).

4.7. Handling Undecryptable Messages

An MUA might receive an apparently encrypted message that it cannot currently decrypt. For example, when an MUA does not have regular access to the secret key material needed for decryption, it cannot know the cryptographically protected Header Fields or even whether the message has any cryptographically protected Header Fields.

Such an undecrypted message will be rendered by the MUA as a message without any Header Protection. This means that the message summary may well change how it is rendered when the user is finally able to supply the secret key.

For example, the rendering of the Subject Header Field in a mailbox summary might change from `[ . . . ]` to the real message subject when the message is decrypted. Or the message's placement in a message thread might change if, say, References or In-Reply-To have been removed or obscured (see [Section 4.6](#)).

Additionally, if the MUA does not retain access to the decrypting secret key, and it drops the decrypted form of a message, the message's rendering may revert to the encrypted form. For example, if an MUA follows this behavior, the Subject Header Field in a mailbox summary might change from the real message subject back to [. . .]. Or the message might be displayed outside of its current thread if the MUA loses access to a removed References or In-Reply-To Header Field.

These behaviors are likely to surprise the user. However, an MUA has several possible ways of reducing or avoiding all of these surprises, including:

- Ensuring that the MUA always has access to decryption-capable secret key material.
- Rendering undecrypted messages in a special quarantine view until the decryption-capable secret key material is available.

To reduce or avoid the surprises associated with a decrypted message with removed or obscured Header Fields becoming undecryptable, the MUA could also:

- Securely cache metadata from a decrypted message's protected Header Fields so that its rendering doesn't change after the first decryption.
- Securely store the session key associated with a decrypted message so that attempts to read the message when the long-term secret key is unavailable can proceed using only the session key itself. For example, see the discussion about stashing session keys in [Section 9.1](#) of [\[RFC9787\]](#).

4.8. Guidance for Automated Message Handling

Some automated systems have a control channel that is operated by email. For example, an incoming email message could subscribe someone to a mailing list, initiate the purchase of a specific product, approve another message for redistribution, or adjust the state of some shared object.

To the extent that such a system depends on end-to-end cryptographic guarantees about the email control message, Header Protection as defined in this document should improve the system's security. This section provides some specific guidance for systems that use email messages as a control channel that want to benefit from these security improvements.

4.8.1. Only Interpret Protected Header Fields

Consider the situation where an email-based control channel depends on the message's cryptographic signature and the action taken depends on some Header Field of the message.

In this case, the automated system **MUST** rely on information from the Header Field that is protected by the mechanism defined in this document. It **MUST NOT** rely on any Header Field found outside the Cryptographic Payload.

For example, consider an administrative interface for a mailing list manager that only accepts control messages that are signed by one of its administrators. When an inbound message for the list arrives, it is queued (waiting for administrative approval) and the system generates and

listens for two distinct email addresses related to the queued message -- one that approves the message and one that rejects it. If an administrator sends a signed control message to the approval address, the mailing list verifies that the protected To Header Field of the signed control message contains the approval address before approving the queued message for redistribution. If the protected To Header Field does not contain that address, or there is no protected To Header Field, then the mailing list logs or reports the error and does not act on that control message.

4.8.2. Ignore Legacy Display Elements

Consider the situation where an email-based control channel expects to receive an end-to-end encrypted message -- for example, where the control messages need confidentiality guarantees -- and where the action taken depends on the contents of some MIME part within the message Body.

In this case, the automated system that decrypts the incoming messages and scans the relevant MIME part **MUST** identify when the MIME part contains a Legacy Display Element (see [Section 4.5.3.1](#)), and it **MUST** parse the relevant MIME part with the Legacy Display Element removed.

For example, consider an administrative interface of a confidential issue tracking software. An authorized user can confidentially adjust the status of a tracked issue by a specially formatted first line of the message Body (for example, `severity #183 serious`). When the user's MUA encrypts a plaintext control message to this issue tracker, depending on the MUA's [HCP](#) and its choice of legacy value, it may add a Legacy Display Element. If it does so, then the first line of the message Body will contain a decorative copy of the confidential Subject Header Field. The issue tracking software decrypts the incoming control message, identifies that there is a Legacy Display Element in the part (see [Section 4.5.3.1](#)), strips the lines comprising the Legacy Display Element (including the first blank line), and only then parses the remaining top line to look for the expected special formatting.

4.9. Affordances for Debugging and Troubleshooting

Note that advanced users of an MUA may need access to the original message, for example, to troubleshoot problems with the rendering MUA itself or problems with the SMTP transport path taken by the message.

An MUA that applies these rendering guidelines **SHOULD** ensure that the full original source of the message as it was received remains available to such a user for debugging and troubleshooting.

If a troubleshooting scenario demands information about the cryptographically protected values of Header Fields, and the message is encrypted, the debugging interface **SHOULD** also provide a "source" view of the Cryptographic Payload itself, alongside the full original source of the message as received.

4.10. Handling RFC8551HP Messages (Backward Compatibility)

Section 1.1.1 describes some drawbacks to the Header Protection scheme defined in [RFC8551], referred to here as [RFC8551HP](#). An MUA **MUST NOT** generate an [RFC8551HP](#) message. However, for backward compatibility, an MUA **MAY** try to render or respond to such a message as though the message has standard Header Protection.

The following two sections contain guidance for identifying, rendering, and replying to [RFC8551HP](#) messages. Corresponding test vectors are provided in Appendices C.2.5, C.2.6, and C.3.17.

4.10.1. Identifying an RFC8551HP Message

An [RFC8551HP](#) message can be identified by its MIME structure, given that all of the following conditions are met:

- It has a well-formed Cryptographic Envelope consisting of at least one Cryptographic Layer as the outermost MIME object.
- The Cryptographic Payload is a single `message/rfc822` object.
- The message that constitutes the Cryptographic Payload does not itself have a well-formed Cryptographic Envelope; that is, its outermost MIME object is not a Cryptographic Layer.
- No `Content-Type` parameter of `hp=` is set on either the Cryptographic Payload or its immediate MIME child.

Here is the MIME structure of an example signed-and-encrypted [RFC8551HP](#) message:

```
A └─ application/pkcs7-mime; smime-type="enveloped-data"
   ↓ (decrypts to)
B └─ application/pkcs7-mime; smime-type="signed-data"
   ↓ (unwraps to)
C └─ message/rfc822 [Cryptographic Payload]
   └─ multipart/alternative [Rendered Body]
      └─ text/plain
      └─ text/html
```

This meets the definition of an [RFC8551HP](#) message because:

- Cryptographic Layers A and B form the Cryptographic Envelope.
- The Cryptographic Payload, rooted in part C, has `Content-Type: message/rfc822`.
- Part D (the MIME root of the message at C) is itself not a Cryptographic Layer.
- Neither part C nor part D have any `hp` parameters set on their `Content-Type`.

4.10.2. Rendering or Responding to an RFC8551HP Message

When an MUA has precisely identified a message as an [RFC8551HP](#) message, the MUA **MAY** render or respond to that message as though it were a message with Header Protection as defined in this document by making the following adjustments:

- Rather than rendering the message Body as the Cryptographic Payload itself (part C in the example above), render the [RFC8551HP](#) message's Body as the MIME subtree that is the Cryptographic Payload's immediate child (part D).
- Make a comparable modification to [HeaderSetsFromMessage](#) (Section 4.2.1) and [HeaderFieldProtection](#) (Section 4.3.1): Both algorithms currently look for the protected Header Fields on the Cryptographic Payload (part C), but they should instead look at the Cryptographic Payload's immediate child (part D).
- If the Cryptographic Envelope is signed-only, behave as though there is an `hp="clear"` parameter for the Cryptographic Payload; if the Envelope contains encryption, behave as though there is an `hp="cipher"` parameter. That is, infer the sender's cryptographic intent from the structure of the message.
- If the Cryptographic Envelope contains encryption, further modify [HeaderSetsFromMessage](#) to derive `refouter` from the actual outer message Header Fields (those found in part A in the example above) rather than looking for `HP-Outer` Header Fields with the other protected Header Fields. That is, infer Header Field confidentiality based on the unprotected Header Fields.

The inferences in the above modifications are not based on any strong end-to-end guarantees. An intervening MTA may tamper with the message's Outer Header Section or wrap the message in an encryption layer to undetectably change the recipient's understanding of the confidentiality of the message's Header Fields or the message Body itself.

4.11. Rendering Other Schemes

Other MUAs may have generated different structures of messages that aim to offer end-to-end cryptographic protections that include Header Protection. This document is not normative for those schemes, and it is **NOT RECOMMENDED** to generate these other schemes, as they can either have structural flaws or simply render poorly on Legacy MUAs. A conformant MUA **MAY** attempt to infer Header Protection when rendering an existing message that appears to use some other scheme not documented here. Pointers to some known other schemes can be found in [Appendix F](#).

5. Sending Guidance

This section describes the process an MUA should use to apply cryptographic protection to an email message with Header Protection.

When composing a message with end-to-end cryptographic protections, an MUA **SHOULD** apply Header Protection.

When generating such a message, an MUA **MUST** add the `hp` parameter (see [Section 2.1.1](#)) only to the Content-Type Header Field at the root of the message's Cryptographic Payload. The value of the parameter **MUST** indicate whether the Cryptographic Envelope contains a layer that provides encryption.

5.1. Composing a Cryptographically Protected Message Without Header Protection

For contrast, we first consider the typical message composition process of a Legacy Crypto MUA, which does not provide any Header Protection.

This process is described in [Section 5.1](#) of [RFC9787]. We replicate it here for reference. The inputs to the algorithm are:

- `origbody`: The traditional unprotected message Body as a well-formed MIME tree (possibly just a single MIME leaf part). As a well-formed MIME tree, `origbody` already has Structural Header Fields (Content-*) present.
- `origheaders`: The intended Non-Structural Header Fields for the message, represented here as a list of `(h, v)` pairs, where `h` is a Header Field name and `v` is the associated value. Note that these are Header Fields that the MUA intends to be visible to the recipient of the message. In particular, if the MUA uses the Bcc Header Field during composition but plans to omit it from the message (see [Section 3.6.3](#) of [RFC5322]), it will not be in `origheaders`.
- `crypto`: The series of cryptographic protections to apply (for example, "sign with the secret key corresponding to X.509 certificate X, then encrypt to X.509 certificates X and Y"). This is a routine that accepts a MIME tree as input (the Cryptographic Payload), wraps the input in the appropriate Cryptographic Envelope, and returns the resultant MIME tree as output.

The algorithm returns a MIME object that is ready to be injected into the mail system.

5.1.1. ComposeNoHeaderProtection

Method signature:

```
ComposeNoHeaderProtection(origbody, origheaders, crypto) -> mime_message
```

Procedure:

1. Apply `crypto` to MIME part `origbody`, producing MIME tree output.
2. For each Header Field name and value `(h, v)` in `origheaders`:
 - i. Add Header Field `h` to output with value `v`.
3. Return output.

5.2. Composing a Message with Header Protection

To compose a message using Header Protection, the composing MUA uses the following inputs:

- all the inputs described in [Section 5.1](#)

- hcp: a [Header Confidentiality Policy](#), as defined in [Section 3](#)
- respond: if the new message is a response to another message (e.g., "Reply", "Reply All", "Forward", etc.), the MUA function corresponding to the user's action (see [Section 6.1](#)), otherwise null
- refmsg: if the new message is a response to another message, the message being responded to, otherwise null
- legacy: a boolean value, indicating whether any recipient of the message is believed to have a Legacy MUA. If all recipients are known to implement this document, legacy should be set to false. (How an MUA determines the value of legacy is out of scope for this document; an initial implementation can simply set it to true.)

To enable visibility of User-Facing but now removed/obscured Header Fields for decryption-capable Legacy MUAs, the Header Fields are included as a decorative Legacy Display Element in specially marked parts of the message (see [Section 2.1.2](#)). This document recommends two mechanisms for such a decorative adjustment: one for a text/html Main Body Part of the email message and one for a text/plain Main Body Part. This document does not recommend adding a Legacy Display Element to any other part.

Please see [Section 7.1](#) of [\[RFC9787\]](#) for guidance on identifying the parts of a message that are a Main Body Part.

5.2.1. Compose

Method signature:

```
Compose(origbody, origheaders, crypto, hcp, respond, refmsg, legacy) ->  
mime_message
```

Procedure:

1. Let newbody be a copy of origbody.
2. If crypto contains encryption and legacy is true:
 - i. Create ldlist, an empty list of (header, value) pairs.
 - ii. For each Header Field name and value (h,v) in origheaders:
 - a. If h is User-Facing (see [Section 1.1.2](#) of [\[RFC9787\]](#)):
 - I. If hcp(h,v) is not v:
 - A. Add (h,v) to ldlist.
 - iii. If ldlist is not empty:
 - a. Identify each leaf MIME part of newbody that represents the "main Body" of the message.
 - b. For each "Main Body Part" bodypart of type text/plain or text/html:
 - I. Adjust bodypart by inserting a Legacy Display Element Header Field list ldlist into its content and adding a Content-Type parameter hp-legacy-display with value 1 (see [Section 5.2.2](#) for text/plain and [Section 5.2.3](#) for text/html).

3. For each Header Field name and value (h, v) in `origheaders`:
 - i. Add Header Field h to MIME part `newbody` with value v .
4. If `crypto` does not contain encryption:
 - i. Set the `hp` parameter on the Content-Type of MIME part `newbody` to `clear`.
 - ii. Let `newheaders` be a copy of `origheaders`.
5. Else (if `crypto` contains encryption):
 - i. Set the `hp` parameter on the Content-Type of MIME part `newbody` to `cipher`.
 - ii. If `refmsg` is not null, `respond` is not null, and `refmsg` itself is encrypted with Header Protection:
 - a. Let `response_hcp` be a single-use [HCP](#) derived from `respond` and `refmsg` (see [Section 6.1](#)).
 - iii. Else (if this is not a response to an encrypted, header-protected message):
 - a. Set `response_hcp` to `hcp_no_confidentiality`.
 - iv. Create a new empty list of Header Field names and values `newheaders`.
 - v. For each Header Field name and value (h, v) in `origheaders`:
 - a. Let `newval` be `hcp(h, v)`.
 - b. If `newval` is `v`:
 - I. Let `newval` be `response_hcp(h, v)`.
 - c. If `newval` is not null:
 - I. Add ($h, newval$) to `newheaders`.
 - vi. For each Header Field name and value (h, v) in `newheaders`:
 - a. Let string `record` be the concatenation of h , a literal `:` (ASCII colon (0x3A)) followed by ASCII space (0x20), and v .
 - b. Add Header Field "HP-Outer" to MIME part `newbody` with value `record`.
6. Apply `crypto` to MIME part `newbody`, producing MIME tree output.
7. For each Header Field name and value (h, v) in `newheaders`:
 - i. Add Header Field h to output with value v .
8. Return output.

Note that both new parameters (`hcp` and `legacy`) are effectively ignored if `crypto` does not contain encryption. This is by design, because they are irrelevant for signed-only cryptographic protections.

5.2.2. Adding a Legacy Display Element to a text/plain Part

For a list of obscured and removed User-Facing Header Fields represented as (header, value) pairs, concatenate them as a set of lines, with one newline at the end of each pair. Add an additional trailing newline after the resultant text, and prepend the entire list to the Body of the text/plain part.

The MUA **MUST** also add a Content-Type parameter of hp-legacy-display with value 1 to the MIME part to indicate that a Legacy Display Element was added.

For example, if the list of obscured Header Fields was [("Cc", "alice@example.net"), ("Subject", "Thursday's meeting")], then a text/plain Main Body Part that originally looked like this:

```
Content-Type: text/plain; charset=UTF-8

I think we should skip the meeting.
```

would become:

```
Content-Type: text/plain; charset=UTF-8; hp-legacy-display=1

Subject: Thursday's meeting
Cc: alice@example.net

I think we should skip the meeting.
```

Note that the Legacy Display Element (the lines beginning with Subject: and Cc:) is part of the Body of the MIME part in question.

This example assumes that the Main Body Part in question is not the root of the Cryptographic Payload. For instance, it could be a leaf of a multipart/alternative Cryptographic Payload. This is why no additional Header Fields have been injected into the MIME part in this example.

5.2.3. Adding a Legacy Display Element to a text/html Part

Adding a Legacy Display Element to a text/html part is similar to how it is added to a text/plain part (see [Section 5.2.2](#)). Instead of adding the obscured or removed User-Facing Header Fields to a block of text delimited by a blank line, the composing MUA injects them in an HTML <div> element annotated with a class attribute of header-protection-legacy-display.

The content and formatting of this decorative <div> have no strict requirements, but they **MUST** represent all the obscured and removed User-Facing Header Fields in a readable fashion. A simple approach is to assemble the text in the same way as [Section 5.2.2](#), wrap it in a verbatim <pre> element, and put that element in the annotated <div>.

The annotated `<div>` should be placed as close to the start of the `<body>` as possible, where it will be visible when viewed with a standard HTML renderer.

The MUA **MUST** also add a Content-Type parameter of `hp-legacy-display` with value 1 to the MIME part to indicate that a Legacy Display Element was added.

For example, if the list of obscured Header Fields was `[ ("Cc", "alice@example.net"), ("Subject", "Thursday's meeting") ]`, then a `text/html` Main Body Part that originally looked like this:

```
Content-Type: text/html; charset=UTF-8

<html><head><title></title></head><body>
<p>I think we should skip the meeting.</p>
</body></html>
```

would become:

```
Content-Type: text/html; charset=UTF-8; hp-legacy-display=1

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>Subject: Thursday's meeting
Cc: alice@example.net</pre></div>
<p>I think we should skip the meeting.</p>
</body></html>
```

This example assumes that the Main Body Part in question is not the root of the Cryptographic Payload. For instance, it could be a leaf of a `multipart/alternative` Cryptographic Payload. This is why no additional Header Fields have been injected into the MIME part in this example.

5.2.3.1. Step-by-Step Example for Inserting a Legacy Display Element into `text/html`

A composing MUA **MAY** insert the Legacy Display Element anywhere reasonable within the message as long as it prioritizes visibility for the reader using a Legacy MUA that is capable of decryption. This decision may take into account special message-specific HTML formatting expectations if the MUA is aware of them. However, some MUAs may not have any special insight into the user's preferred HTML formatting and still want to insert a Legacy Display Element. This section offers a non-normative, simple, and minimal step-by-step approach for a composing MUA that has no other information or preferences to fall back on.

The process below assumes that the MUA already has the full HTML object that it intends to send, including all of the text supplied by the user.

1. Assemble the text exactly as specified for `text/plain` (see [Section 5.2.2](#)).
2. Wrap that text in a verbatim `<pre>` element.
3. Wrap that `<pre>` element in a `<div>` element annotated with the class `header-protection-legacy-display`.

4. Find the `<body>` element of the full HTML object.
5. Insert the `<div>` element as the first child of the `<body>` element.

5.2.4. Only Add a Legacy Display Element to Main Body Parts

Some messages may contain a `text/plain` or `text/html` subpart that is *not* a Main Body Part. For example, an email message might contain an attached text file or a downloaded web page. Attached documents need to be preserved as intended in the transmission, without modification.

The composing MUA **MUST NOT** add a Legacy Display Element to any part of the message that is not a Main Body Part. In particular, if a part is annotated with `Content-Disposition: attachment`, or if it does not descend via the first child of any of its `multipart/mixed` or `multipart/related` ancestors, it is not a Main Body Part and **MUST NOT** be modified.

See [Section 7.1](#) of [RFC9787] for more guidance about common ways to distinguish Main Body Parts from other MIME parts in a message.

5.2.5. Do Not Add a Legacy Display Element to Other Content-Types

The purpose of injecting a Legacy Display Element into each Main Body Part is to enable rendering of otherwise obscured Header Fields in Legacy MUAs that are capable of message decryption but don't know how to follow the rest of the guidance in this document.

The authors are unaware of any Legacy MUA that would render any MIME part type other than `text/plain` and `text/html` as the Main Body. A generating MUA **SHOULD NOT** add a Legacy Display Element to any MIME part with any other Content-Type.

6. Replying and Forwarding Guidance

An MUA might create a new message in response to another message, thus acting both as a receiving MUA and as a sending MUA. For example, the user of an MUA viewing any given message might take an action like "Reply", "Reply All", "Forward", or some comparable action to start the composition of a new message. The new message created this way effectively references the original message that was viewed at the time.

For encrypted messages, special guidance applies, because information can leak in at least two ways: leaking previously confidential Header Fields and leaking the entire message by sending the reply or forward to the wrong party.

6.1. Avoid Leaking Encrypted Header Fields in Replies and Forwards

As noted in [Section 5.4](#) of [RFC9787], an MUA in this position **MUST NOT** leak previously encrypted content in the clear in a follow-up message. The same is true for protected Header Fields.

Values from any Header Field that was identified as either encrypted-only or signed-and-encrypted based on the steps outlined above **MUST NOT** be placed in cleartext output when generating a message.

In particular, if Subject was encrypted, and it is copied into the draft encrypted reply, the replying MUA **MUST** obscure the unprotected (cleartext) Subject Header Field.

When crafting the Header Fields for a reply or forwarded message, the composing MUA **SHOULD** make use of the HP-Outer Header Fields from within the Cryptographic Envelope of the reference message to ensure that Header Fields derived from the reference message do not leak in the reply.

On a high level, this can be achieved as follows: Consider a Header Field in a reply message that is generated by derivation from a Header Field in the reference message. For example, the To Header Field is typically derived from the reference message's Reply-To or From Header Fields. When generating the outer copy of the Header Field, the composing MUA first applies its own [Header Confidentiality Policy](#). If the Header Field's value is changed by the HCP, then it is applied to the Outer Header Section. If the Header Field's value is unchanged, the composing MUA re-generates the Header Field using the Header Fields that had been on the outside of the original message at sending time. These can be inferred from the HP-Outer Header Fields located within the Cryptographic Payload of the referenced message. If that value is itself different than the protected value, then it is applied to the Outer Header Section. If the value is the same as the protected value, then it is simply copied to the Outer Header Section directly. Whether it was changed or not, it is noted in the protected Header Section using HP-Outer, as described in [Section 2.2.1](#).

See [Appendix D.2](#) for a simple worked example of this process.

Below we describe a supporting algorithm to handle this. It produces a list of Header Fields that should be obscured or removed in the new message even if the sender's choice of [Header Confidentiality Policy](#) wouldn't normally remove or obscure the Header Field in question. This is effectively a single-use HCP. The normal sending guidance in [Section 5.2](#) applies this single-use HCP to implement the high-level guidance above.

6.1.1. ReferenceHCP

The algorithm takes two inputs:

- A single referenced message `refmsg`
- A built-in MUA `respond` function associated with the user's action. The `respond` function takes a list of Header Fields from a referenced message as input and generates a list of initial candidate message Header Field names and values that are used to populate the message composition interface. Something like this function already exists in most MUAs, though it may differ across responsive actions. For example, the `respond` function that implements "Reply All" is likely to be a different from the `respond` that implements "Reply".

As an output, it produces an ephemeral single-use [Header Confidentiality Policy](#), specific to this kind of response to this specific message.

Method signature:

```
ReferenceHCP(refmsg, respond) -> ephemeral_hcp
```

Procedure:

1. If `refmsg` is not encrypted with Header Protection:
 - i. Return `hcp_no_confidentiality` (there is no header confidentiality in the reference message that needs protection).
2. Extract `refouter`, `refprotected` from `refmsg` as described in [Section 4.2](#).
3. Let `genprotected` be a list of `(h, v)` pairs generated by `respond(refprotected)`.
4. Let `genouter` be a list of `(h, v)` pairs generated by `respond(refouter)`.
5. For each `(h, v)` in `genprotected`:
 - i. If `(h, v)` is in `genouter`:
 - a. Remove `(h, v)` from both `genprotected` and `genouter` (this Header Field does not need additional confidentiality).
6. Let `confmap` be a mapping from a Header Field name and value `(h, v)` to either a string or the special value `null` (this mapping is initially empty).
7. For each `(h, v)` remaining in `genprotected`:
 - i. Set `result` to the special value `null`.
 - ii. For each `(h1, v1)` in `genouter`:
 - a. If `h1` is `h`:
 - I. Set `result` to `v1`.
 - iii. Insert `(h, v) -> result` into `confmap`.
8. Return a new [HCP](#) from `confmap` that tests whether `(name, val_in)` is in `confmap`; if so, return `confmap[(name, val_in)]`; otherwise, return `val_in`.

Note that the key idea here is to reuse the MUA's existing `respond` function. The algorithm simulates how the MUA would pre-populate a reply to two traditional messages whose Header Fields have the values `refouter` and `refprotected`, respectively (independent of any cryptographic protections). Then, it uses the difference to derive a one-time [HCP](#). This [HCP](#) takes into account both the referenced message's sender's preferences and the derivations that can happen to Header Field values when responding. Note that while some of these derivations are straightforward (e.g., `In-Reply-To` is usually derived from `Message-ID`), others are non-trivial. For example, the `From` address may be derived from `To`, `Cc`, or the MUA's local address preference (especially when the MUA received the referenced message via `Bcc`). Similarly, `To` may be derived from `To`, `From`, and/or `Cc` Header Fields depending on the MUA implementation and depending on whether the user clicked "Reply", "Reply All", "Forward", or any other action that generates a response to a message. Reusing the MUA's existing `respond` function incorporates these nuances without requiring any extra configuration choices or additional maintenance burden.

6.2. Avoid Misdirected Replies

When replying to a message, the composing MUA typically decides who to send the reply to based on:

- the Reply-To, Mail-Followup-To, or From Header Fields
- optionally, the other To or Cc Header Fields (if the user chose to "Reply All")

When a message has Header Protection, the replying MUA **MUST** populate the destination fields of the draft message using the protected Header Fields and ignore any unprotected Header Fields.

This mitigates against an attack where Mallory gets a copy of an encrypted message from Alice to Bob and then relays the message to Bob with an additional Cc to Mallory's own email address in the message's outer (unprotected) Header Section.

If Bob knows Mallory's certificate already, and he replies to such a message without following the guidance in this section, it's likely that his MUA will encrypt the cleartext of the message directly to Mallory.

7. Unprotected Header Fields Added in Transit

Some Header Fields are legitimately added in transit and could not have been known to the sender at message composition time.

The most common of these Header Fields are Received and DKIM-Signature, neither of which are typically rendered, either explicitly or implicitly.

If a receiving MUA has specific knowledge about a given Header Field, including that:

- the Header Field would not have been known to the original sender and
- the Header Field might be rendered explicitly or implicitly,

then the MUA **MAY** decide to operate on the value of that Header Field from the unprotected Header Section, even though the message has Header Protection.

The MUA **MAY** prefer to verify that the Header Fields in question have additional transit-derived cryptographic protections before rendering or acting on them. For example, the MUA could verify whether these Header Fields are covered by an appropriate and valid ARC-Authentication-Results (see [RFC8617]) or DKIM-Signature (see [RFC6376]) Header Field.

Specific examples of Header Fields that are meaningful to the user are commonly added by the transport agents that appear below.

7.1. Mailing List Header Fields: List-* and Archived-At

If the message arrives through a mailing list, the list manager itself may inject Header Fields (most have a List- prefix) in the message:

- List-Archive
- List-Subscribe
- List-Unsubscribe
- List-Id
- List-Help
- List-Post
- Archived-At

For some MUAs, these Header Fields are implicitly rendered by providing buttons for actions like "Subscribe", "View Archived Version", "Reply List", "List Info", etc.

An MUA that receives a message with Header Protection that contains these Header Fields in the unprotected Header Section and that has reason to believe the message is coming through a mailing list **MAY** decide to render them to the user (explicitly or implicitly) even though they are not protected.

8. Email Ecosystem Evolution

The email ecosystem is the set of client-side and server-side software and policies that are used in the creation, transmission, storage, rendering, and indexing of email over the Internet.

This document is intended to offer tooling needed to improve the state of the email ecosystem in a way that can be deployed without significant disruption. Some elements of this specification are present for transitional purposes but would not exist if the system were designed from scratch.

This section describes these transitional mechanisms, as well as some suggestions for how they might eventually be phased out.

8.1. Dropping Legacy Display Elements

Any decorative Legacy Display Element added to an encrypted message that uses Header Protection is present strictly for enabling Header Field visibility (most importantly, the Subject Header Field) when the message is viewed with a decryption-capable Legacy MUA.

Eventually, the hope is that most decryption-capable MUAs will conform to this specification and there will be no need for injection of Legacy Display Elements in the message Body. A survey of widely used decryption-capable MUAs might be able to establish when most of them do support this specification.

At that point, a composing MUA could set the legacy parameter defined in [Section 5.2](#) to false by default or could even hard-code it to false, yielding a much simpler message construction set.

Until that point, an end user might want to signal that their receiving MUAs are conformant to this document so that a peer composing a message to them can set legacy to false. A signal indicating capability of handling messages with Header Protection might be placed in the user's cryptographic certificate or in outbound messages.

This document does not attempt to define the syntax or semantics of such a signal.

8.2. More Ambitious Default Header Confidentiality Policy

This document defines a few different forms of [Header Confidentiality Policy](#). An MUA implementing an [HCP](#) for the first time **SHOULD** deploy `hcp_baseline` as recommended in [Section 3.3](#). This [HCP](#) offers the most commonly expected protection (obscuring the Subject Header Field) without risking deliverability or rendering issues.

The HCPs proposed in this document are relatively conservative and still leak a significant amount of metadata for encrypted messages. This is largely done to ensure deliverability (see [Section 1.3.2](#)) and usability, as messages without some critical Header Fields are more likely to not reach their intended recipient.

In the future, some mail transport systems may accept and deliver messages with even less publicly visible metadata. Many MTA operators today would ask for additional guarantees about such a message to limit the risks associated with abusive or spam mail.

This specification offers the [HCP](#) formalism itself as a way for MUA developers and MTA operators to describe their expectations around message deliverability. MUA developers can propose a more ambitious default [HCP](#) and ask MTA operators (or simply test) whether their MTAs would be likely to deliver or reject encrypted mail with that [HCP](#) applied. Proponents of a more ambitious [HCP](#) should explicitly document the [HCP](#) and name it clearly and unambiguously to facilitate this kind of interoperability discussion.

Reaching widespread consensus around a more ambitious global default [HCP](#) is a challenging problem of coordinating many different actors. A piecemeal approach might be more feasible, where some signaling mechanism allows a message recipient, MTA operator, or third-party clearinghouse to announce what kinds of HCPs are likely to be deliverable for a given recipient. In such a situation, the default [HCP](#) for an MUA might involve consulting the signaled acceptable HCPs for all recipients and combining them (along with a default for when no signal is present) in some way.

If such a signal were to reach widespread use, it could also be used to guide reasonable statistical default [HCP](#) choices for recipients with no signal.

This document does not attempt to define the syntax or semantics of such a signal.

8.3. Deprecation of Messages Without Header Protection

At some point, when the majority of MUA clients can generate cryptographically protected messages with Header Protection, it should be possible to deprecate any cryptographically protected message that does not have Header Protection.

For example, as noted in [Section 9.1](#), it's possible for an MUA to render a signed-only message that has no Header Protection the same as an unprotected message. And a signed-and-encrypted message without Header Protection could likewise be marked as not fully protected.

These stricter rules could be adopted immediately for all messages. Or an MUA developer could roll them out immediately for any new message but still treat an old message (based on the Date Header Field and cryptographic signature timestamp) more leniently.

A decision like this by any popular receiving MUA could drive adoption of this standard for sending MUAs.

9. Usability Considerations

This section describes concerns for MUAs that are interested in easy adoption of Header Protection by normal users.

While they are not protocol-level artifacts, these concerns motivate the protocol features described in this document.

See also the usability commentary in [Section 2](#) of [\[RFC9787\]](#).

9.1. Mixed Protections Within a Message Are Hard to Understand

When rendering a message to the user, the ideal circumstance is to present a single cryptographic status for any given message. However, when message Header Fields are present, some message Header Fields do not have the same cryptographic protections as the main message.

Representing such a mixed set of protection statuses is very difficult to do in a way that an Ordinary User can understand. There are at least three scenarios that are likely to be common and poorly understood:

- A signed message with no Header Protection.
- A signed-and-encrypted message with no Header Protection.
- A signed-and-encrypted message with Header Protection as defined in this document, where some User-Facing Header Fields have confidentiality but some do not.

An MUA should have a reasonable strategy for clearly communicating each of these scenarios to the user. For example, an MUA operating in an environment where it expects most cryptographically protected messages to have Header Protection could use the following rendering strategy:

- When rendering a message with a signed-only cryptographic status but no Header Protection, an MUA may decline to indicate a positive security status overall and only indicate the cryptographic status to a user in a message properties or diagnostic view. That is, the message may appear identical to an unsigned message except if a user verifies the properties through a menu option.
- When rendering a message with a signed-and-encrypted or encrypted-only cryptographic status but no Header Protection, overlay a warning flag on the typical cryptographic status indicator. That is, if a typical signed-and-encrypted message displays a lock icon, display a lock icon with a warning sign (e.g., an exclamation point in a triangle) overlaid. For example, see the graphics in [\[chrome-indicators\]](#).
- When rendering a message with a signed-and-encrypted or encrypted-only cryptographic status with Header Protection but where the Subject Header Field has not been removed or obscured, place a warning sign on the Subject line.

Other simple rendering strategies could also be reasonable.

9.2. Users Should Not Have to Choose a Header Confidentiality Policy

This document defines the abstraction of a [Header Confidentiality Policy](#) object for the sake of communication between implementers and deployments.

Most email users are unlikely to understand the trade-offs between different policies. In particular, the potential negative side effects (e.g., poor deliverability) may not be easily attributable by a normal user to a particular [HCP](#).

Therefore, MUA implementers should be conservative in their choice of default [HCP](#) and should not require the Ordinary User to make an incomprehensible choice that could cause unfixable, undiagnosable problems. The safest option is for the MUA developer to select a known, stable [HCP](#) (this document recommends `hcp_baseline` in [Section 3.3](#)) on the user's behalf. An MUA should not expose the Ordinary User to a configuration option where they are expected to manually select (let alone define) an [HCP](#).

10. Security Considerations

Header Protection improves the security of cryptographically protected email messages. Following the guidance in this document improves security for users by more directly aligning the underlying messages with user expectations about confidentiality, authenticity, and integrity.

Nevertheless, helping the user distinguish between cryptographic protections of various messages remains a security challenge for MUAs. This is exacerbated by the fact that many existing messages with cryptographic protections do not employ Header Protection. MUAs encountering these messages (e.g., in an archive) will need to handle older forms (without Header Protection) for quite some time, possibly forever.

The security considerations from [Section 6](#) of [\[RFC8551\]](#) continue to apply for any MUA that offers S/MIME cryptographic protections, as well as [Section 3](#) of [\[RFC5083\]](#) (Authenticated-Enveloped-Data in Cryptographic Message Syntax (CMS)) and [Section 14](#) of [\[RFC5652\]](#) (CMS more broadly). Likewise, the security considerations from [Section 8](#) of [\[RFC3156\]](#) continue to apply for any MUA that offers PGP/MIME cryptographic protections, as well as [Section 13](#) of [\[RFC9580\]](#) (OpenPGP itself). In addition, these underlying security considerations are now also applicable to the contents of the message Header Section, not just the message Body.

10.1. From Address Spoofing

If the From Header Field was treated like any other protected Header Field by the receiving MUA, this scheme would enable sender address spoofing.

To prevent sender spoofing, many receiving MUAs implicitly rely on their receiving MTA to inspect the unprotected Header Section and verify that the From Header Field is authentic. If a receiving MUA displays a From address that doesn't match the From address that the receiving and/or sending MTAs filtered on, the MUA may be vulnerable to spoofing.

Consider a malicious MUA that sets the following Header Fields on an encrypted message with Header Protection:

- Outer: From: <alice@example.com>
- Inner: HP-Outer: From: <alice@example.com>
- Inner: From: <bob@example.org>

During sending, the MTA of example.com validates that the sending MUA is authorized to send from alice@example.com. Since the message is encrypted, the sending and receiving MTAs cannot see the protected Header Fields. A naive receiving MUA might follow the algorithms in this document without special consideration for the From Header Field. Such an MUA might display the email as coming from bob@example.org to the user, resulting in a spoofed address.

This problem applies both between domains and within a domain.

This problem always applies to signed-and-encrypted messages. This problem also applies to signed-only messages because MTAs typically do not look at the protected Header Fields when confirming From address authenticity.

Sender address spoofing is relevant for two distinct security properties:

- Sender authenticity: relevant for rendering the message (which address to show the user?)
- Message confidentiality: relevant when replying to a message (a reply to the wrong address can leak the message contents)

10.1.1. From Rendering Reasoning

Section 4.4.3 provides guidance for rendering the From Header Field. It recommends a receiving MUA that depends on its MTA to authenticate the unprotected (outer) From Header Field to render the outer From Header Field if both of the following conditions are met:

- From Header Field Mismatch (as defined in Section 4.4.1.1) and
- No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

Note: The second condition effectively means that the inner (expected to be protected) From Header Field appears to have insufficient protection.

This may seem surprising since it causes the MUA to render a mix of both protected and unprotected values. This section provides an argument as to why this guidance makes sense.

We proceed by case distinction:

- Case 1: Malicious sending MUA.
 - Attack situation: The sending MUA puts a different inner From Header Field to spoof the sender address.
 - In this case, it is "better" to fall back and render the outer From Header Field because this is what the receiving MTA can validate. Otherwise, this document would introduce a new way for senders to spoof the From address of the message.
 - This does not preclude a future document from updating this document to specify a protocol for legitimate sender address hiding.
- Case 2: Malicious sending/transiting/receiving MTA (or anyone meddling between MTAs).
 - Attack situation: An on-path attacker changes the outer From Header Field (possibly with other meddling to break the signature; see below). Their goal is to get the receiving MUA to show a different From address than the sending MUA intended (breaking MUA-to-MUA sender authenticity).
 - Case 2.a: The sending MUA submitted an unsigned or encrypted-only message to the email system. In this case, there can be no sender authenticity anyway.
 - Case 2.b: The sending MUA submitted a signed-only message to the email system.
 - Case 2.b.i: The attacker removes or breaks the signature. In this case, the attacker can also modify the inner From Header Field to their liking.
 - Case 2.b.ii: The signature is valid, but the receiving MUA does not see any valid binding between the signing certificate and the addr-spec of the inner From Header Field. In this case, there can be no sender authenticity anyways (the certificate could have been generated by the on-path attacker). This case is indistinguishable from a malicious sending MUA; hence, it is "better" to fall back to the outer From Header Field that the MTA can validate. Note that once the binding is validated (e.g., after an out-of-band comparison), the rendering may change from showing the outer From address (and a

warning) to showing the inner, now validated From address. In some cases, the binding may be instantly validated even for previously unseen certificates (e.g., if the certificate is issued by a trusted certification authority).

- Case 2.c: The sending MUA submitted a signed-and-encrypted message to the email system.
 - Case 2.c.i: The attacker removes or breaks the signature. Note that the signature is inside the ciphertext (see [Section 5.2](#) of [RFC9787]). Thus, assuming the encryption is non-malleable, any on-path attacker cannot break the signature while ensuring that the message still decrypts successfully.
 - Case 2.c.ii: The signature is valid, but the receiving MUA does not see any valid binding between the signing certificate and the addr-spec of the inner From Header Field. See case 2.b.ii.

As the case distinction shows, the outer From Header Field is either the preferred fallback (in particular, to avoid introducing a new spoofing channel) or just as good (because just as modifiable) as the inner From Header Field.

Rendering the outer From Header Field does carry the risk of a "temporary downgrade attack" in cases 2.b.ii and 2.c.ii, where a malicious MTA keeps the signature intact but modifies the outer From Header Field. The MUA can resolve this temporary downgrade by validating the certificate-to-addr-spec binding. If the MUA never does this validation, the entire message could be fake.

If there were a signaling channel where the MTA can tell the MUA whether it authenticated the From Header Field, an MUA could use this in its rendering decision. In the absence of such a signal, and when end-to-end authenticity is unavailable, this document prefers to fall back to the outer From Header Field. This default is based on the assumption that most MTAs apply some filtering based on the outer From Header Field (whether the MTA can authenticate it or not). Rendering the unprotected outer From Header Field (instead of the protected inner one) in case of a mismatch retains this ability for MTAs.

If the MUA decides not to rely on the MTA to authenticate the outer From Header Field, it may prefer the inner From Header Field.

10.2. Avoid Cryptographic Summary Confusion from the hp Parameter

When parsing a message, the recipient MUA infers the message's Cryptographic Status from the Cryptographic Layers, as described in [Section 4.6](#) of [RFC9787].

The Cryptographic Layers that make up the Cryptographic Envelope describe an ordered list of cryptographic properties as present in the message after it has been delivered. By contrast, the hp parameter to the Content-Type Header Field contains a simpler indication: whether the sender originally tried to encrypt the message or not. In particular, for a message with Header Protection, the Cryptographic Payload should have a hp parameter of cipher if the message is encrypted (in addition to signed) and clear if no encryption is present (that is, the message is signed-only).

As noted in [Section 2.1.1](#), the receiving implementation should not inflate its estimation of the confidentiality of the message or its Header Fields based on the sender's intent if it can see that the message was not actually encrypted. A signed-only message that happens to have an `hp` parameter of `cipher` is still signed-only.

Conversely, since the encrypting Cryptographic Layer is typically outside the signature layer (see [Section 5.2](#) of [RFC9787]), an originally signed-only message could have been wrapped in an encryption layer by an intervening party before receipt to appear encrypted.

If a message appears to be wrapped in an encryption layer, and the `hp` parameter is present but is not set to `cipher`, then it is likely that the encryption layer was not added by the original sender. For such a message, the lack of any HP-Outer Header Field in the Header Section of the Cryptographic Payload **MUST NOT** be used to infer that all Header Fields were removed from the message by the original sender. In such a case, the receiving MUA **SHOULD** treat every Header Field as though it was not confidential.

10.3. Caution About Composing with Legacy Display Elements

When composing a message, it's possible for a Legacy Display Element to contain risky data that could trigger errors in a rendering client.

For example, if the value for a Header Field to be included in a Legacy Display Element within a given Body part contains folding whitespace, it should be "unfolded" before generating the Legacy Display Element: All contiguous folding whitespace should be replaced with a single space character. Likewise, if the Header Field value was originally encoded per [RFC2047], it should be decoded first to a standard string and re-encoded using the charset appropriate to the target part.

When including a Legacy Display Element in a `text/plain` part (see [Section 5.2.2](#)), if the decoded Subject Header Field contains a pair of newlines (e.g., if it is broken across multiple lines by encoded newlines), any newline **MUST** be stripped from the Legacy Display Element. If the pair of newlines is not stripped, a receiving MUA that follows the guidance in [Section 4.5.3.2](#) might leave the later part of the Legacy Display Element in the rendered message.

When including a Legacy Display Element in a `text/html` part (see [Section 5.2.3](#)), any material in the Header Field values should be explicitly HTML escaped to avoid being rendered as part of the HTML. At a minimum, the characters `<`, `>`, and `&` should be escaped to `<`, `>`, and `&`, respectively (for example, see [HTML-ESCAPES]). If unescaped characters from removed or obscured Header Field values end up in the Legacy Display Element, a receiving MUA that follows the guidance in [Section 4.5.3.3](#) might fail to identify the boundaries of the Legacy Display Element, cutting out more than it should or leaving remnants visible. And a Legacy MUA parsing such a message might misrender the entire HTML stream, depending on the content of the removed or obscured Header Field values.

The Legacy Display Element is a decorative addition solely to enable visibility of obscured or removed Header Fields in decryption-capable Legacy MUAs. When it is produced, it should be generated minimally and strictly, as described above, to avoid damaging the rest of the message.

10.4. Plaintext Attacks

An encrypted email message using S/MIME or PGP/MIME tends to have some amount of predictable plaintext. For example, the standard MIME Header Fields of the Cryptographic Payload of a message are often a predictable sequence of bytes, even without Header Protection, when they only include the Structural Header Fields `MIME-Version` and `Content-Type`. This is a potential risk for known-plaintext attacks.

Including protected Header Fields as defined in this document increases the amount of known plaintext. Since some of those Header Fields in a reply will be derived from the message being replied to, this also creates a potential risk for chosen-plaintext attacks, in addition to known-plaintext attacks.

Modern message encryption mechanisms are expected to be secure against both known-plaintext attacks and chosen-plaintext attacks. An MUA composing an encrypted message should ensure that it is using such a mechanism, regardless of whether it does Header Protection.

11. Privacy Considerations

11.1. Leaks When Replying

The encrypted Header Fields of a message may accidentally leak when replying to the message. See the guidance in [Section 6](#).

11.2. Encrypted Header Fields Are Not Always Private

For encrypted messages, depending on the sender's [HCP](#), some Header Fields may appear both within the Cryptographic Envelope and on the outside of the message (e.g., `Date` might exist identically in both places). [Section 4.3](#) identifies such a Header Field as signed-only. These Header Fields are clearly *not* private at all, despite a copy being inside the Cryptographic Envelope.

A Header Field whose name and value are not matched verbatim by any HP-Outer Header Field from the same part will have an encrypted-only or signed-and-encrypted status. But even Header Fields with these stronger levels of cryptographic confidentiality protection might not be as private as the user would like.

See the examples below.

This concern is true for any encrypted data, including the Body of the message, not just the Header Fields: If the sender isn't careful, the message contents or session keys can leak in many ways that are beyond the scope of this document. The message recipient has no way in principle to tell whether the apparent confidentiality of any given piece of encrypted content has been broken via channels that they cannot perceive. Additionally, an active intermediary aware of the recipient's public key can always encrypt a cleartext message in transit to give the recipient a false sense of security.

11.2.1. Encrypted Header Fields Can Leak Unwanted Information to the Recipient

For encrypted messages, even with an ambitious [HCP](#) that successfully obscures most Header Fields from all transport agents, Header Fields will be ultimately visible to all intended recipients. This can be especially problematic for Header Fields that are not User-Facing; the sender may not expect such Header Fields to be injected by their MUA. Consider the three following examples:

- The MUA may inject a User-Agent Header Field that describes itself to every recipient, even though the sender may not want the recipient to know the exact version of their OS, hardware platform, or MUA.
- The MUA may have an idiosyncratic way of generating a Message-ID Header Field, which could embed the choice of MUA, time zone, hostname, or other subtle information to a knowledgeable recipient.
- The MUA may erroneously include a Bcc Header Field in the `origheaders` of a copy of a message sent to the named recipient, defeating the purpose of using Bcc instead of Cc (see [Section 11.4](#) for more details about risks related to Bcc).

Clearly, no end-to-end cryptographic protection of any Header Field as defined in this document will hide such a sensitive field from the intended recipient. Instead, the composing MUA **MUST** populate the `origheaders` list for any outbound message with only information the recipient should have access to. This is true for messages without any cryptographic protection as well, of course, and it is even worse there: Such a leak is exposed to the transport agents as well as the recipient. An encrypted message with Header Protection and a more ambitious [Header Confidentiality Policy](#) avoids these leaks that expose information to the transport agents, but it cannot defend against such a leak to the recipient.

11.2.2. Encrypted Header Fields Can Be Inferred from External or Internal Metadata

For example, if the To and Cc Header Fields are removed from the unprotected Header Section, the values in those fields might still be inferred with high probability by an adversary who looks at the message either in transit or at rest. If the message is found in a mailbox, or being delivered to a mailbox, for example, `bob@example.org`, it's likely that Bob was in either To or Cc. Furthermore, encrypted message ciphertext may hint at the recipients: For S/MIME messages, the `RecipientInfo`, and for PGP/MIME messages, the key ID in the Public Key Encrypted Session Key (PKESK) packets will all hint at a specific set of recipients. Additionally, an MTA that handles the message may add a Received Header Field (or some other custom Header Field) that leaks some information about the nature of the delivery.

11.2.3. Encrypted Header Fields May Not Be Fully Masked by HCP

In another example, if the [HCP](#) modifies the Date Header Field to mask out high-resolution timestamps (e.g., rounding to the most recent hour), some information about the date of delivery will still be attached to the email. At the very least, the low-resolution, global version of the date will be present on the message. Additionally, Header Fields like Received that are added during

message delivery might include higher-resolution timestamps. And if the message lands in a mailbox that is ordered by time of receipt, even its placement in the mailbox and the unobscured Date Header Fields of the surrounding messages could leak this information.

Some Header Fields like From may be impossible to fully obscure, as many modern message delivery systems depend on at least domain information in the From Header Field for determining whether a message is coming from a domain with "good reputation" (that is, from a domain that is not known for leaking spam). So even if an ambitious HCP opts to remove the human-readable part from any From Header Field and to standardize/genericize the local part of the From address, the domain will still leak.

11.3. A Naive Recipient May Overestimate the Cryptographic Status of a Header Field in an Encrypted Message

When an encrypted (or signed-and-encrypted) message is in transit, an active intermediary can strip or tamper with any Header Field that appears outside the Cryptographic Envelope. A receiving MUA that naively infers cryptographic status from differences between the external Header Fields and those found in the Cryptographic Envelope could be tricked into overestimating the protections afforded to some Header Fields.

For example, if the original sender's HCP passes through the Cc Header Field unchanged, a cleanly delivered message would indicate that the Cc Header Field has a cryptographic status of signed. But if an intermediary attacker simply removes the Header Field from the unprotected Header Section before forwarding the message, then the naive recipient might believe that the field has a cryptographic status of signed-and-encrypted.

This document offers protection against such an attack by way of the HP-Outer Header Fields that can be found on the Cryptographic Payload. If a Header Field appears to have been obscured by inspection of the outer message but an HP-Outer Header Field matches it exactly, then the receiving MUA can indicate to the user that the Header Field in question may not have been confidential.

In such a case, a cautious MUA may render the Header Field in question as signed (because the sender did not hide it) but still treat it as signed-and-encrypted during reply to avoid accidental leakage of the cleartext value in the reply message, as described in [Section 6.1](#).

11.4. Privacy and Deliverability Risks with Bcc and Encrypted Messages

As noted in [Section 9.3](#) of [\[RFC9787\]](#), handling Bcc when generating an encrypted email message can be particularly tricky. With Header Protection, there is an additional wrinkle. When an encrypted email message with Header Protection has a Bcc'ed recipient, and the composing MUA explicitly includes the Bcc'ed recipient's address in their copy of the message (see the "second method" in [Section 3.6.3](#) of [\[RFC5322\]](#)), that Bcc Header Field will always be visible to the Bcc'ed recipient.

In this scenario, though, the composing MUA has one additional choice: whether or not to hide the Bcc Header Field from intervening message transport agents by returning null when the HCP is invoked for Bcc. If the composing MUA's rationale for including an explicit Bcc in the copy of the message sent to the Bcc recipient is to ensure deliverability via a message transport agent that inspects message Header Fields, then stripping the Bcc field during encryption may cause the intervening transport agent to drop the message entirely. This is why Bcc is not explicitly stripped in `hcp_baseline`.

On the other hand, if deliverability to a Bcc'ed recipient is not a concern, the most privacy-preserving option is to simply omit the Bcc Header Field from the protected Header Section in the first place. An MUA that is capable of receiving and processing such a message can infer that since their user's address was not mentioned in any To or Cc Header Field, they were likely a Bcc recipient.

Please also see [Section 9.3](#) of [\[RFC9787\]](#) for more discussion about Bcc and encrypted messages.

12. IANA Considerations

This document registers an email Header Field, describes parameters for the Content-Type Header Field, and establishes a registry for Header Confidentiality Policies to facilitate HCP evolution.

12.1. Registration of the HP-Outer Header Field

IANA has registered the following Header Field in the "Permanent Message Header Field Names" registry within the "Message Headers" registry group <<https://www.iana.org/assignments/message-headers>> in accordance with [\[RFC3864\]](#).

Header Field Name	Protocol	Status	Reference
HP-Outer	mail	standard	Section 2.2.1 of RFC 9788

Table 2: Addition to the Permanent Message Header Field Names Registry

Note that the Template and Trace columns are empty and therefore not included in the table.

The Author/Change Controller ([Section 4.5](#) of [\[RFC3864\]](#)) for this entry is the IETF.

12.2. Reference Update for the Content-Type Header Field

This document defines the Content-Type parameters known as `hp` (in [Section 2.1.1](#)) and `hp-legacy-display` (in [Section 2.1.2](#)). Consequently, IANA has added this document as a reference for Content-Type in the "Permanent Message Header Field Names" registry as shown below.

Header Field Name	Protocol	Reference
Content-Type	MIME	[RFC4021] and RFC 9788

Table 3: Permanent Message Header Field Names Registry

Note that the Template and Trace columns are empty and therefore not included in the table.

12.3. New Mail Header Confidentiality Policies Registry

IANA has created a new registry titled "Mail Header Confidentiality Policies" within the "MAIL Parameters" registry group <<https://www.iana.org/assignments/mail-parameters/>> with the following content:

Header Confidentiality Policy Name	Description	Recommended	Reference
hcp_no_confidentiality	No header confidentiality	N	Section 3.2.3 of RFC 9788
hcp_baseline	Confidentiality for Informational Header Fields: Subject Header Field is obscured, Keywords and Comments are removed	Y	Section 3.2.1 of RFC 9788
hcp_shy	Obscure Subject, remove Keywords and Comments, remove the time zone from Date, and obscure display-names	N	Section 3.2.2 of RFC 9788

Table 4: Mail Header Confidentiality Policies Registry

Note that hcp_example_hide_cc is offered as an example in [Section 3](#) but is not formally registered by this document.

The following textual note has been added to this registry:

Adding an entry to this registry with an N in the "Recommended" column follows the registration policy of Specification Required. Adding an entry to this registry with a Y in the "Recommended" column or changing the "Recommended" column in an existing entry (from N to Y or vice versa) requires IETF Review.

Note that during IETF Review, the designated expert must be consulted. Guidance for the designated expert can be found in [Section 3.4.2](#).

Additionally, this textual note has been added to the registry:

The [Header Confidentiality Policy](#) Name never appears on the wire. This registry merely tracks stable references to implementable descriptions of distinct policies. Any addition to this registry should be governed by guidance in [Section 3.4.2](#) of RFC 9788.

13. References

13.1. Normative References

- [RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <<https://www.rfc-editor.org/info/rfc2045>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, DOI 10.17487/RFC3864, September 2004, <<https://www.rfc-editor.org/info/rfc3864>>.
- [RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, DOI 10.17487/RFC5083, November 2007, <<https://www.rfc-editor.org/info/rfc5083>>.
- [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <<https://www.rfc-editor.org/info/rfc5234>>.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <<https://www.rfc-editor.org/info/rfc5322>>.
- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/info/rfc5652>>.
- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <<https://www.rfc-editor.org/info/rfc8126>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <<https://www.rfc-editor.org/info/rfc8551>>.

- [RFC9580] Wouters, P., Ed., Huigens, D., Winter, J., and Y. Niibe, "OpenPGP", RFC 9580, DOI 10.17487/RFC9580, July 2024, <<https://www.rfc-editor.org/info/rfc9580>>.
- [RFC9787] Gillmor, D. K., Ed., Hoeneisen, B., Ed., and A. Melnikov, Ed., "Guidance on End-to-End Email Security", RFC 9787, DOI 10.17487/RFC9787, May 2025, <<https://www.rfc-editor.org/info/rfc9787>>.

13.2. Informative References

- [chrome-indicators] Schechter, E., "Evolving Chrome's security indicators", Chromium Blog, May 2018, <<https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html>>.
- [CSS] Bos, B., Ed., "Cascading Style Sheets Level 2 Revision 2 (CSS 2.2) Specification", W3C First Public Working Draft, 12 April 2016, <<https://www.w3.org/TR/2016/WD-CSS22-20160412/>>. Latest version available at <<https://www.w3.org/TR/CSS22/>>.
- [HTML-ESCAPES] W3C, "Using character escapes in markup and CSS", 12 August 2010, <<https://www.w3.org/International/questions/qa-escapes#use>>.
- [PEP-EMAIL] Marques, H. and B. Hoeneisen, "pretty Easy privacy (pEp): Email Formats and Protocols", Work in Progress, Internet-Draft, draft-pep-email-02, 16 December 2022, <<https://datatracker.ietf.org/doc/html/draft-pep-email-02>>.
- [PEP-GENERAL] Birk, V., Marques, H., and B. Hoeneisen, "pretty Easy privacy (pEp): Privacy by Default", Work in Progress, Internet-Draft, draft-pep-general-02, 16 December 2022, <<https://datatracker.ietf.org/doc/html/draft-pep-general-02>>.
- [PGPCONTROL] UUNET Technologies, Inc., "Authentication of Usenet Group Changes", 27 October 2016, <<https://ftp.isc.org/pub/pgpcontrol/>>.
- [PGPVERIFY-FORMAT] Lawrence, D. C., "Signing Control Messages, Verifying Control Messages", <<https://www.eyrie.org/~eagle/usefor/other/pgpverify>>.
- [PROTECTED-HEADERS] Einarsson, B. R., juga, and D. K. Gillmor, "(Deprecated) Protected E-mail Headers", Work in Progress, Internet-Draft, draft-autocrypt-lamps-protected-headers-03, 16 April 2025, <<https://datatracker.ietf.org/doc/html/draft-autocrypt-lamps-protected-headers-03>>.
- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <<https://www.rfc-editor.org/info/rfc1035>>.
- [RFC2047] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, DOI 10.17487/RFC2047, November 1996, <<https://www.rfc-editor.org/info/rfc2047>>.

-
- [RFC2049] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, DOI 10.17487/RFC2049, November 1996, <<https://www.rfc-editor.org/info/rfc2049>>.
- [RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, DOI 10.17487/RFC3156, August 2001, <<https://www.rfc-editor.org/info/rfc3156>>.
- [RFC3851] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, DOI 10.17487/RFC3851, July 2004, <<https://www.rfc-editor.org/info/rfc3851>>.
- [RFC4021] Klyne, G. and J. Palme, "Registration of Mail and MIME Header Fields", RFC 4021, DOI 10.17487/RFC4021, March 2005, <<https://www.rfc-editor.org/info/rfc4021>>.
- [RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <<https://www.rfc-editor.org/info/rfc5751>>.
- [RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <<https://www.rfc-editor.org/info/rfc5890>>.
- [RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <<https://www.rfc-editor.org/info/rfc5891>>.
- [RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <<https://www.rfc-editor.org/info/rfc6376>>.
- [RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <<https://www.rfc-editor.org/info/rfc7489>>.
- [RFC7929] Wouters, P., "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP", RFC 7929, DOI 10.17487/RFC7929, August 2016, <<https://www.rfc-editor.org/info/rfc7929>>.
- [RFC8162] Hoffman, P. and J. Schlyter, "Using Secure DNS to Associate Certificates with Domain Names for S/MIME", RFC 8162, DOI 10.17487/RFC8162, May 2017, <<https://www.rfc-editor.org/info/rfc8162>>.
- [RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <<https://www.rfc-editor.org/info/rfc8617>>.
- [RFC9216] Gillmor, D. K., Ed., "S/MIME Example Keys and Certificates", RFC 9216, DOI 10.17487/RFC9216, April 2022, <<https://www.rfc-editor.org/info/rfc9216>>.
-

Appendix A. Table of Pseudocode Listings

This document contains guidance with pseudocode descriptions. Each algorithm is listed here for easy reference.

Method Name	Description	Reference
HeaderSetsFromMessage	Derive "outer" and "protected" sets of Header Fields from a given message	Section 4.2.1
HeaderFieldProtection	Calculate cryptographic protections for a Header Field in a given message	Section 4.3.1
ReferenceHCP	Produce an ephemeral HCP to use when responding to a given message	Section 6.1.1
ComposeNoHeaderProtection	Legacy Message composition with end-to-end cryptographic protections (but no Header Protection)	Section 5.1.1
Compose	Compose a message with end-to-end cryptographic protections including Header Protection	Section 5.2.1

Table 5: Table of Pseudocode Listings

Appendix B. Possible Problems with Legacy MUAs

When an email message with end-to-end cryptographic protection is received by a MUA, the user might experience many different possible problematic interactions. A message with Header Protection may introduce new forms of user experience failure.

In this section, the authors enumerate different kinds of failures we have observed when reviewing, rendering, and replying to messages with different forms of Header Protection in different Legacy MUAs. Different Legacy MUAs demonstrate different subsets of these problems.

A conformant MUA would not exhibit any of these problems. An implementer updating their Legacy MUA to be compliant with this specification should consider these concerns and try to avoid them.

Recall that "protected" refers to the "inner" values, e.g., the real Subject, and "unprotected" refers to the "outer" values, e.g., the dummy Subject.

B.1. Problems Viewing Messages in a List View

- Unprotected Subject, Date, From, and To Header Fields are visible (instead of being replaced by protected values)
- Threading is not visible

B.2. Problems When Rendering a Message

- Unprotected Subject is visible
- Protected Subject (on its own) is visible in the Body
- Protected Subject, Date, From, and To Header Fields are visible in the Body
- User interaction needed to view the whole message
- User interaction needed to view the message Body
- User interaction needed to view the protected Subject
- Impossible to view the protected Subject
- Nuisance alarms during user interaction
- Impossible to view the message Body
- Appears as a forwarded message
- Appears as an attachment
- Security indicators not visible
- Security indicators do not identify the protection status of Header Fields
- User has multiple different methods to reply (e.g., reply to outer, reply to inner)
- User sees English "Subject:" in Body despite message itself being in non-English
- Security indicators do not identify the protection status of Header Fields
- Header Fields in the Body render with local Header Field names (e.g., showing "Betreff" instead of "Subject") and dates (TZ, locale)

B.3. Problems When Replying to a Message

Note that the use case here is:

- User views a message, to the point where they can read it
- User then replies to the message, and they are shown a message composition window, which has some UI elements
- If the MUA has multiple different methods to reply to a message, each way may need to be evaluated separately

This section also uses the shorthand UI:x to mean "the UI element that the user can edit that they think of as x".

- Unprotected Subject is in UI:subject (instead of the protected Subject)
- Protected Subject is quoted in UI:body (from Legacy Display Element)

- Protected Subject leaks when the reply is serialized into MIME
- Protected Subject is not anywhere in UI
- Message Body is *not* visible/quoted in UI:body
- User cannot reply while viewing protected message
- Reply is not encrypted by default (but is for legacy signed-and-encrypted messages without Header Protection)
- Unprotected From or Reply-To Header Field is in UI:To (instead of the protected From or Reply-To Header Field)
- User's locale (lang, TZ) leaks in quoted Body
- Header Fields not protected (and in particular, Subject is not obscured) by default

Appendix C. Test Vectors

This section contains sample messages using the specification defined above. Each sample contains a MIME object, a textual and diagrammatic view of its structure, and examples of how an MUA might render it.

The cryptographic protections used in this document use the S/MIME standard, and keying material and certificates come from [RFC9216].

These messages should be accessible to any IMAP client at `imap://bob@header-protection.cmrg.net/` (any password should authenticate to this read-only IMAP mailbox).

Copies of these test vectors can also be downloaded separately at <https://header-protection.cmrg.net>.

If any of the messages downloaded differ from those offered here, this document is the canonical source.

C.1. Baseline Messages

These messages offer no Header Protection at all and can be used as a baseline. They are provided in this document as a counterexample. An MUA implementer can use these Messages to verify that the reported Cryptographic Summary of the Message indicates no Header Protection.

C.1.1. No Cryptographic Protections over a Simple Message

This message uses no cryptographic protection at all. Its Body is a text/plain message.

It has the following structure:

```
└─ text/plain 152 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Subject: no-crypto
Message-ID: <no-crypto@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:00:02 -0500
User-Agent: Sample MUA Version 1.0
```

This is the
no-crypto
message.

This message uses no cryptographic protection at all. Its body
is a text/plain message.

```
--
Alice
alice@smime.example
```

C.1.2. S/MIME Signed-Only signedData over a Simple Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a text/plain message. It uses no Header Protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 3856 bytes
  └─ (unwraps to)
    └─ text/plain 206 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="signed-data"
Subject: smime-one-part
Message-ID: <smime-one-part@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:01:02 -0500
User-Agent: Sample MUA Version 1.0

MIILGQYJKoZIhvcNAQcCoIILCjCCCwYCAQExDTALBg1ghkgBZQMEAgEwggFCBgkq
hkiG9w0BBwGggGzBIIIBL01JTUUtVmVyc2l1b2JogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IG0KQ29udGVudC1UcmFuc2Z1ci1F
bmNvZGluc2ogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtY251LXBhcnQNCm1l
c3NhZ2UuDQoNC1RoZXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0
aWEgUEtDUyM3IHNPZ251ZERhdGEuICBUaGUNCnBheWxvYWQgaXMgYSB0ZXh0L3Bs
YWluIG1lc3NhZ2UuIEI0IHVzZXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0aXN0
IA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSS5CVIeh7j00Boq0MA0GCSqGSIb3DQEBAQUAMFUDTALBgNVBAoT
```

```

BE1FVEYxETAPBgNVBAsTCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMg
U1NBIEln1cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzEXMBUGA1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCalsn6i8Gi44/oAVAn5GnCK4PHHNjrSfWUnne1N41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT905NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCreZu
TtMc1zy++MxQlqdn9WZLh0A0peNZKGMVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhbWdH
dZ5qDTII2PVX1X3K7/c0NxbvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGewy
6SCf58duq/A0EksCAW1b+MD8QH9Yj7CFsmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQCDBDA0BgNVHQ8BAf8EBAMC
BSAwHQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBAAJFEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEEDQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkFgXQLgy7GrW7SrZeBc5IEcjoN9f/gsox/Ht9Ii6zyBZVjdao
x644DsiLQOEP4YMS7y4q94RFFdmdzEbDLyX9sfUhvdTxDN00oHz53PYDBh4zE4Na
r2inc0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVt1
uLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyEx156BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80l1h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vR
hZjVD6FYMIIDzzCCAreAwIBAgITN0EFee1f0Kpolw69Phqzpq1zANBgkqhkiG
9w0BAQ0FAADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGx1IExBTVBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MTthaGA8yMDUyMDkYnZAA2NTQxOFowOzENMASGA1UEChMESUVU
RjERMA8GA1UECzMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWN1IExvdmVsYWN1MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4tFa/pd0/KLpZbJOAer0sI7Aja07B1GuMUFJeSTulamNfCwDcDKY63PQW1+DI
Ls7GxVwXurhYdZlaV5hcUqVackPvedBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
N012DRVDBpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtwS1q7
ktknBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSebwXLJe3VMvbvQjOBmPEYlaJBUIKk01zQ1Pq90njlsJL0wID
AQAB04GvMIGsMAWGA1UdEwEB/wQCMAAFwYDVR0gBBADjAMBgpghkgBZQMCAATAB
MB4GA1UdEQQXMBWBE2FsaWN1QHNTaW1lLmV4YW1wbGUwEwYDVR01BAwwCgYIKwYB
BQUHAWQwDgYDVR0PAAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQE+qV6BdP7GKJ19naIs3Bj
J0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukYr7agyHahixRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9Eiae6aCHHBh0iPU7IPkazgPYgkLD59fk4P
GHnYxs1Fhd06zZk9E8zwlc1ALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+u
CDNG/D0qyTbY4fGkieUHx/tHuzUszZxJjGCAGawggH8AgEBMGwwVTENMASGA1UE
ChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6a
qdcwCwYJYIZIAWUDBAIBOGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHAQAQBgkq
hkiG9w0BCQUxX3K7/c0NxbvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGewy
FLYz1CbB/xsgb5+a0sgYLUg094upq1ZXLWswDQYJKoZIhvcNAQEBBQAEggEAB0i5
kcjRmMF4LK94svcf192padnfUTSyjJtrIf6R6C7xy87VzsmP0PCmHgZ0mTCuvY2D
iKuMId6WPVdjuRUaW6xkgYtgYjPDhy80NY0a9wXEQtjn448G0UHDm21cJyu9LTAg
orSzcT2pwEuGzNdsHW8LB5GtJKYct3RS0+jlbSr7WpZFY1mUrwpsm2r8za2Ko0cy
t/E7Qz/8hT4HU52Na7pS1ZnxrasLr5prSjDSSKs4QK3ncJR8jhF9by0pDCoYgswy
zYaeJt0N+8uv7ab/kBaE3wfZlipMSFRJIh+QeXCkIHo5fW5bn/REZHxMMdMfdPh
bqYT1i46156CS0qyxA==

```

C.1.2.1. S/MIME Signed-Only signedData over a Simple Message, No Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-one-part
message.

This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a text/plain message. It uses no header protection.

--
Alice
alice@smime.example
```

C.1.3. S/MIME Signed-Only multipart/signed over a Simple Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a text/plain message. It uses no Header Protection.

It has the following structure:

```
└ multipart/signed 4187 bytes
  └ text/plain 224 bytes
    └ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature"; boundary="253";
  micalg="sha-256"
Subject: smime-multipart
Message-ID: <smime-multipart@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:02:02 -0500
User-Agent: Sample MUA Version 1.0

--253
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-multipart
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a text/plain
message. It uses no header protection.

--
```

Alice
alice@smime.example

--253

Content-Transfer-Encoding: base64

Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXRob3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqlWajj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZvPMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdW8wHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlNhpHGH29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpeYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PFB5v94M5274XYxW2W4uKGd7QGnUZROsVSYkGiWDp1JhqXwFdZ8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBAQUAMFUDALBgNVBAoTBE1FVEYx
ETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NBIEI
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzys02kaYWTut3
SryCqeHEFBzFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKRiVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMA5GCMCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFvL2zLItHQYSHJeuKWqQENMGZmZmB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjD/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZL
RAzEf7GHqgB/Nyjoad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKza1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCafwCAQEwBDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjA5NTAyMDJa
MC8GCSqGSIb3DQEJBDEiBCAB+IATfw3+2k09hwjUYxzW+Z12sfFp2dTb1pmXGS+7
DzANBgkqhkiG9w0BAQEFAASCAQANJdfU8Dt0pINW4FeIWPdexndYvHYy7jFg5ICy
wIkh1DcqmbdvB4PXcksbJ0zkSVjdjXPdYQYRS4E5C1AEevEe+OkFd16UoGaadoaq
OjyGnuuIEJJbRG2UUZZWMyJW2g8OZRAGZjYgEgVbVflmxqRjFRaelGUorHaHoxk40
LomKSVRTUG11eEhmRmxIY4wKhwc0U9PKjCQFRhu3t1ZkGSfPn9jvdNTJkg85WUPk

```
WqmOyrup6DH4Gb84By+0IMk3vflrOyAw3kbsj6Ij+zymAlH61YypnAvddFBIuZPL
2LYdIHPLmq8KGrzcgkjP+Y58hf9U+6gp0KPU8DAG0vxYs0

--253--
```

C.1.4. S/MIME Signed and Encrypted over a Simple Message, No Header Protection

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses no Header Protection.

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 6720 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 3960 bytes
    ↓ (unwraps to)
    └ text/plain 241 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: smime-signed-enc
Message-ID: <smime-signed-enc@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:03:02 -0500
User-Agent: Sample MUA Version 1.0

MIITXAYJKoZIhvcNAQcDoIITTCCE0kCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBE1FVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGi78Tibx6BFPvdJW+VbgXY631bpi8XsHhD0
vTxHFVivRovgyH6v1vvobDE1xv6VdbyzVT4LEsiGbDzr0t022oXSBV3JkzJez5fw
umUNX49fx31aXa7GDlp0G7YHfzfxSCskt7rREceVzbp3qR46nGGbreosgbVqpiuUX
m3+ghxULxFZBggDJAFhWwH1cWtQ5lp6zAior+Fc0A480HErdNCqE0+21j3/3wIP
oQR6Aqx9beav1jJsJTVGm2BaCpCvLI4aooptm4LqMxXIe33FkzUDexJclwXJgx8y
r8yW3MroptDD7zJQMFu7LMgUYZ2VqTlJBVpST13ZNQ+wxWHRz8wggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFUMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU10YyBSU0EgQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAcBM/QDMNvyAPH1G0py8AovZ7
NHpupXUirN6AZBINxb9rbgM5bv3XAUWKIeNg8cI4I+TF/RXYLnwTr8YSjThp1/+Q
DvcV5T1DyJB1HU5S7VFZHSMrJFw9+14nn83id60n5MSEqtn+Ec5DZaeKo0WXdFXx
Q/QqLoQVx10X5awyChHk6s/oIdgXPAiF7ZJkT35FAGuv/Dx9o2ch17o1SIcgf0ej
8K0txmm2e2ez8bluhZw1DaGDBiYsUIjw3VF9vQqUnhEisQZx0g5j0xGc2kE7Mk3q
wiH8xydBCzKRQfq4ze+m13uyPPgMDJi50pJq00rarsKz4dV+YWbz/5YVKnlMZjCC
EC4GCSqGSIb3DQEHATAdBg1ghkgBZQMEAAQIEEBRNCCx1UMI10KK9qZck9jaAghAA
c8Gt6ZgbCpV3HW0byl0nE4w+Vhxs8Z/1+nNlgrtaL6/ZDHZkfdc+1hk9LUeAr09
QfHkfGMYxWF5BqUk315BI40EYL8kU/dcqTFpWt/Fa4yWodfNGLThjoSfryHJFeC
vBjBcaOkil9EsFpeFB4Qe5DY7/rcAgNCM5N6N3eRTPsIzguArEWX5fz7u1LuI3dt
/c3LsaGlmeHCB9bKhewhqa/jj3fxntB8CRDoSAUwt0t1lzx/GjHNXboz1vH6230o
VPABjb/fqf6l203gszY2RE6wI7zHydlz2DgkpFdjyVk1Jub2+QkrQA7Brn9gES/I
gshjTIF+OL3me4UBxww0Bxtt46yz8FpVVOK4MunYe14U4p1SR1WEZGRLPDL+bydN
```


vXdstX39Eg8YChAdt5o5pPQ7bUo3Qkk0X9glJdyVNsTpWREj+F+/6do/JPStJSQt
TYgnXdjkHP4/w6+Xq0cogfEVp6in7KkwfZ0v+SdZK++IPm/rMOsZlP9MbM9Lk0A1
6xAB4MmPl0UDs5KQB5NYWvt034PQv8NRqfs7m1S7F4gvCaaAA1SZdqRn7kIdiNqg
RUFYTkHf5/g+pJ/Ysw9lIvIAOXHtnrbsT0xbrsIzL5wbkvCDW6ZTQIQ4kP9D0NT1
1JcxNVj10GprUztmYgq0y+wIjJ3DLXHSSdugy3S/qEjiCCZwN8zAVl+c8Aii fgfP
zpI4QU1552EC8HyoIUZSQP50/dIy6ABLEDcwZKJ8nGJdSLurpD0V68p/hWk+Q6mu
I7Dqid1NT0yehBKvZRE8jr7wclUm73xX/PhOqY158N6wNsekUHOHYERKU0BzRScQ
+YJ9tcsmpLdE6jAzJB/vjjgoiLxIMci0PAXVdGjixY3QhLh4DJTWkwhIr4kMkv0
OdcIw3q2+9sxT4fbFMROIXLUahE5qGbIyyvpPgWRmP/otP4jEyCgHuBxHKar630J
q381rmnb6Cqybc/Gmfxb0hX78DTn9hWag7fYh6u0yFmuH2bWvXW+ff+yeAy0/PCR
hxv0jZ+e3yx0Z4d8Q4Jk6kT6+HaP1tAMvJc4dubvP0+nQFZsHcxdlMrmBel+xpg5
DP1cGvtwQicVbCYWPKJINDcn9fExd1BiooF6yfaQ6a2h9zFpaevu5EqxRso57zpl
fv9PpPiuT9xQvFYtTg07cD8negTwJxVZwhP+PXdcTuw0khCaW8I65SnKcvyYZpG
0t+Rr4U10oXs/0ERZLxQbJLIRIxsfeKwvFBZ8QXp30mfQ+4M41C0/f6cN00TpF
LlNM6YyJWYQ38UDpirxgrp+yS0mCCFF+OjVC5AHsS+0rozv8IOWG8A8KKgryfNMs
tLrLctIOXLL900J4D0P3noqEQnY0I9Qq9X7f2Zv+f1G2sp0qrA8+frrxyB9H1VKu
Nqo+S2qq/c3d1EvDtVG8YU4gCFeZzUq2nAsZcIoD157z7M512cQrCabLcZAYG4T
/PwRQpb9EqPwzuEBPZq997VbzzWKzqOuJPx4TeT8ksJawZzvs0/Gi5YL8inCV0Hx
vz2vmsWlL2sDDCus6vc17X5p0qckNW5A7J/uG0Xylkb2ZxTR0xP1wd4P3Ncw0S8m
3TVIiSKsNDHd3/ZEBkTeVlcmkprNeApZ6toTc3/izJ020gLDtdjfu85nEVTIsalg
Syq8uGagBIQPpNb/EmICF1s78/b7MPu/NtF47Z0j8LiljS5xac1s/mT9X0EPw28z
ZmL6/5I+UKMKsJuaoSAJ5TcK13TONCd0teBt0dxMZHBw4Ix/YKESKCFu9B3IyoLq
kuCKtuGG6KNyIDYhkrLHs4wvQrhuky5r+wuzIE/HcM8mDWSaX+qEsGp0BUvFaDQZ
oNxuups1wKXsE03I2WY0T4vVu6FbkQxVusmX5KcXqJzaPu7bfaA9YpEyc0b0psC
YXMyUoplAtGQFwptKKxbhjBNoaIK26hnhREHga0cD1YWTau1p0bwTTRCqsYi0Vr9
iHmXjOrI3Hzz5Nks40iF1tATULhL3dNzpZjIfdfMWsY6rFIfo+CaC/VpXFFv19UD
1TDD7NyMSLNKGHMq4yDB0Qo9TyfiU4p2Asq3T+kFcS6X5WqdXeM2KwaDPuUL13J/
6ulUm5tm+8rQ5hf3jbxSmoC73HYywM0pdnv4BwghDetE3mdcVcSWYS38H5p0ZFh6
NhTKY9PT7poeW2U/rmlfu0wKP97bIWVYiUM+F47fukbGymGztGJVqYt0JoLC3HT/
cVZhUaAqFkgbDBpGA+bAnkzD1jHl3wZya4rb2LmhYSZM1xNqkKolQ+t3VhZ9FpgD
FFA7UWxGGjW2N2k/zJLdYNLjMtBRb2idEh0KXmxadRWRazIb1IjWGiXRtKmPRvWS
IPN138WtWF/fTpV5XP+Knk7SDZYzq2AZ8f98QDimmopz0N2cBDQRMUD32t4hFzHz
K7IBAx+fkQdw8JkX4JDJSGzMKM8gl05dp0NZYSNB4ucEcmchi+7nMKszz5A0Nsjr
1V/khpZapoTjCTH9WZegijMsaiU+sir1SadRTdnYxiwkJH5g/Xf0e+3/+1+BDPb3
ac0vB86womwCoUgRnnfJWPL07Dky5+p9BqYvKkmHuhzkL208+/gy+Z/aPnfZ1Syt
dz0gzSgvFrmRPKASmP3KVGM6w/UwEhlD03HjNo0dv6qyQsy1dY6M4IA2tsCvKYg
qCw1zzZMs/P+PSkZtwwsQ9Zkn1b/wq1AFDqxjs3cysQeBLt0wAGBIRtnetvsWht9
yxAMlanLX01Wh8PtNewJY2LZZkhkOWCXP30VSqrzmwhGyX61wMH2AAv+mu6hD3ci
tyhD44SvQUVV0VSCSyPSIcDZsdHL+XjuY7WDuiFh6v9Jb3KKZqbuoXoet44BtOuY
RTit8UQJBGqReS9YJGh14U2ra1dvKLoZHIZdyxob12fu4QkTDAjGIvDzYuxuVaZL
W0NaHpBNi10QUitx5e6JvyjIKtwM6Y/3/0o9pInhXDezk3t78NyctFR08xFQY3LJ
DN3S2EgXj1jWmd5E0/z+Tccg7d8hEn+0vVCRRQksqiPIEcZ1f/xgfm01F0fnI1Pb
OJfUSuZpTvnWtvCTOn62XmWj+4jzXBmopauAqf9XzDj6NshGkrPVrdotEhFoYYRu
OH00K4dUQf57JkVv56tuHkCAGUUGqVRzf9h2wcXP77vsUx0gpjXSKv4SMx7IULW0
jCz1WNqQXPFny6j60BJzZ8wd6nFshHcYbvCP+BKxx7WB3j5Pqxr3/s9S9daCgMQ4
gWiPM0zuSgoTz2ggjqv31QMAXvkBSE+DIAuh9BPw5pwoMsdMYT9eV+DrbN4dhy6t
P/4zCB4NQcyU2vP8P9piBLhcjunadSdITTna3D/fA6VdhidmuF5ieCzo1sTAGH6H
/VRPjxvA9gBeDtko120xoIaLpBF7I75UuFziIzuGuSE11Af1S+I4NOD9tw0Gw+XU
/lvzqk4NHZ/j91GvRxTRj0eFWRuTKXDvVj6Z07vW118tJs+IpslaZgo5/sE7Ntx/
kTpAFcckTfz4iG0ngjlbVv7Do9fM1ndyUz8KxxznxBkS5kWW63rsobm1Lpfks9zD
qIcxIldwnbKDufmd6kKgu66wjtfxKcGK+JQ09r2G+E0vDHL03CUHjVafLEN1Rwt9
4Caj4WW5dcVQh+r3cYNeM50WHsKQ4leBxdVHLswnLa4PsIH5LqUDaFUFVE0XbD0I
SnqIMMCdqGsGGsBIEDjop0rYj8rqyUP85j43/eTE2Jv7mQsvcyAqH5f0zb8MkGD
8AsdOxVIbgYYaLaB01pWcQE/jRv4D7c00D20M1DQzED9Ydzv151jHE+71LVUbSkA
LQoYXJzLJn16DRYbSynXXFiRPmgAq9sfPEf+CoR47zpQUVXACRPLieRSDajlnj/U
XaoLV6JVFLY7+FQeW/W0YE1Iz4R2NJXdbXtaNNbjLnrS+8sW99cVY/yzMUjsohys
5Vjun8GPVRYVYAx003J5bdzeFPLxOhy70f461JxL0kBELzWatCMm+MwBbrJCphS
0PlziAmYr5EGUEhA2pmv5050k83Z7C41mdbrRDraw++N0fq7mSm9ZgJRwbslrP+d

```

eFLWEfWIEoZ333XsmbJSi1E/MhJ3dCevVc33rEwaUv0JK8p0SMQj0ft13yPYs+V1
YU/spQFYsXMhF8I4ZKQwGErIQEY5erTLbnhCRZgJgteQ0CkiQwB+U9JVnaJByjTw
DpY21mtfKIVndc5rrThpDDI2uEiS+u42z5UxZiXiTYthWvrx7HQAcf9JP4INCe57
tvuGXDDfN2Hu5Yfnu6CdTqrovkbEzYt2kEzCXKvNZGcp58Nhbybt6Pw4Iju5XsA+
bptyQfmSSW6Ph6dXub9VJQK1F00nhyyq6+Th+DXaNeRnXx12jfykX+mUUFN6KHkK
9Td5k+yyIOGWe6oEeG4nwwytaDqduK9jBEna65c0Bh5Ru1CvabCEXsHT3ovdvgrL
oJU05WjAGGpdHpXUTlCwZHL02zgD9L86zaZdi0fe9EcRxi/4NcbWkRhSoZTBur0+
KwuMH5ijXlI4Bb6Ygt8Z9VUsTqr/QjdlnGVkIWS0qkw+3EVuHsB+ukx19hTXihCz
TDPgBaI8twdD5UfxnlgmM88304Rt4JsraLb3YtX8SD2p0g4GFfkEVKMJXYjWz6M
cTyDUBnyyShRHtInBjnn6a1MBkq0t1vu1RmUw0hd1Ua7ripH64qJFe938SJBu3yC
7divmSGh36en0ix6/hwq8uYVv00RiyuMQmGs3KVVIByIL43RVhlthvcc006I6l3s
U40BsdC/zXG4iZr5PT0LhAUgmX60cPy2INFx+E/Idy45sN0pj7zfTSxrg5br72gg
dIZQkGYe3KJhMvHvkaA40IEjG1jU95Bx+bFoojWUaMUI4wlhhz0bppZF/bkENLhGq
IXVMYUfa0GFSvfhfXN7r3VvRpzkh7mgJrsIFwG035ZhZq904Z1Yw11N9pns8X2s6
PsSOZAO/E0NOMLSr0onmHy2wqGY7kSMprd9FI7ESe1hwLgqh2pVNesYGqx1Aw0AD
9rDktHKChXqAQDYELV/D1239rxc3tVFzoXtkk6BcNlwq/hvksAjk1/sMNA9x70Af
gfe/zFZQNhWFNzuGd6ADf4Io+Wg9+L60JZmgBx6A9IiTygG9D38yREzQl0BgfGx4
xlkbs830d0gKafDVTMWCNomv0QicU9kdirLUA0Y17N5yIR3TMH8p2kkkyYH0hMdX
TQ5v4K/0UYQteADMquJIJQiIfs0Edfd6to46yWIWLCQSJpN+M2iw0Qo0P0jevCkC
RVZ0xXALDuEEUJLj1SrRV0x5drsqLoClAeH1Li/ZFm+I6qA2pVKrxohwndGimR
3FVKgLzC1srGGXsIGqoq5ueeN2ZTIQ60yJh/ERLfd0uEeVCv7UIBRwQ9WrNaaFY1
10toJc+0XZ617xSFoKWnyA==

```

C.1.4.1. S/MIME Signed and Encrypted over a Simple Message, No Header Protection, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"

MIILPAYJKoZIhvcNAQcCoIILLTCCCykCAQExDTALBglghkgBZQMEAgEwggF1Bgkq
hkiG9w0BBWgGggFWBIIIBUK1JTUUtVmVyc2l1b2JogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQCXGhaW47IGNoYXJzZXQ9InV0Zi04IG0KQ29udGVudC1UcmFuc2Z1ci1F
bmNvZGluZz0gN2JpdA0KDKQpUaGlzIGlzIHROZQ0Kc21pbWUtc2l1bmVklWVuYw0K
bWVzc2FnZS4NCg0KVGHpcyBpcyBhIHNPZ251ZC1hbmtQW5jcnldwGVkIFMvTU1N
RSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2ln
bmVkrGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbG0KbWVzc2FnZS4g
SXQgdXNlcyBubyBoZWZkZXIgcHJvdGVjdGlvbi4NCg0KLS0gdQpBbG1jZQ0KYWxp
Y2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJU
h6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFmgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmawNh
dGlvbiBBdXR0b3JpdHkwIBcNMtKxMTIwMDY1NDE4WHgPMjA1MjA5MjcWjU0MTha
MDsxDTALBgNVBAOTBE1FVEYxETAPBgNVBAsTCExBTBTVBTFdHMRcwFQYDVQDEw5B
bG1jZSBMb3ZlbgFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqV
KfqLwaLjj+gBUCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID
lB/wlbdmadXPmrszyidmbuZm0pB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdS
NRFxrfKeoQEFXg0aGdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1
ZkuE4A6141koaZXC5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv
9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIB
aVv4wPxAf1iPsIVKarUCAwEAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYZIAWUDAgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxl
MBMGA1UdJQMMAAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIFIDAdBgNVHQ4EFgQU
o1NB1UQ8gCkVfAej80e0r83zdw8wHwYDVR0jBBgwFoAukTC0fAcXDKfxCSH1Nhpn
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKcCsTKcFqQMPTryujRGzJdYA+R9

```

```
eBAuDLsatbtKt14FzkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjgOyIs5AQ/hgxLv
Lir3hEUvZ2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLro
r2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKgd7QGnUZROsvSY
kGiWdp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzS
WHUz1F00juyu0fQsqm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIIC
t6ADAgECAhM3QQV57XV/QqmiXDr0+Gr0mqnXMA0GCSqGSib3DQEBDQUAMFuxDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUg
TEFNUFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSib3DQEB
AQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijSN0R8K/hN8D+l078oulls
k4ASvSwjsCNo7sHUa4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6uFh1mVpX
mFxSpUBYQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2
Gxzyms02KaYWTut3SryCqeHEFbZFkBAurMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wX
VgkWFf10ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElNAtJ7B
tZcs17dUy9u9C0gEyKriVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAawGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYET
YWxpY2VAC21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8B
Af8EBAMCBsAwHQYDVR00BBYEFLv2zLIthQYSHJeuKWqQENMgZmZzMB8GA1UdIwQY
MBaAFJEwjnWHFwyn8QkoZTYaZxxodvRZMA0GCSqGSib3DQEBDQUAA4IBAQBziaI2
p86poGkjD/4Kkk0HG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzh
W/JVdYn30UxfyrZlRAZef7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEN
t1sRx1cvb7HVX524bKZa1oPTUN1m6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9C
Dr40pq2JCKzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0T
zPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNTjh+Aq
J5QfH+0e7NSzNnEmMYICADCCafwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTQSBZDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpo1w69Phqzpq1zALBg1ghkgBZQME
AgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCsGqGSib3DQEBJBTPEFw0y
MTAyMjAxNTAzMDJAMC8GCSqGSib3DQEBJBTPEiBCD1UvgsJW6j30yo/fAeR1vd2Kst
erfZdXyJSku5gnNGRTANBgkqhkiG9w0BAQEFAASCAQAYPeerPzpSeDL0FAep2p3r
y/xmN2pXvMsg10QI/r6H/WIUpXga0Z3Z5M1/VsZtKIbFGv/3en7GoqKc0w7/R26B
qKvtjt+0K7CW1BaWKRqcx7hTIVJXQhT7UnQLnT5daf/BiPbf73FEKo0E4N0cvsVY
237ni7VR/Rz/uz3Tnhe0sBk7H/AEmKiaPbnJj8wFoc6E8Vtusy5ZIrhX6YEq6e3A
YIJ01cm+cNWBa7k0RT2pyKZ3yF2IIcoqyEfw/QkPkh6KM5hKS0UhbvQRpdK0v5u+
r/KmOuAbX04XzLZY+RYfDPG/grj+YxeJEgZlUfLgx8pJET9J0RkTImNh1zVVU+r4
```

C.1.4.2. S/MIME Signed and Encrypted over a Simple Message, No Header Protection, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses no header protection.

--
Alice
alice@smime.example
```

C.1.5. No Cryptographic Protections over a Complex Message

This message uses no cryptographic protection at all. Its Body is a multipart/alternative message with an inline image/png attachment.

It has the following structure:

```
├─ multipart/mixed 1402 bytes
│   └─ multipart/alternative 794 bytes
│       ├── text/plain 206 bytes
│       ├── text/html 304 bytes
│       └─ image/png inline 232 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="e68"
Subject: no-crypto-complex
Message-ID: <no-crypto-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:00:02 -0500
User-Agent: Sample MUA Version 1.0

--e68
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="f70"

--f70
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
no-crypto-complex
message.
```

```

This message uses no cryptographic protection at all.  Its body
is a multipart/alternative message with an inline image/png
attachment.

--
Alice
alice@smime.example
--f70
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>no-crypto-complex</b>
message.</p>
<p>This message uses no cryptographic protection at all.  Its body
is a multipart/alternative message with an inline image/png
attachment.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--f70--

--e68
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGGoAAAANSUhEUgAAABQAAAAUCAyAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQejOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--e68--

```

C.1.6. S/MIME Signed-Only signedData over a Complex Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses no Header Protection.

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 5253 bytes
  ↓ (unwraps to)
  └─ multipart/mixed 1288 bytes
    └─ multipart/alternative 882 bytes
      └─ text/plain 260 bytes
      └─ text/html 355 bytes
      └─ image/png inline 236 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="signed-data"

```

MIIPIwIYJKoZIhvcNAQCoIIPFDCCDxACAQExDTALBg1ghkgBZQMEAgEwggVMBGkqhkiG9w0BBWGgggU9BIIFOU1JTUUtVmVyc21vb3JogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjUzMyINCg0KLS01MzMNCk1JTUUtVmVyc21vb3JogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHR1cm5hdG12ZTsgYm91bmRhcnk9IjZkMSINCg0KLS05MzENCkNvbnRlbnQtVHlwZTogdGV4dC9wbGFpb3JsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlc1FbmNvZGluzGZogN2JpdA0KDQpUaGlzIGlzIHRO0K0c21pbWUw215LXBhcncY29tGxleA0KBWVzc2FnZSN4NCg0KVGHpcyBpcyBhIHNpZ251ZU1ibmx5IFMvTU1NRSBtZXNzYWdlIHZpYSBQSO0NTIzcG12lnbmVkrGF0YS4gIFRoZQ0KcGF5bG9hZCBpcyBhIG11bHRpcGFydC9hbHR1cm5hdG12ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lDQppbWFnZS9wbmcgYXR0YWNobWVudC4gSXQgdXN1cyBubyBZWfKZXIgcHJvdGVjdGlvbi4NCg0KLS0gDQpBbG1jZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KLS05MzENCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc21vb3JogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQoNCjxodG1sPjxoZWfKpJx0aXRszT48L3RpdGx1PjwvaGVhZD48Ym9keT4NCjxwPlRoaXMgaXMGdGhlDQo8Yj5zbWltZS1vbmUtcGFydC1jb2wbGV4PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGEGc2lnbmVklW9ubHkgUy9NSU1FIg1lc3NhZ2UgdmlhIFBLQ1MjNyBzYzWuZWR5XHRlIAgVGHlDQpwYXls2bFkIGlZlIGegbXVsdGlvYXJ0L2FsdG9ybWf0aXZlIG1lc3NhZ2Ugd2l0aCBbhiBpbmxpbmUNCmltYWdlL3BuZyBhdHRhY2htZW50LiBjDDB1c2VzIG5vIGhlYWRLciBwcm90ZWN0aW9uLjwvcD4NCjxwPjx0dD4tLSA8YnIvPkFsaWNlPGJyLz5hbG1jZUBzbWltZS5leGFtcGx1PC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tOTMxLS0NCg0KLS01MzMNCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiaBiYXNlNjQNCKNvbnRlbnQtRG1zcG9zaXRpb246IGlubGluZQ0KDQppVkJPuncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFBVUNBUFBQU0aViwTkbFBQUFjRWxUFVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZlD2taDQpzZ3J6ZmNxVklwTDJqbzA0NDdnWURwYUfYaymtPbkpIa0loQWZUUFJpY21oQWY1WUpydzd2anYwWldSVO0vdWxpDQpZ2FBmMVFAfMTERDL4CHBK0HdBQUFBQkqSVTVFcmTKZ2dnPT0NCg0KLS01MzMtLQ0KoIIHpjCCA88wggK3oAMCAQICEW8tJb0R0ZdKzJUH6HuPTQgIRQwDQYJKoZIhvcNAQENBQAwVTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNFUMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EGQ2VydG1maWNhdGlvbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WHgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBA0TBElFVEYxETAPBgNVBAStCExBTVBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfLwaLjJ+gBUCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1maFIDlB/wlbdmadXPmrszyidmbuZM0pB5voVfifLYy3i0x7Y0qzXr16udP07k0sV+uF1SNRFxrfKeoQEFXgOaGdmnx40G/e3p1fIKM0pZzL0oAJF5m500xzPL74zFCWp2fZkUeA46141koazXCNS5XL7wWTLMLNf9Bby5ksKqUqEHAMd1nmoNMggY9VfVfcv9w423GG8FtpSX+TWzB2zNS20F+XIVznRG5DeoLq8v88Z5bLpIJ/nx26r8A4SSwIBAv4wPxAf1iPsIVKarUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQA4wDAYKIZIAWUDAgEwATAeBgNVHREEFzAVgRnHbG1jZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkvfAEj80eOr83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSH1NhpHGH29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCsTKcFqQMPTryuJRgzJdYA+R9eBAuDLsatbtKtl4FzkRy0g31/+Cw7H8e30iLrPIfLWN1qjHrjg0yIs5AQ/hgxLvLir3hEUvZ23MRsMtjh2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLrork2X4P5uXxaP0LIZRzWmkw1RF7F0D7PfB5v94M5274XYxW2W4uKgd7QGnUZROsSykGIWdp1JhqXwfDz8A0emITGXnoEAFvjjCqh64P1hIeMorj36pgL19oWZD6YrZSWHUz1F00juyuOfQsm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAHm3QQV57XV/QgmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBAQUAMFUDALBgNVBA0TBElF

```
VEYxETAPBgNVBAsTCExBTVBTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NB
IEN1cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMQQWxpY2UgTG92ZWxhY2UwgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo
7sHUa4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+95
0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2GxzYms02kaYW
Tut3SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfC
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9
C0gEyKriVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcWFYETYWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAw
HQYDVR00BBYEFLv2zLiThQYSHJeuKWQqENMgZmZzMB8GA1UdIwQYMBaAFJEwjnW
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEEDQUAA4IBAQBziaI2p86poGkjD/4K
kk0HG25nY/0eNARD6/oF0/sYonX2doiZcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZlRAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRxlcvb7HV
X524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP
0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AQJ5QfH+0e7NSz
NnEmMYICADCCafwCAQEwBDBVMQ0wCwYDVQKEwRJRVRGMREwDwYDVQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTQSBZDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzppq1zALBglghkgBZQMEAgGgATAYBgkq
hkiG9w0BCCQMxCwYJKoZIhvcNAQcBMBwGCsGSIb3DQEJBTBTEPFw0yMTAyMjAxNzAx
MDJAMC8GCSqGSIb3DQEJBDiBCDw/DGldVr1aM/U2iIYH8C6YHskLUihv8FIEUZC
JPECvDANBgkqhkiG9w0BAQEFAASCAQA/sn8ReNdvJH803Ejzs7eF6tBy6DYD5dFE
aLVxB6o3G6gHcupmwvHvL6zouALUoh+zKyrXuWNCpQGfbUqXoAC2cQ6ejwtz3Qnm
4L6amZZQC3NnwFfyT0rIvGrMdT1M/39igmep2ZUq9BQS7vq0mYQzSgkGm148y0fI
QDeuJZGcw1EcFZuFUZPX4J9kvUu5twvDQoPnTitPVGJ9C21B6PRkYjKW7JAmNtBL
qRbwZbt0jbrhAszzkRG5P8jR+35FIkG6abSF8hwYix0fJokUn3YnU7G6pRM7DSGg
S9MtDUy34GtdUQ70XfL1La5kpQfUFBBQ5qf1KuvIrBsYX6qjWAVs
```

C.1.6.1. S/MIME Signed-Only signedData over a Complex Message, No Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="533"

--533
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="931"

--931
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex
message.

This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a multipart/alternative message with an inline
image/png attachment. It uses no header protection.
```

```
--
Alice
alice@smime.example
--931
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a multipart/alternative message with an inline
image/png attachment. It uses no header protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--931--

--533
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAACe1EQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQej0ywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRUErkJggg==

--533--
```

C.1.7. S/MIME Signed-Only multipart/signed over a Complex Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses no Header Protection.

It has the following structure:

```
├─ multipart/signed 5230 bytes
│   └─ multipart/mixed 1344 bytes
│       ├── multipart/alternative 938 bytes
│       │   ├── text/plain 278 bytes
│       │   └── text/html 376 bytes
│       └── image/png inline 232 bytes
└─ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature"; boundary="4e5";
  micalg="sha-256"
```



```

Subject: smime-multipart-complex
Message-ID: <smime-multipart-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:02:02 -0500
User-Agent: Sample MUA Version 1.0

--4e5
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="0be"

--0be
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="cb6"

--cb6
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-multipart-complex
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no header protection.

--
Alice
alice@smime.example
--cb6
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no header protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--cb6--

--0be
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUUEUgAAABQAAAAUCAyAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQej0ywiwYnCtxDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

```

--0be--

--4e5

Content-Transfer-Encoding: base64

Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCc0CAQExDTALBg1ghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdG1vbiBBdXRob3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTBVTIFdHMRcwFQYDVQDEw5BbG1jZSBMb3Z1bGFj
ZTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqlWALjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBCGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVGRNhbG1jZUBzbW1tZS5leGFtcGx1MBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlNhpHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKCfQqMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKgd7QGnUZROsVSykGiWdp1JhqXwfdz8
A0enITGXnoEkAFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUXDTALBgNVBAoTBE1FVEYx
ETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NB1EN1
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQKQEWJRVRGMREwDwYDVQLEWhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwOrjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUBYQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2GxzYms02kaYWTut3
SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbB1fkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgnVHSAEEDAOMAwGCMCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEF1v2zLiThQYSHJeuKWqQENMGZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjD/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZ1
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JCKzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQKQEWJRVRGMREwDwYDVQLEWhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IEExBTBVTIFJfJTQSBDBXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpq1zALBg1ghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjA5MjA5MDJa
MC8GCSqGSIb3DQEJBDEiBCDQTcb+2QaMhBSls10nLpoJyHSnq4gNzFYU45gwqAHj
7jANBgkqhkiG9w0BAQEFAASCAQCYM1/HD0Ka4aZwwLS4xMGoyFzGn5G2C3ph0jKS
mCVbpfAxeHnsnuFjdCYzgN/mdBC0qs4P2/rBGWY3DpDhNkdaB+Q2/IZmI1UgyRTM
oc1bWWQfTLX1BuI/mJKqHBhJn0y17UXCUAnvSoYGFhjmQTSr3k4PsdJod78pEa
9+Yx61BGVyznuhHaGuB7lh/S9pxAYtoJFUuIVq+frSN5xhmisPXluFHC3UPu3Hyb
3w6gm+bTL4NDNWwXXSn5wfm9Ru05b3eAEv9pADPZ2TKZPxrfe4wPNzArgYwdn3k

```
6NdLv9w4mZmSSi0y0lfKo3cgo4rZuN6CeLCgqZ0GjIJS43v+
--4e5--
```

C.1.8. S/MIME Signed and Encrypted over a Complex Message, No Header Protection

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses no Header Protection.

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 8710 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 5434 bytes
    ↓ (unwraps to)
    └ multipart/mixed 1356 bytes
      └ multipart/alternative 950 bytes
        └ text/plain 295 bytes
          └ text/html 390 bytes
            └ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: smime-signed-enc-complex
Message-ID: <smime-signed-enc-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:03:02 -0500
User-Agent: Sample MUA Version 1.0
```

```
MIIZHAYJKoZIhvcNAQcDoIIZDTCCGQkCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBE1FVEYxETAPBgNVBAstCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIEU1cnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAAWNP5pH9dbDPudHqXSo0/ngH17DGuH0uRFS
i68xp82mL0/liolbzronottFipHvmMHYZ+dL6fqVLlqY85FtCp/6r6ik1muQzP3g
TGRtiY5SvNBnm9bqSMcf0wHRAat7gKVKLktFXeQN5vUmaxW4H+RXBQHFXpoTljF7
z/z2oPxLYiazyV+srwr1SF7N8NvwXgtewhV/GDQZKGZEQq1X4XPRy1XDPdi+vHwU
0gxqwrZAhAkN8sAIs+82yMff+OE60fqI+pPWxrR0YIEEXK/DB14e1yA0u+keo/eD
NWFKE7g2BihWcp10wDEZHqEupPPN52LCHihyzpBdG0ubSpqYm3AwggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECzMITEFNUFUMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2Vydg1maWNhdG1vbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAEALPDG21i48vBIODVbDuAZnJ
AIJPGuV9pVAU6AqQ3+WWPd7kx8ct2WJPWpU0oKsvFyyNsTc8n61VTrwf1R1AcGhj
kkX7VGb71lpnC8ygaSqPF6KtkMICcW3nNdXBUqYR2n6npGD1z7CzE1QbMgC53E1l
VqC56yHjeSiyLJKyyZBq/0bDjveFHndHCWoIQG7f1HcA8CY4bNNTC6YzQhQNbc69
hS+S+Wwj0tpmNXLVZq491Rs1zPOUN2XjwE638rUqe1M/McBAwAXFQ+YBPdjWhiDg
SrAjN8xnTyi4XJIdabs5RIVg+NWDHuhdiTlzU8M5kY2ShAuGHY0F04451/e/CDCC
Fe4GCSqGSIb3DQEHAAdBg1ghkgBZQMEAAIEEGsnW1gQI420rjxx3Fn9pySAghXA
P71fxkSiJhQ9hJFuk1VtxPLYVxD6RroosTILpBn/eB28f0yA1z5pIhxx6CH35SuL
```

MzuFsnN99/Lmv0e9z9Dc1UCrWLUhod5uVQilrdouxXl1jMdZlNGDj1zc10+82ahAP
KotYU/8AmtUHiGGS4BvR9t15fBF2172KYhlh1MHIU8x0C99vq0q41vBqtC9cmCzS
ht9TxlwRACQgAxADyzSKMc2rtqkAEqGRNBHxq09KxI9pJ6qkj3rQ5aL+epnkYoGN
B5thIQCoG7x/jNzN+mRdtvi3LhM7Uce1TU0N83VoBxpiH3o04re5CUB8ELEYSsm0
4ZN/5AFQ3RQyZS0z1tgWzahrzo91VCvbdnM0irtXZPjpS/NoR/0ZokjE5Iw3SnJZ
35gdvu48eGStmKDFiTs/TXkuPQcMd2a0/joDD+/XNtuSdatXWp+PvELMYR5Z4Pbz
KMo1jMj5n3j/0+6WF8Fg1Dx8vr9JwHTP/4FFjh3qC1aMZxh4PjLEB4dD8rWJQdJA
p/3wS3+d+0kSkhnjG2dT5/6MtRwX5HFQlRvEAbdBIJee0GTAlLn974Li9JiutWzz
sVxTyD+6IBTYSoKQVbL8Th29J081sh5OV2bZ7EFpU6iwWMTEjKQBML9PLs/B03ME
Z0sd8Lh3+RLMm3hsCh6ixAyDBX0xJUpW5dbbnKMffsUwdRxBB008rMFjURSSfJ4G
HzqXh1Lr5XEoKG7UQxW/2brMx7gf30XsKq0YWQ7t6eniMkItu/lcndywe58q9nZF
h5NmmXH7Wf/YhcH3HywFXRv/0tSs3EgpjIgwGbeggwrND8LKx15kdRpT8egu6s0r
b4D8PhzYwKz87V+6fd6rDBvarWD60i+t847eVdaGPZ3qVvAMlQs51lAzLPUsqkU/
zLIL1c1SxCSofWebd81CJ/6khs8tWpoiEQugHMRjyLykbax+jHeA7UD4+XZhgaBN
j6VJxeiQ3Euaqs6NdVe5KLQGVcpRayoiFbsI/NogUY2WM0pfccGHtLA1KbZga5nX
ba6kox8cLSgf2w4B2CGEFAYl/yCXIvEbJE+L5vMYLd5dtW2UsR5HeD5i8NZ2+hYC
oDq8hcNYSCT1CX2BTd7bCrC0aP38p12Q+k0VV6J2y+lyL+P5hVtcY0XaOfQqWjhf
7tpMxMMGqiaHP/Megtx5x9pudrERLHpJNf57kx/YoiD0fKPSxNmKMfCWkJF0r/H
9PPYER1ir51S62YQvqW9s2rwhjCSiL/YQVXpGoR16JRmcIB0VMsT4a9ArSFUDKnt
7x30W+CQ0ff4U+l0sfE/jfLwtPB29h1i5JFvbrzc9oyi+xDa4Iy/St4bbS6wulQ9
lo7PgPM/Oo8/Crav4vd20tKhNQUr9YaC8a5n3fnc1F256tcZunUg2G4Mvm1ZJt7
oVslu/jayws1uQWdpA8ldSwnDq4wOFN5y9xCj0UgCaYqRSwB5auAlCUo8WXYIkyn
rhO+TwOigrJvZ2AgJjxh31CqClADwn2jBYkooDE71Yf00XjR6a8LBWRs4jCyInbu
ykdEdDcr11peNN0AhMKBFd670Qp/eQWtcrjWuM3q0sZfSF6YuKQJb1t0yRQontpo
dWFHw5RNI5p51x4b131XfpQ+dg6JECpbgnjCp03tVRMzAlv1j8m0P3dZr8XBr/8F
c1128rmsvIGNWPTU8N6sAzBvWC3hnuq0fmiyvlnF4+lk5DJWfXVPHTMTc24x0p0z
z1gM7+x/v+SIQuH3VvmEtQCCKtEXUHW+sSYRhAlwG1h8Ii88RNgg6TpTqicX20pX
WICs5PLwa9BnYk3IAgyWfHhYEqY4ZYbq3lMnkaCZ0G30LXRqIZtumMTFK0j8Rft6
YI7wtpXImenNYZ0VSqS1S5hwLrYR3BjxjV088ZhUao2cA+c+Gdown3j/v+BpkJgf
5AvNcx4z29oJmYq/lCChu1UHIuKdu/zyMgljgJoTbvtLB/HoIYj1BCgIoknhrWz8
Rxsxd1+TupdzN0fQw9jmszQdwpalTL9gitqjeky3Lt8mfw+r11aTiPSS667pZebq
fBdh+FlokKqhprCFYZbD81V36anMHWkbDxj4/E1Ba58jZbC1w6GDDQ5uSLSXgbGw
vb255hmcWco8N78G3nsWtvgyR9P4zRjfu/KM9IPzReHeQkE1CispMCf7Zx6+LJrF
w1W4V17159d5q1K0DKGInUpjGrBZo06/rb/QJYmh0CvAGbKVUnX7sWzoGIbzTN3g
zGEV/yAlROQDEANmCoIKieVlThjDf++eUKiDbdbkhrP40P4+b6DhSSdk3o1NCQ/G
P01HfVna9diWNUb35TsUy067EsNpNF1bAJ4/3/e46+h8JxSiD97umeFDeNEC00JA
0PcKX7x6kdFYZ7StiQWIgkK81XrSv22vjdrHAUx0FP2m8mgknWr0TEFRnvAZdYem
qUTR6g+eqq6+H9cE+VYutjzStfx5b8y34VER6SmqH09yBggTG82zYii0o5d2qmbE
riuRHabQEt9ybAeY4BjaBR/o3iH2G45KVvUOp1vXvAoGCcgzCMHqRC1z0ZzcD03
fXD2LSPHqf4IcqQcPetejTSiLjdzjkBsw8EZBCfEtZN3/BFyZRM7giilL4qLb6dM+
p4yzwC2qHe8g1AFhUx9BwynN8iSRgBQzCIgA6A8kdXXwWAGJCygs3FUKZ4mB00LR
YxElYI9ga0BifFW0mdmLauNc3Lc9zORmd8X9vjLsEWcY5vQWQ1Ao/Yfj5cdBf31S
jrDwKQf0B+Het9Y64x9wHrzsTyF337+PPVtw6PIru52GBk/Zcn/sCMmgcS4R7igf
eIyWagLmtwKr1ZRGb8KYyElMDM5gT86ptGJyoyAhRz2dlvuHBXuxYZP1IAg1Rtql
0+rj/0d6b0ZfJW8fLhba957Gf0xL1dXuuZIMqyJ+y0K20rsVWYsR5hE4kXqXghs
aIZFbIsbSIfhRZopjKlUuVx6IPrcQ3qMmw1hnmGTTmDR/N9GRae80u1QmWkexdw
VzPflEjb2gTpBhNTEFvP4KePmBoKtFVjfs0F+0ezE6aKDr1RID0ux5k1HgpS1gMP
CKFJmgCs07bKgnWiAYgEiYKIocXmvJA0Znz1XVuly6XxZk+SHqUggDnINxKusWwy
a+SrV4vgeQWS3qTFGvTKRGURfygPergdA2h/Ra9VSJVARv08Ifo9e/H6kCq/ZaaM
qJoXVKRUp4QRtHdEV3e2qUcGBS00EG1xEPNBT9kp1RHnGzQGKDPQGTpeSwkZrVzP
NAW+cgRaCq3ebuGWZYddUpRH6cUhv9+/GYxA+g2LntKu1544vmar+96nVjLkscw6
Ely1/xc4q5ADYEErCjgJTx1bGBH/lKdHGanC0JVKld+sIm1XGy2BVAzR+fcYSAII
Z8WkZcu/Xkv3pVYIx/tnl8Lx8kktJltyxkm482hUnzZy208knv61Jr+BbzkvMv9D
mQJpjowogQ79tLqaJVuJtFm9IleTMRLiMxQ07TgHpd6GTpy60SUks/F3Yn4ZY0a5
51PDfuqK6yB54qXjCCGKuRwji/z2B+qdE+hL8RCUXB1Kfr5Cvs0SpNKn4ccFrVaa
SX418VQHS1JZtwmRVeyX5LuCznF+g+vnng6h+fwGqzVLU4napv2IdU0ULxSB3eU
sWEzhcI7JRUsyg0EeseQ/0N8WydYwYU8CSGmygTPf19SI0ojZowc8dZ1yaU037GP
/Y+707Ly0HZXxheMVBomZTenvyfhRsHniXNgYRIRkL3YSCVmh1oTN+IOXoLYxWVK

pHhz0se1v4Tcy9wPzKdM0h/YB11LLyskl6vXElLo45jTFpUr8SQ10IxH8eeeUfw8
PJ6yfu/w8gwk6R2x9VbJTrYHuI451oKNZ89jHhhPH1x+PDj0V3ugKabNM0JD9u1G
t5fN+kFz8A3jKMAtkABHHFmBJD8Y1lmRPazRSX8EF7hvtU+YgIc2z5yULwny2LWL
VTRQyGoj/NDdRRt9MsPf0ZBLvVBPHcJWdWY4kLQDPCE5CrH8F9fsIuh89icDUMUP
y0jI7rCydpcJdv0v65SSscf63MRdsZvYw0m1JgRdSqki8e+qy77o12qXw5eTeIV
7T+YWRb051WuV0Z0JPv7tu3rdTCGs1sTAe1FISU3AzrB9fNG5eHNmPnjZ1yq0lpL
J9BXVvNmWN2cVLutEfimcVRW/aeWuY3+HgSMH0hiqR92mRN6VY6PbdQ+rT914fUz
Vmy5LIN/kZjdeizQyTdgfrRG9pGDEimdlPPia5nCxCwGqXkGPezjzNEWzHo/C4W
knfRMJpMbUJqZVe5u0SE466nh0KIF8nmR2fMzYYpnayCsJoh0AgghIAh940FGz/T
Fp8hKykir4JuzspCI43sGwqZFVICfG0EtisIjZhPUn4VTvxdXsjMoC8ebVUpiMsw
/IihAFjMc5GdU5bP/F2oHiRh+B4e80nSTdzS7PXb6tZ1g7ccazZ5ezp3rE0c5Q0X
yJ/UBiy29VmvLNPV5JBsZQdqC0kOHfz5zqXqnZLdp9XjuW/DD4uahd/t7fWkAjK1
IN820m8GTMjrKSblbvSHRXXQk4sDC7+4K8a6M6hcDXZ51ggDdJkqgGDeyoquA2Za
+AX0XQPozqryfKggqqLL0kmBtfz5PJzDkgXof1VrbslAjQ4VsFjsIKeb4igc3IcS
snPjPC0ujVK/UpK0nci30yo6EreEsxvRml1jUZ2NZycdJ+qGxL9hK5GwfqFxDp
6eqt5X/bHLs+BK5R6G7qZRgk11zsMI+OLj9wkNRf65yxdWiRE0/+0gewAX1sWbxI
soA6zPzvjk1hnz+r0Hnip/ak+QIcdEBMWfUIpJXd92MW57IH5g93CL62v0/w2Kom
AoBVbHsbzFj97vbc6umT2CTM1F7NS4Rxb8xvuwgLaK11Li9QBhMcm47u1l84Jcuu
3IW6nC1v8SH77deDefBYZQJaeBH1HiBoC5Md1LgWP2EKYPEACnn0oPXW4h0jBRT4
yNVviniI7/4Pwdux39cDeXg4GbM3FDRTD/4srBF02p19A9UsADNE6h83bCBTrZXb
9SNeObOhZ4sVXQ80fj7rr5oI8NmcFeI5wcogypd9esWitWGcE5i5wC+3n9nuFvft
X8yOkEDXwDzR8qWgG1rl6A6JZnCL1N2fYJHki0pu/NuFDCCXrlA4tvI8/E2ZmYy7
PtcEuz0NmKxK28pxKXleGX07ioVVMY6iHhEtGuotiFXjt6USG66KenDcXXRSle+0
T3ICsHy7b29G9D6ZKxgPA2K10a8oTvvaea5ptclHchK5WCyRcvdpoei1Vz75K52p
HThqwLkRD7blE/iIva2R465ghWQLV/lc6L4jPIX6YQXE+uLt5TWQkWZ4gNsBVKds
KMgUQdy//yqmxxjImRsB/3wVcp947Y0zbuQNKHH4Yn2cfsofnuWQRN600glCtX7i
HH1WTu4d16i2oDzWkgBhvfGJMwRFxfytdVc2AaHeBvzTsItyW6dV2YkX/P3C51e
8zTSzM/+ZLF02Mg+kY0+GUaJohjx06dt45xKSbUYq4beE22VVZ0440buDgNPv7by
dp86PRFz7yLNKvglQd3XFg3EtQsG2YlS5TpGHqQe2ZxY7inlfzdnktxYAfJrXwkb
LGLVPNM00ipwTpPnAASHzwy7630X/Lh50u7MT2B7C08tCihanl3gQqvZvQ7ufNUF
3edpbAkvv23lVXIMPFCssgMpGFFnG9NogqXHJc5PzTESr+p7QuH+gvySHvYYkulh
w7ZtNiBBd7qu6ire1igXaYN0gVizoIyDintGWxHTaL6fN0AYf2CJRzvragn03t86
IkVistrRakh2eyZlwmG84wN4Vuj7dNARVcyK1HTIiz+zjReh2ouRW6ZMw4SVA5Fk
dUlQAHMmM4NG+BSEk8qxIG02VXkaD+Bw9Z9oLcjE2lRfxc5QYc0smUD41m/dqbs8
kDYc8I10Nlf19073hZmAvqpDSIO/R20F6v2rHpxRGgoY3GGz3vz1U+sAzwCdT25A
rqPwwAIS3ocPUXbzbX2BpoItIhM9GR+zy0DVxZ8rdGuiskRNaa67lZesn3yTHth
3firVDH9ASlmKYJ7Igf/51Ms2KNm90x5794cE4KJG6k6I2exALrWJXEjdm+A2br3
08kfgY7mi6PrkKyFLdTx6m84bSkuIstdfXvq2rrdS1eTqmEppIEuSx5i34L9A1Y8
qMiUbQUpThLhoQ0fdfrKAAdJRPEYH8nn2yoiZnmEKaH3N97cRiYDZLa/YBZXGnny
06uh3wezJRYa9QpSQH5mubiNC1fBoHzHGQEYTEZUaYJqqjAc4bx3yyacYnFTEPtX
mOT2S4o9Pz32f6wv0BT6xJz0FEMoh25gURmymISZKMU1pFePNNTmmP6x1K4pI2Pi
VAJUuyS70ARKdnjKwciPFU7VB4JubPvsd0TpihU4MzngSuohAcUhvRFYDNB7CwgU
igyOSURUVw0RnNslCSJxnalxpenfouN6vfUe48wk0tq/vGnJkiepuyuDm7b+q00Y
j3iTqIJYVDlo9sNj1zjFN7T/zWgu5w32TU70eJ82PpBtj0FgWyaSi8dQGZgf4oxT
0hMKjRQAXPJs9f/NZzrR80oa04EZrTGoYu4+T97e5S19iyxKD4clciqsLVAPISbh
BgYR+K6yHPT86vhql4d0rg07l9DYt3G1RiDhRCe12YA5iuNBBF2Wxbt5wZl29cdr
PFmHJvYg+jIC37UYBw9qv2ABsUI8AUJc8gMqvylnIuillwBPz4hYfo/AAyZe+o40i
cKwLe/UamiqdfPOVQeeN/BkXXaqr2EPDKUSeaShDrui+VKTVgKbJDbImWJjdjQd
6ugnYd3ahi8Zk3+v6Taz0a7ZUtnGqvarOX6S4EH+h8H+CnLyu0Pron5wJIssCMD2
cNDVB8a/n26EiQUg+fsakGyCIEqin5nSSdzgBlDiM0ghav5onizmKyqxHtHjZvRP
/1tGNaoYDwgfSDycM5QGsMD4JUFmozQ/NZsNeGfJEjyZpsI4v64jzcs4QxEbJoDP
/K8v9kiCQZ3NtkHGDRcUBWNBdKij8wgOPA JMhweFIA6UnHoqJdbPzNwsAAjMVN2Z
vtvsfFtuDu5BALHyKAlf67WbdKfFYqfktnmR2rPXa5U/3WWiS6cOLly6h+cseQvS
bPn77hbn6y2tRQ0IMstJ7pBIlim6m/duKc7PZz1u/tANP/gKkHzhthMyAErE0PmqM
PlfvT8ju0UpwGpiF1T1E3SRodx5/q8NV6TSKANWeKN7nahusiB5CV02Ec1hjATXR
XmPo08kyxwYYK7P+oBOXS2gM/uZy3If5hIEfmxxJ+5F19cNiotTQwJM7Jmbag10
MtW7IWC7g+sDYln9L8hCxnCjoh331ss7c3470XB9pTy8EBnRdX5IRW9QuoRcMcZw


```

r2inC0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVt1
uLi hne0Bp1GUTkr0mJBol g6dSYa18Hw8/ANHpyEx156BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80l1h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vR
hZjVD6FYMIIDzzCCAre gAwIBAgITN0EFee11f0Kpolw69Phqzpq1zANBgkqhkiG
9w0BAQ0FAADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQMLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGx1IEExBTBVTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcm10eTA
Fw0x0TEwMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAAGA1UEChMESAUVU
RjERMA8GA1UECzMITEFNUFNgV0cxZzFzAVBgNVBAMTDkFsaWN1IExvdmVsYWN1MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pd0/KLPzBJOAER0sI7Aja07B1GuMUFJeSTu1amNfCwDcDkY63PQW1+DI
Ls7GxVwXurhYdZ1aV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
N012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAelqzJOMayCQtwS1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSebwWXLJe3VMvbvQj0BmpEYlaJBUIKk01zQ1Pq90njlsJL0wID
AQAB04GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCAATAB
MB4GA1UdEQQXMBWBE2FsaWN1QHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAWQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCACAEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
J0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukYr7agyHahIXRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9Eiae6aCHHBh0iPU7IPkazgPYgkLD59fk4P
GHnYxs1Fhd06zZk9E8zwlclALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAAGA1UE
ChMESUVURjERMA8GA1UECzMITEFNUFNgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydgG1maWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsQsGSib3DQEHATAcBgkq
hkiG9w0BCQUxXdcNMjEwMjIwMTcwMzAyWjAvBgkqhkiG9w0BCQQxIgQgXYQxbGVS
YbD1RRYrYjMaj8vm0wJceMeGDm9qv/JsQlgwDQYJKoZIhvcNAQEBBQAEggEAbtxK
BK0ie88UC9KGR0/nHIWpXJOnN1/tXtEwsLoypwYiw8XKgcN8zgZ06RikcGX12ijW
Gz2wgA2yIRfnzWBvS6zmBc9r37klP8uhB0GgPrPFTtq+GeLn9hUApYQTb20H1SKM
e34oCU7qv0LYfFN0sDlwxkha1X3AAg4QFcUrnLJRkYFWDH6XvxsHNiLznwsF/+B1
uNiPIi7rhKgG3oLYu4H8qGolM5H+gy17+h4t8hUHZVTxZ6QyT00K+D2J08aazcor
PgJsa85BUfcx0JXs6xcqtLzTafsPOAQB11CUHEied1qX6nlMb2gCXP6psFEXPRGM
rxSLzwv5QtKJCaDfYw==

```

C.1.8.2. S/MIME Signed and Encrypted over a Complex Message, No Header Protection, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="508"

--508
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="804"

--804
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex
message.

```

```

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no header protection.

--
Alice
alice@smime.example
--804
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no header protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--804--

--508
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUheUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xBA
MAgS739nO3TpRw20dqpbfARQejOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--508--

```

C.2. Signed-Only Messages

These messages are signed-only, using different schemes of Header Protection and different S/MIME structures. They use no [Header Confidentiality Policy](#) because the HCP is only relevant when a message is encrypted.

C.2.1. S/MIME Signed-Only signedData over a Simple Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft.

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 4189 bytes
  ↓ (unwraps to)
  └─ text/plain 233 bytes

```


Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="signed-data"
Subject: smime-one-part-hp
Message-ID: <smime-one-part-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:06:02 -0500
User-Agent: Sample MUA Version 1.0
```

```
MIIMEAYJKoZIhvcNAQcCoIIMATCCC/0CAQExDTALBglghkgBZQMEAgEwggI5Bgkq
hkiG9w0BBWGgggIqBIICJk1JTUUtVmVyc2l1bWVjogMS4wDQpDb250ZW50LVRyYW5z
ZmVYLUVuY29kaW5nOia3Yml0DQpTdWJqZWNoIbZbWltZS1vbmUtcGFydC1ocA0K
TWVzc2FnZS1JRDogPHNtaW11LW9uZS1wYXJ0LWhwQGV4YW1wbGU+DQpGcm9t0iBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NC1RvOiBCb2IgPGJvYkZbWltZS5l
eGFtcGx1Pg0KRGF0ZTogU2F0LCAyMCGZWIGmJyMSAAMDownjowMiAtMDUwMA0K
VXN1ci1BZ2VudDogU2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXB1
OiB0ZXh0L3BsYWlu0yBjaGFyc2V0PSJ1dGYt0CI7IGhwPSJjbGVhciINCg0KVGhp
cyBpcyB0aGUNCnNtaW11LW9uZS1wYXJ0LWhwDQpTZXNzYWdlLlg0KDQpUaGlzIGlz
IGEgc2lnbmVklW9ubHkgUy9NSU1FIG1lc3NhZ2Ugdm1hIFBLQ1MjNyBzaWduZWRE
YXRhLiAgVGHlDQpwYXl5b2FkIGlzIGEgdGV4dC9wbGFpbiBtZXNzYWdlLiBjdB1
c2VzIHRoZSBIZWFKZXIgaUUhjvDGvjdG1vbG0Kc2NoZW11IGZyb20gdGhlIGRyYWZ0
Lg0KDQotLSANckFsaWNlDQphbGljZUBzbWltZS5leGFtcGx1DQqgggemMIIDzzCC
AregAwIBAgITDy01vRE5l0rOQ1SHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0w
CwYDVQQKEwRJRVRGRmREwDwYDVQQLEWhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1
IExBTBTB1FJTQSBZDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgaFw0xOTExMjAwNjU0
MThaGA8yMDUyMDkyNzA2NTQxOQ0FowOzENMA8GA1UEChMESUVURjERMA8GA1UECXMl
TEFNUFMgV0cxZmFzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAmPUp+ovBouOP6AFQJ+RpwP0DxxzY60n1lJ53pTeN
SiJlWkwTww/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+Ithj
LeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/N
kug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmsw
qpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQ
ury/zxn1sukgn+fHbqvWdhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwG
A1UdEWB/wQCAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWB
E2FsaWNlQHNtaW11LmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0P
AQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSME
GDAWGBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgU14
oJyxMpwWpAy10vK6NEbM11gD5H14EC4Muxq1u0q2XgX0SBHI6DfX/4LDsfx7fSIu
s8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2Mfbh1Ib3U8QzTjqB8+dz2
AwYeMxODWq9opwtA/1T0kRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gz
nbvhdjFbZbi4oZ3tAadr1E5K9JiQaJYOnUmGpFb8PPwDR6chMZeeGSAW++OIKqH
rg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sNOo2kc1nTX185RH
NrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc0vT4as6aqdcw
DQYJKoZIhvcNAQENBQAwVTENMA8GA1UEChMESUVURjERMA8GA1UECXMlTEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdG1vbiBBdXRo
b3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBTB1FfHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
bGFjZTCCASlWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehY0BY+TZp/
T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwDrRjFBSXkk7pWpjXwsA3A5G
0tz0FpfgyC70xsVcF7q4WHWZwleYXFK1QHJD73nQwXP968+A/3rBX7Ph00DBbZnf
itOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH16syTjG
sgkLcLNaU5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXNde/
N+iDz3X0ze0j0fqXgq4SWcC0nsG1lyXt1TL270I6ATKRJWiqVCCpDtc0NT6vdJ
45bCSzsCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQMA4wDAYKIZI
```

```

AWUDAgEwATAeBgNVHREEFzAVGRNhbG1jZUBzbWltZS5leGFtcGx1MBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIGwDADBGNVHQ4EFgQUu/bMsi0dBhIc
l64papAQ0yBmZnMwHwYDVR0jBBgwFoAUKTCOfAcXDKfXCShlNhpnHGh29FkwDQYJ
KoZIHvcNAQENBQADggEBAH0JoJanzqmgasN3/gqSQ4cbbmdj/R40BEPr+gXT+xiid
fZ2iLWYyTneuK6AChwKfnNvOFb8lV1iffRtF/KtmVEDMR/sYeqAH83KM5p3e12
lVh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVfnbhsp1rWg9NQ2WbpCmK+2oMh
2oYl0Z/wvXmt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj10yD5Gs4D2I
JCw+fX50Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcB
VyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMiIB/AIBATBsMFUx
DTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQDEyhTYW1w
bGUgTEFNUFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/Qqmi
XDr0+GrOmqnXMASGCWCGSAFlAwQCAaBpMBGCSqGSIb3DQEJAzELBgkqhkiG9w0B
BwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MDYwMlowLWYJKoZIhvcNAQkEMSIE
IHBk91pcJj0zJrTyR0H0dfUnQMocTlHVb6WXTpS3gYx1MA0GCSqGSIb3DQEBAQUA
BIIBABWhy/yIy9RLS30dZZTlUNChBhZNHjpSSoL3v0Jmz0HeYJVblzBgpyPU33Tu
JALxlGuGp4yb016yQREHMXNFZJkrqWcIAMZG/4tG7WIHXm0AGIcx18BKKEpnt1m
ki00/NWzFY9TW1pYd/+CC7Q8Asc+S2Nd269HGrFFpL36r74Gt2xJDxn11N3coBh3
khaFt+p5GkqqrNUtfGeo0iff+66x/oW9A/AtNE+iKwx7mEtuk0hBgTXgyr3bi+ev
sEQzWYVLYVS7TCsCM5A1LxHZHv5gVcX1EMTZi7rRaNKKEmUcA9vbJYBSOWlmR/o4
FeLYNUvUvFvXvV9YCb/0R0pgp9Aw=

```

C.2.1.1. S/MIME Signed-Only signedData over a Simple Message, Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```

MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-one-part-hp
Message-ID: <smime-one-part-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:06:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="clear"

This is the
smime-one-part-hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a text/plain message. It uses the Header Protection
scheme from the draft.

--
Alice
alice@smime.example

```

C.2.2. S/MIME Signed-Only multipart/signed over a Simple Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a text/plain message. It uses the Header Protection scheme from the draft.

It has the following structure:

```
└─ multipart/signed 4435 bytes
   └─ text/plain 250 bytes
      └─ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature"; boundary="78f";
  micalg="sha-256"
Subject: smime-multipart-hp
Message-ID: <smime-multipart-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:07:02 -0500
User-Agent: Sample MUA Version 1.0
```

```
--78f
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-multipart-hp
Message-ID: <smime-multipart-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:07:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="clear"
```

This is the
smime-multipart-hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a text/plain
message. It uses the Header Protection scheme from the draft.

```
--
Alice
alice@smime.example
```

```
--78f
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"
```

```
MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCcC0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECxMITEFNUFmgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQUU1QUYBSU0EgQ2VydGhmaWNhdGlvbiBBdXR0b3Jp
dHkwIBcNMTEwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTA5MDsxDTALBglghNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTBVTIFdHMRcwFQYDVQQDEw5BbGJjZSBMb3Z1bGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBABJqVKfLwLjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLoAJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
```

```

B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAAQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRnHbG1jZUBzbW1tZS5leGFtcGxlMBMGA1UdJQQMAAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdW8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAlFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRy0g31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUv2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKGd7QGnUZROsVSyKgiWdp1JhqXwfdZ8
A0enITGXnoEkAFvviCqH64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBAQUAMFUDALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTBTIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFNUFMgU1NBIEENl
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqeHEFbZfKB4urMk4xrIJC3CzWruS2Q0FHbB1fkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAAGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETyWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFvL2zLiThQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHfWyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjD/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/Nyjoad3pdpVYEDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JCKzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpp1zALBglghkgBZQMEAgGgATAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMbWGCsGSIb3DQEJBTEPFw0yMTAyMjAxNTA3MDJa
MC8GCSqGSIb3DQEJBDEiBCAIw1Q7hUXhrDaz3LXMFp0A3q3nvlhWh9ejLg/g9kjk
vDANBgkqhkiG9w0BAQEFAASCAQAc10M6ZwFazFvsP+/siWSN0EM0YWxu0zvCmSWC
0QwnAQ/dSwXcKMcej0wWMKTDTSYBUjxFVE0chcK6FMH2gHDVb/PztWrSECmvh6F
utJ2SRxs0uGrFkee3hR0kowu0u9pDXasLtWP2MnB5pSMWX5QMpya1UxYcbIoaU0x
Jeu5zjbYf/0o2tINvZHP+r+wxQZ7qTaEzviQ+IV0KoJanfU3Qd/giS6MuySwozP
r3E7YAy309dZT7zL6AR5CsC1I0coo7X1PRNnBXXLMecR/v5cXniGV+GNf8xYaiGA
iT9IwiJZa6psfTSFjzUWTic0jGx3GcLzr+BIm+MEBCSRzDum

```

--78f--

C.2.3. S/MIME Signed-Only signedData over a Complex Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 5647 bytes
  ↓ (unwraps to)
  └─ multipart/mixed 1570 bytes
    └─ multipart/alternative 934 bytes
      └─ text/plain 287 bytes
      └─ text/html 382 bytes
      └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"
Subject: smime-one-part-complex-hp
Message-ID: <smime-one-part-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:06:02 -0500
User-Agent: Sample MUA Version 1.0
```

[illegible]

```

DQotLWUyZS0tDQqgggemMIIDzzCCAreAwIBAgITDy01vRE5l0rOQ1SHoe49NAaK
tDANBgkqhkiG9w0BAQ0FAADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBVTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTagFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMASG
A1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIEExv
dmVsYWNlMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBou0P
6AFQJ+Rwpw0DxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8g0UH/CVt2Zp
1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6h
AQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXj
WShp1cI3lcvvBZMswt41/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2
lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvWdhJLAfPw/jA/EB/
WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBggp
hkgBZQMCAATABMB4GA1UdEQQXMBWBE2FsaWNlQHNTaW1lLmV4YW1wbGUwEwYDVR0l
BAwwCgYIKwYBBQUHAWQwDgYDVR0PAAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyA
KRV8ASpW546vzfN3DzAFBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTAN
BgkqhkiG9w0BAQ0FAAOCAQEAU14oJyxMpwWpAyl0vK6NEbM11gD5H14EC4Muxq1
u0q2XgXOSBHI6dFX/4Ldsfx7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZ
ncxGwy2MfbH1Ib3U8QzTjQb8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuivZfg/m5fF
o/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR1E5K9JiQaJY0nUmG
pfB8PPwDR6chMZeegSQAW++0IKqHrg/WEh4yiuPfpmAvX2hZkPpivNJYdTPUXTS0
7K459CyqbqG+sN0o2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQIC
EzdBBXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMASGA1UEChME
SUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBS
U0EGQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1
MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExBTBVTIFdH
MRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFiZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0w
I2juwdRrjFBSXkk7pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZWIeYXFKlQHJD
73nQwXP968+A/3rBX7Ph00DBbZnfItOLPgPEwjttdg0VQQ6Wz+CRQ/YbHPKaw7aR
phZ063dKvIKp4cQVtkWQH6syTjGsgkLcLNaU5LZDQUdsGV+SAo3nBdWCRYV+I65
x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fQXgq4SWC0nsG1lyXt1TL
270I6ATKRGIWQVCCpDtc0NT6vdJ45bCSzsCawEAa0BrzCBrdAMBgNVHRMBAf8E
AjaAMBcGA1UdIAQMA4wDAYKIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBz
bW1tZS5leGFtcGx1MBMGA1UdJQQMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIG
wDAdBgNVHQ4EFgQUu/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0jBBgwFoAUKTCO
fAcXDKfXCShlNhpNHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgasN3
/ggSQ4cbbmdj/R40BEP+r+gXT+xiidfZ2iLWYyTneuK6AChwKfnNv0Fb8lV1iffR
TF/KtmVEDMR/sYeqAH83KM5p3e12lVh40HhyI0qNuz50ShNaACsioQ23WxHGvy9v
sdVfnbhsplRwG9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0IOvg6mrYkK
TM/RCGnumghxwYToj10yD5Gs4D2IJCw+fx50Dxh52MbNRYXTus2ZPRPM8JXNQc4G
Wv4km3M4rKnJdD6hnoQ9rNeozIcBVybyQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s
1LM2cSYxggIAMIIB/AIBATBsMFuXDTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExB
TVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NBIEU1cnRpZm1jYXRpb24g
QXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+Gr0mqnXMAsgCWCGSAFlAwQCAaBpMBGg
CSqGS1b3DQeJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3
MDYwMlowLWYJKoZIhvcNAQkEMSIEIGbRm8jphDRUXRWIk4vxhAup+YZsmtrednWv
3iPoigWSMA0GCSqGS1b3DQeBAQUABIIEBAEHG833PIy7iky90k2pN22fjSF6xtjlt
h1Pi4Eh9PSjQ5Rdrsv9pJFFsBhSLOXv+08fwYfS1rUrgwsCVM064zz5MT1Kj4Y4Z
a6ztE9weXTlciQyd0WER6lV1BDP4GwUaz+BBCoKKB0DTHq+nPNo97XtTCUfo55Vz
55vmNXxqWQ952hzw+qxxTxKzdYApFd9cZYzvV4otZgtvZDu3sn6GWFCtVpN4+6TR
xClE93q+LZwvJyXFRFWHcKqUfQ16ZAomBadrJ1RU3BmRXn6DAI/J/yhm70egdN
00r/+EuyWAZp0r/GCsSGXt2owaAkGPuZf6kPc0mLhb/VFdeY16wy9J0=

```

C.2.3.1. S/MIME Signed-Only signedData over a Complex Message, Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-one-part-complex-hp
Message-ID: <smime-one-part-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:06:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="e2e"; hp="clear"

--e2e
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="200"

--200
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex-hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the Header Protection scheme from
the draft.

--
Alice
alice@smime.example
--200
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex-hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the Header Protection scheme from
the draft.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--200--

--e2e
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQejOywiwYnCtxDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--e2e--
```

C.2.4. S/MIME Signed-Only multipart/signed over a Complex Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft.

It has the following structure:

```
├─ multipart/signed 5520 bytes
│   └─ multipart/mixed 1628 bytes
│       └─ multipart/alternative 990 bytes
│           ├── text/plain 304 bytes
│           ├── text/html 402 bytes
│           └─ image/png inline 232 bytes
└─ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature"; boundary="ba4";
  micalg="sha-256"
Subject: smime-multipart-complex-hp
Message-ID: <smime-multipart-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:07:02 -0500
User-Agent: Sample MUA Version 1.0

--ba4
MIME-Version: 1.0
Subject: smime-multipart-complex-hp
Message-ID: <smime-multipart-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:07:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="b14"; hp="clear"

--b14
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="f1a"

--f1a
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-multipart-complex-hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
```



```

signature (multipart/signed). The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft.

--
Alice
alice@smime.example
--f1a
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex-hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--f1a--

--b14
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGGoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCTkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicHaf5YJrw7vfv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRu5ErkJggg==

--b14--

--ba4
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQCoIIJ0TCCc0CAQExDTALBg1ghkgBZQMEAgEwCwYJKoZI
hvcNAQCoBIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECzMITEFNUFmgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BE1FVEYxETAPBgNVBAStCExBTVBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3ZlbGFj
ZTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAlJqVKfqlWALjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLoAJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYZIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDADBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUkTC0fAcXDKfxCSH1NhpHGH29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfpnc9gMGHjMTg1qvaKcLQP5UzpeYPLror2X4P5uXxaP0LIZR

```

```

zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKGd7QGnUZROsvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSib3DQEBDQUAMFUxDTALBgNVBAoTBE1FVEYx
ETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NBIEI1
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSib3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzys02kaYWTut3
SryCqeHEFbZfKB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFV2zLIthQYSHJeuKWQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSib3DQEBDQUAA4IBAQBziaI2p86poGkjd/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZL
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCafwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTlBTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpq1zALBglghkgBZQMEAgGgATAYBgkqhkiG
9w0BCCQMxCwYJKoZIhvcNAQcBMBwGCsqGSib3DQEBDBTEPFw0yMTAyMjAxNzA3MDJa
MC8GCSqGSib3DQEBDBTEiBCDKNV54rM1AYeFevF+c3DI/JjX14STIx3nsp5B95mHf
gTANBgkqhkiG9w0BAQEFAASCAQBWQxNUY6IG27ju4XS4aApRfPoBUjk6m7uUMIQF
/VCEpXLvWRkn6B9k7L9MMrMJPRKR03oCzimaPjTKH3JKTxdj0gWtb2eELmIaRWY
n0TaAK/3/h2dqMbPXYXgmWRQPsgFs42m6zWF4CH3YpurTvQC5gB0PSEPF0B0Hdcm
77bRs4AcPf1mfGThUG3YUNXuJ99BKb3Zz3lQiTohvti9eHRYAMXL/XdP7TLiGVm
Ee7uoUREekXvLmj8C6B3z8fiTfiWlqENU7J2BkrVF0KgW5X9ANwhekNR0Ex6X05R
NVcBYNKNxCxuKMBHcE47Ytt8AuV4NoDWk2yumc8T6sM0Wkue

```

```
--ba4--
```

C.2.5. S/MIME Signed-Only signedData over a Complex Message, Legacy RFC 8551 Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 Header Protection ([RFC8551HP](#)) scheme.

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 5696 bytes
  ↓ (unwraps to)
  └─ message/rfc822 1660 bytes
    └─ multipart/mixed 1612 bytes
      └─ multipart/alternative 974 bytes
        └─ text/plain 296 bytes
          └─ text/html 394 bytes
            └─ image/png inline 232 bytes

```

MIIQaQYJKoZIhvcNAQCoIIQWjCCEFYCAQEeXTALBglghkgBZQMEAgEwGgaSBgkqhkiG9w0BBBgGgggaDBIIGf01JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVR5cGU6IG1lc3NhZ2UvcmZjODIyDQoNck1JTUUtVmVyc2lrbjogMS4wCkNvbRlbnQtVHlwZTogbXBvdGlwYXJ0L21peGVkOyBib3VuZGFyeT0iZTY4IgpTdWJqZWN0OiBzbWltZS1vbmUtcGFnY2tjb21wbG94LXMJYzgzNTFhcApnZXNZYwdlLHV0E0ia8c21pbWUTb251LXBhcncQY29tcGxleClYzM4NTUuXtaHBAXzhhbBSzT4KRNJbToGOWxpY2UgPGFsaWNlQHNTaW1lLmV4YW1wbGU+C1Rv0iBCb2IgPGJvYkBzbWltZS5leGFtcGxlPgpEYXR0iBTYXQsIDIwIEZlYiAyMDIxIDEyOjI2OjAyIC0wNTAwClVzZXItQWdlnQ6IFNhbXBsZSBNUUEgVmVyc2lrbjoiAxljAKCi0tZTY4Ck1JTUUtVmVyc2lrbjogMS4wCkNvbRlbnQtVHlwZTogbXBvdGlwYXJ0L2FsdGVybmlF0aXZl0yBib3VuZGFyeT0iYmJhIgoKLS1iYmEKQ29udGVudC1UeXB0iB0ZXh0L3BsYWlu0yBjaGFyc2V0PSJ1cy1hc2NpaSIKTUNRS1WZXJzaW9u0iaXljAKQ29udGVudC1UcmFuc2Z1ciFbmNyZGluZzogNa2JpdAoAKVGhpCyBpcyBA0aGUKc21pbWUTb251LXBhcncQY29tcGxleClYzM4NTUuXtaHBABWVzcFncZSAKCLRoaxMgaXMGYSBzaWduZWQtb25seSBTL0J TUUGbWVzc2FnZSB2aWEgUEtDUyM3IHNP251ZERhdGEuICBUaGUKCGF5bG9hZCBpcyBhIG11bHRpcGFydC9hbHR1cm5hdG12ZSBtZXNZYwdlIHdpdGggYW4gaW5saW5lCm1tYwdlL3BuZyBhdHRhY2htZW50LiBjdCB1c2VzIHROZSBsZWdhY3kgUkZDIHg1NTEGaGVhZGVyCnByb3RlY3Rpb24qKFJGQzg1NTFIUCkge2NoZW1lLGoKLS0gCkFsawWNlCmFsaWNlQHNTaW1lLmV4YW1wbGUkLS1iYmEKQ29udGVudC1UeXB0iB0ZXh0L2h0bWw7IGN0eXZjZXZxOInVzLWFZy2lpIgpNSU1FLVZ1clnNpb2VhIDEuEMAPdb250ZW50LVRyY5ZzZmVyLUUuY29kaW50niaA3Yml0Cgo8aHRb248aGVhZDI4dG10bGU+PC90aXR5ZT48L2hlYWQ+PGJvZjZhK+CjxwPlRoaxMgaXMGdGh1cjxiPnNtaW1lLW9uZS1wYXJ0LWNvbXBsZXgtcmZjODU1MWhwPC9iPgptZXNZYwdlLjwvcD4KPHA+VGhpCyBpcyBhIHNP251ZC1vbm5lIFMvTU1NRSBtZXNZYwdlIHZpYSBQS0NTIzcg21lbmVkrRGF0YS4gIFRoZQpwYXlsb2FkIGlzIGEgbXVsdGlwYXJ0L2FsdGVybmlF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUKaW1hZ2UvcG5nIGF0dGFjaG1lbnQuIEl0IHVzZXMGdGh1IGx1Z2FjesBSRkMG0DU1MSBoZWFkZXIKHvdGlvjdG1vbiAoUkZ0DU1MUhQKSbZY2h1bWUUPC9wPgo8d48dHQ+LSoGPGJyLz5BbgJYLZTxici8+WypY2VAC21pbWUUXzhhbXBsZTWvdH0w+PC9wPjwvYm9keT48L2h0bWw+CiotYmJhIJS0KCiotZTY4CkNvbRlbnQtVHlwZTogaW1hZ2UvcG5nCKNvbRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IGJhc2U2NApDb250ZW50LURpc3Bvc2l0aW9u0iBpbmxpbmUKCm1lQk9SdzBLR2dvQUFBQU5TVVhfVWdBQUFCUUFBUQVFVQ0FZQUFBQ05pUjBOQUFBQWNfbEVVRVl0MnVWVE94YkEKTUfnUzc20W5PM1RwUncyMGRxcGJMqVJRWPpPeXdPd1luQ3RRREtuYmNMazY2c3FsVCt6dDljaWRrRs2S3drWgpzZ3J6ZmNxVk1wTDJqbzA0NDdnWURwZUFayytBPbkIa0l0QWZUUFJyY2l0QWY1WUpdydz2anYwWldSV00vdWxpCnZKUERGxUVoya0RE0XhwGQ40FBQUFCSlJVNUUYapa2cn2cPQ0aKLS1l1jgtLQqggemMIIDzzCCAregAWIBAgITDY0lvREF5Sl0rOQ1SHoe49NAakTDANBGkhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRMREwDWYDVQMLEwhMQU1QuYBXRxExMC8GA1UEAxMoU2FtcGx1IEExBTBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcm10eTAgFW0xOTExmjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOZENMAsgA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxZzAvVBGNVBAMTDkfSaWNlIEExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQMIIIBCgKCAQEAmPU+ovBoOuP6AFQJ+Rpwp0DXxzY60nl1J53pTeNsIJlWktw/cxQq0t4u2svWYB8gOUH/Cvt2Zp1c+auzPKJZ2afH5mY6kHm+hVB+IthjLeI7HtgbrNeuXq50/TdTsx5XR1IEXGT8ph6aueVA5oZ2afHg4b97enV8gozR0/Nkuq4AkHmbk7THNc8vvjMUJanZ/VmS4TgDqXiWSHp1cI3lcvvBZM

```
wt41/0HJvSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5
chWfNEbkN6hQury/zxn1sukgn+fHbqvwDhJLAGFpW/jA/EB/WI+whUpqtQIDAQAB
o4GvMIGsMAwGA1UdEwEB/wQMAAwFwYDVR0gBBADjAMBgpghkgBZQMCATABMB4G
A1UdEQQXMBWBE2FsaWNlQHNTaW1lLmV4Yw1wbGUUwEwYDVR0lBAwwCgYIKwYBBQUH
AwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3
DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0F
AAOCAQEAgU14oJyxMpwWpAy10vK6NEbM11gD5H14EC4Muxq1u0q2XgX0SBHI6DfX
/4Ldsfx7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U
8QzTjQB8+dz2AwYeMx0DWq9opwtA/LT0kRg8uuiVZfg/m5fFo/QshlHNaaTDVEXs
U4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR1E5K9JiQaJY0nUmGpfB8PPwDR6chMZee
gSQA+W+0IKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o
2kc1nTX185RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc
Ovt4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAAGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFUMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1UyBSU0EgQ2VydG1maWNh
dGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTha
MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDQVQDEw5B
bGljZSBMb3ZlbgFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0
iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwdRrjFBSXkk7
pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZwleYXFK1QHJD73nQwXP968+A/3rB
X7Ph00DBbZnfit0LPgPEWjTtdg0VQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQV
tkWQH16syTjGsgkLcLnau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxxqmqjV3d/
2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJW1QVC
CpDtc0NT6vdJ45bCSzsCAwEAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBGA1UdIAAQ
MA4wDAYKYZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxl
MBMGA1UdJQMMAAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
u/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTC0fAcXDKfxCSHlNhpN
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgaSN3/gqSQ4cbbmdj/R40
BEPr+gXT+xiidfZ2iLWYyTneuK6AchWkfnNv0Fb81V1iffRtF/KtmVEDMR/sYeq
AH83KM5p3e12lVh40HhyI0qNuz5oShNaACSioQ23WxHGvY9vsdVfnbhsplrWg9NQ
2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0I0vg6mrYkKTM/RCGnumghxwYT0
j10yD5Gs4D2IJCw+fX50Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDD6h
noQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMiIB
/AIBATBsMFuXDALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYD
VQQDEyhtYW1wbGUgTEFNUFUMgU1NBIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5AhM3
QQV57XV/QqmiXDr0+Gr0mqnXMASGCWCGSAFlAwQCAaBpMBGCSqGSIB3DQEJAJZEL
BgkqhkiG9w0BBWewHAYJKoZIhvcNAQkFMQ8XDITxMDIyMDE3MjYwMjUwLWYJKoZI
hvcNAQkEMSIEIPo6cfj2PNIuP7W8SRv7KpxepLUu9zPga1LeN0BNuSo/MA0GCSqG
SIB3DQEBAQUABIIBAB012cJS02iaJg5nB/+gal+wZn3h0P1WW6n8YQ957q/TxIj
Iny59ctj4CokVarB3uAm50r1TpK1h1x/hse1MsZgWQ0ew+omUQqKJg3RLZ9R8wsv
0l8SN5WMNDiNSRNC9a3MFtSVPEOCT90XdQdQ2kqeRkL/fthatcF8gI+p4+p0P2+U
d0fnKCjP9nPobyBcXkljv0pRriu7snqQi100I1aqd4VwocIm8YV65la0/9522f6e
/4Zi30oBLuIz1+pT2z6frPzUJfd6UbGtSiAwRHyfIJHZ2PAYt94iMv7U0VmK3GmJ
TkzFm1if4dpFLofdkEtUX8Is+DPf+/ZB1MvrrQk=
```

C.2.5.1. S/MIME Signed-Only signedData over a Complex Message, Legacy RFC 8551 Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="e68"
Subject: smime-one-part-complex-rfc8551hp
Message-ID: <smime-one-part-complex-rfc8551hp@example>
```

```

From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:26:02 -0500
User-Agent: Sample MUA Version 1.0

--e68
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="bba"

--bba
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex-rfc8551hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the legacy RFC 8551 header
protection (RFC8551HP) scheme.

--
Alice
alice@smime.example
--bba
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex-rfc8551hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData. The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the legacy RFC 8551 header
protection (RFC8551HP) scheme.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--bba--

--e68
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQejOywiwYnCtkDKnbcLk66sqlT+z9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIHafTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--e68--

```

C.2.6. S/MIME Signed-Only multipart/signed over a Complex Message, Legacy RFC 8551 Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 Header Protection ([RFC8551HP](#)) scheme.

It has the following structure:

```
├─ multipart/signed 5624 bytes
│   └─ message/rfc822 1718 bytes
│       └─ multipart/mixed 1670 bytes
│           └─ multipart/alternative 1030 bytes
│               └─ text/plain 324 bytes
│                   └─ text/html 422 bytes
│                       └─ image/png inline 232 bytes
└─ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature"; boundary="a61";
  micalg="sha-256"
Subject: smime-multipart-complex-rfc8551hp
Message-ID: <smime-multipart-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:27:02 -0500
User-Agent: Sample MUA Version 1.0

--a61
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="91c"
Subject: smime-multipart-complex-rfc8551hp
Message-ID: <smime-multipart-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:27:02 -0500
User-Agent: Sample MUA Version 1.0

--91c
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="b87"

--b87
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

This is the
smime-multipart-complex-rfc8551hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 header protection
(RFC8551HP) scheme.

--

Alice
alice@smime.example
--b87
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

```
<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex-rfc8551hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed). The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 header protection
(RFC8551HP) scheme.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--b87--
```

--91c

Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAAcElEQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQeJ0ywiwYnCTkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVmpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--91c--

--a61

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGhmaWNhdGlvbiBBdXR0b3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTA5MDs0DTALBgNVBAoT
BE1FVEYxETAPBgNVBAStCExBTVBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBABJqVKfqlWajj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK

```

arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPtryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKGd7QGnUZROsVSYkGiWdp1JhqXwFdZ8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIB3DQEBDQUAMFUXDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTBTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NBIEEN1
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIB3DQEBQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwOrjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUBYQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqHEFbZfKB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFf10ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEFV2zLItHQYSHJeuKWqQENMgZmZzMBGA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIB3DQEBDQUAA4IBAQBziaI2p86poGkjD/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUaUblR+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsM0GI364IOA0b8PSrJntjh+AjQJ5QfH+0e7NSzNnEm
MYICADCCAFwCAQEwBDBVMQ0wCwYDVQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpq1zALBglghkgBZQMEAgGgATAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCsQGSIB3DQEJBTEPFw0yMTAyMjAxNzI3MDJa
MC8GCSqGSIB3DQEJBDEiBCAYyptCVBhIbJLh1Q0KunV/81vEiJSGLmos08/AoumM
FzANBgkqhkiG9w0BAQEFAASCAQCSBg1wkJFZNTXSwTdjldQxDo4n3twmJl9VyZS0
Al00EiVW2+9Tqu06G+mTSePraLq4L2BvutQ1rKW9jVXJXJ8klx3Y8aY6TGvJ5/RH
3GpwQPjffjauEVAplxnIeLdtUbwJJaColBr6bPHUibtvXS14JqfHvEu7uTgHlpxv
KFZ/VEXf+Lx62gINfpie22d6UC3NxiF6EwPEDLmIjOYILjfmf9McQ2KzAPr6t6x/
hrz6NDG3LeTeLegQ4+onLotaBFsa0QPat0nSFjcaH8j9hFb4RB4avMbT1/5nRR6/
B49Y028fRuAztMvesvs4M8kW6DAJjYj2fFAgT87CdWErzM7r

```

--a61--

C.3. Signed-and-Encrypted Messages

These messages are signed and encrypted. They use PKCS#7 signedData inside envelopedData, with different Header Protection schemes and different Header Confidentiality Policies.

C.3.1. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#).

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 7825 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 4786 bytes
    ↓ (unwraps to)
    └ text/plain 329 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:09:02 -0500
User-Agent: Sample MUA Version 1.0
```

```
MIiWjAYJKoZIhvcNAQcDoIIWfTCCFnkCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFGUjU1NBIElcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAERRjmiJrN88aVGFS2yaskouoeCwZ++b+Xx4
pJQ1bIG5PzkUkiAqDWKhdwAJT+f74rJIneIhgYQkL1NWefgCu07UBT+ciHEBDEhP
+3jciOFRP3Hnynxdw6DpGaUfyk9WnOGjePADIipvHDkRjXWiuuHFCXpQPQthB+
mwYuv6G5Wm9MxHSpAid/UXMkUAYK2zkVMSOdm4BfG9TpmIUqjBm+uo0d3ZjIiCm
wzDMpEEZyZc3Z07jdC7DC1eQBm09co/RnhwpI56kEp2rtQqmRi1waXS3jqHf8EeC
u/X5xskoJlVakhdHteSM0bqJ1v0cNnsSMYbHb3TLQRF+BhPIWt8wggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFGUjU1NBIElcnRpZmljYXR
bXZSbMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAURM6vJvmbdyw0kwK73GhkCBT
DN26jSUwPbZg9MYXICPROANV4oU9gFTF0E/CA4JzCPhPeIyqGA9KHWEpEr9dljFg
HwFIg+jo0VVqa9yHyQ3NvPN9Bmm2fc9JFc9hcj9id/35tEfCV08dUw2KctQaEPKD
OvoJfHrq54FwbCW5u+I/QszuN2U95ggNXg4R3GD3NFgB5vtUPk/hV26H5n0U98Wk
6Fqd76iQbY9Sbq0qxQpDbDcNwdDWYHPDoyuXmmsgGIyCn17PdTcEURrPTCS0590L
oPJy7h8LA9QLd0jg31nF7sXtsJriCIpJ3CFht0fRdi12dVMevhTx3S0cQK1lVDCC
E14GCSqGSIb3DQEHATAdBgllghkgBZQMEAAIEECsb0PK1Byo8Yr3SVUeSGA0AghMw
Kd1hOujWt0vKraLc85HbQ5Lx9Z64dro+3EJj7zNUjPx33hYU+m25DXgdjB+ZsA2Z
1QtUO6MvLqsJKjC1Z9n3yrMc7gsom8PjF2KAia6F9x43EyNv7hagnPvawqKEFPcP
QLF3TTLs12i8rIcn8FwjrdlMqSmVlBIz1dvLD9JKi0KQ4IJxl60jETniZvFZgsRJ
/PXZYzqq7cWoymZrPSX/UksUFR/8pc2AyQR0Ly3JvDZQ+3EykhcXQgRzqtT8TYyN
HB0e+Feo65sjxYQvwmYJJEMRjzercDgAwqYQ3XGroFtDTw+tDjdHIR8/yuXHeWuU
8PxAnaM1QnoZpRvHdIn3zLD6BalgMW98VSGFL54HQL8P60888LxBvstf15lTEyev
EnOUwa6Qx+B777Lzt9n6rvIrJQ5T+rIXBH/U1Rf0QtMxfZC5tSc3Lux5LPDSGdc
c5rM2nh26JCEpoY2FjdrikIJOBK+NUdkyu/mlCmjCF03c7jQm6Q7JFdpG0qmjoQy
gZo8VL4g6gxq0mlaOG+pYK/3QUBAampxn8kJ9zQ2NdVBEjdRk7JD5fqVwa5tZb
RV4IA6bm+mfZzAviibnXI55m6E07wOfHHm/b+KKUmyB17WeKvNm3Z3iTk0tViqun
tZnXjyhVA9fGdwaNYS6njKQSuwQjGmjmltokR0dh6LM0Xg8cgX6us34BHfP0yNe6
HUzXhl0wKLQmTuvbLBQRcNZxVgeSNRvIL/n/08D1Ln3kXJpNL+1WUJZQhBLXVIk
T7Fucb02kDhDXufsJRed/uMizdX6lNHjRF0bGARZp/SD6rn3X+WzJV2BwX8xpEph
iEr6I9hrVDytdoBFsGt/z9FVM04kwp+n6U02ipikVQdKPt1CpsBYkBzwfDaPF0mS
kbwULZhZ1nj3tkAzv9sx5a/z71v92S7LVHDycnUcuvNK4AZB8wZvSXz/8WPxwk30
zmdeeSsn6dyZ5Q9o203Zq6/7k9YhkYD3LDS3XWRkpJmFnmjDL5WEr5ifxVrIq3KM
MAEOs1tqfBMWF4AeA0K0oHa9NAhzLCMSfxNEtXd718Ur2JKkUGxtmCKD/3ep5e5S
```

smIS/Ty3aD47LQYD0kjWhvTnQF61v0vQHRlEKLmf7r1rnAwL2fEwfnMvNZTTiTn4I
nfl1m49CxxzffSv10ECTlKs/RZq7JxcfvuW4qN3yjMKy1dwtRZm9pU5+R0p2Hn9F
C4nZQ4Dre2cPdM1JmvimOnVEyc3703Mi7hF3Nuf7H2j0g4yTMu8Tuk+8J00KukQD
dNz95Bzj89cCb9FJyq5h4Sk+TeVqJzhONpL0Q6f7xrJeJZVefq4RhMMtfFYgNAeZ
/G1f4xHGXFug9okJXFSZCcoLYv4qek50jJrbWM3GeY7l1j9C1xFbs0bqrtBXAImul
60G7uEJdsFR2wBLYv6i9lCwAVKeBSJx6FdfzKzRqsHYUFsMVeNw3kYPbbsXyj3Mx
PLCrB8lP71NHtIEHPkKFgTPvEaVWzXMvz6YA0g6mKxVjI8iVFSE6JBjHtaTX49kJ
w2XXS/eI4DD8y5exJVt1Rb6l/88eh9IiN60UXbUXmtDm/cKnnMD3Nt4H0weIygvU
BHMVw3+p6Uoj/E3lDExSGIX1BTveRZVGz11A0az63UGz18KCz0how+XJrLILJlnH
8MLEF/BarmHe5+09XHF8otp0YPmdhL8RnFfvtStTthxhp2smd5IIBlm13hj1CuV7
KTnVbyBxKX9utmIRmlSy0dvAMR2+jzLoNCUTzWYCu2/IcYw23gW44pFQdUosKmyf
0gyFSNQVQJ+CKADEID9sHwM7yBwKkNEK5jExDn00qyU6B0Wr0i4RYy/J6LrQGMWG
YliQtmyV0fhDjzUATEAGumxVBWbCycDA11DsEp0hSckgowk8aTlXo6tWPeXv5iMq
bCfxUGLY8gmHEf7n+v2yLoCJmZSyTMT0Bh0PjINnNYRWQnsdR+CELSxgmbE651K2
abaYEX/jBZvCvgILPuAHF14WVvHj/BbfMZTfxTRSnjZIKhcP32Bk42WlUo+Hkhtk
sG6xsl614VAqqtRvpDzMK+HsK8YmyCT53d0mb9JEokmu0V4GaMRluaeBGxV88UK
t0tTQB1VZ+/kcSy7SBBuGtNz2kSapRDUjWgXnWDzMDQeMc5rI16WeCRgwVTiRBRb
EWrsrPtG5u/krSm/wwBdd3m9VD0m1Tj+1UoH5+0XeReZjb0se7uQt2W/V/IWpGMy
EK/M/rThL4q8JjY3SNmlzYv9mtrUy+eoFgf+ef0iGSfCynfnK4A12K9LPFvaPnS3
qcTH4FVjuFs4THAfCp5rEoaefUzEY12DBYdLVTNMfKr517bnCs4wp82XGvf4kHJS
y5tM/H456uv1wQRDNJQ321Fbi6xkCC/KujRMYsDsflGo0VSlKi+wVOIH5cvpem57
cKrgBwNyUYtk41/s6t1SWNyDQvFYqCrhN5TEHu+JWCK7poGBdCLzUtSHJemOH0x
Jr9K+LiBnscmgDstq67x0rLwhe3r4PM80cgSuV+Kz91j23RtksSghpeWe9vxCnkx
NsZ/ZddX8ZdNk7uihJZJ/M9/DWEGx4Y12Mk5XI0Shb53Zml03KuLlkN7qj8md0p1
3tfr/FB82zXo5Hk0C7U3Nej9gmqr6S09kSxwqPa04om342FJuYVZgsfw009gSM11
Z5bYKrQ2m1+/oRawRLuU03fCM2tV+thgi8M9SIw13FUZnGevyuGyudbktckRa4FF
wGkERAZpAag836wt3zUWbP4WyZpY0u6soeARvaeYHpxNW3G8nI53fhwKlHeK0ac
geqC9Z7zdkDZRL6gqDjQzjU+sQZDoFPIRh39zC33Yk0Vm/0CRg02NSIYQ7C2tgxy
uE3U06V1L1wbXcBkEJQ653/JYqUKLAOZ3bKRp7FhgJBb1Lg+Qe1dvg5zFPo0BRDS
b7RNyc5ItAJnciqpH5048PvvUgNwY8fNuKojNeK/9a1GLiE9YBeorWVb+rzenxi
OgfS0LdgszpxfYs7ag/y4LGCN7IOa3r22Kshkq0uD+TUBcdni0vWPVco0Qa9VPjC
UVlyypzJdT6cale8SLK75/ABiIo8SEuqgQLbz+diq+AEPY1TLDW/isd9hCGDexFq
ZrPY/rBXLqA43l+EwqfCdN01ZLOaEvCJ3T71Fwt0JoW+/nn5iG3qfj87mzGbMLK2
wEzxxJnFYW9w5IWjL/YlplPRnNZUm6zsGZDd5x10tW+CE+FoklgU8p/MceR0oEwo
BLXknBDjaq0EDLocgmqIUrSvtK0nDgxdCCqy3+DNt87YwunGWUFhjw/SwSH7Dc
ONvvTVsJbMVS8r7G8oJXMGJ+0Kps1VhQ0iZYILDHeX8hoUYyCyzQ/istgAVJ6Lvu
f2nhjw04Dg4ldYGBPVgpjwP07dYaaPmn0pR7qbl7ui+FxLwGKZi3BQk0h9AUy/n/
BkyvsSJgx4TEL4G8JVgEm8+Zz+yDmNu/wDrxQrdIhzd+ws8D9kENuceuM1xm543n
nM0v6d20FygJFaLEQvVGz+HlsfdHhA79vzSP6kz93+1naS3j/0iNThy3e/rrAAq
ORslyqepsr8XtZlCynxKrmG0pDHWf12iKXJdrN6YYgfhBgNXPUhw1VgfhPny39+
j1SB8vXpYP2EW0EiiY9iwk/0sYxqsZz7RfvtYobZVBC2AuYFxeK/FfBsAMtFIY04
qz8/vrw7KviAAf/bAASBIAgfre9pwE3w8YF80dQVx/3mHds3Z/9v4T05CKRB03cY
5fu+GpSBS9EzuKvDmLOIYdq8SyGN/Q0emK3D4omiiklffzGH/Pj6pH50LCsCBhwD
Pnath1A7jZ4+NURX/y487w4gATjTv1i/N1gwHxot0ln5dC5X/ZrTWLcywS7GATko
2/y+8X5IE/0dWiv6tBkRTNIdBuhsuuKEe8H1rJIAoMfhy1xWIgGrfdWZNGe08bJe
CZBFDI4NEo02n0s9wPOWNHkkaTu7dRTKvxFiPqbwb0K702s0vGtnLb6TWqdVE4Bz
K5DmQXob00qX+srs2ULKaE9VhK4agziDGBIy7jy56PmDT071WG5mGYZOLnVjiABr
dnvia5+QGccmwNHNng5EaKW0qu12ekrbN76wcT+e5indntAK103nrw82SR/jJIHCD
B+bS9FmOP6aIh04UWR3NQ0YCbXQzAqRQmJK7aFeBK1k7J/kzX0kEaDcRlqdFv2fs
QyiFnY04Dj+lsfGpdP3rTx9cfi6+bM0VY4aDonF1YZs46bLN2rdMKvG73fFZiCnq
R8yVA8gBre3x52tTvRqQxHAKH8CeBGB05IZGYbA/d1uFpix1cBef8gpD2zFrfr1J
E0cd364G14p9vD+ItE+hHV+B504UmDeyN8r1ACUCpCYXwN9uWwqh1NAsPPgA72x8
bVC2hNGHzAn0p7X7CDK5Jj14lwxDRkOqntAeDZMaYdKzhS6MVRVVXn5e/0g2pX/z
V2rvaDPBWiKgLQJk640JeBGVX0nLAJUqyKd/JkFwu00N16lyG0kZ/YBduLK3xguG
YistXzkYzod+4sb0goix28Q1iYzMvtwqZ84qW5VcjM3nkdUa0UivyQXwyXXJ/Wyf
WWJkBLKfHZ0tJP+Q8RNMJy9oQpqn12And1+Pbc86tPKi/u1V25EcDFgM3FF0cgr1
BKNNw3R9WCXJhP5ym1op3hQv/gI+45iyzsP1G9EtMcHhajM1hkagpKMW9naT1aFy
oi6h3jMatP+Eqk01fDYQo5bAkfvVJ/qDiVjLkz7CDNQsBcgx/XhV71iJkUhQb44/

cyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGh1IGRyYWZ0DQp3
aXRoIHRoZSBoY3BfYmFzZWxpbmUgSGVhZGVyIENvbmZpZGVudG1hbG10eSBQb2xp
Y3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNTaW1lLmV4YW1wbGUNCqCCB6YwggPP
MIICt6ADAgECAhMPLSW9ETmXSs5CVIEh7j00Boq0MA0GCSqGSIB3DQEBDQUAMFUx
DTALBgNVBAOTBE1FVEYxETAPBgNVBAsTCEExBTBVTIFdHMTewLwYDVQQDEyhTYW1w
bGUgTEFNUFMgU1NBIEENlcnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2
NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEXMBUGA1UEAxMQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIB3
DQEBQUAA4IBDwAwggEKAoIBAQCalsn6i8Gi44/oAVAn5GnCh4PHHNjrSfWUUnel
N41KIImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i
2GMt4jse2Dqs165ernT905NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNH
T82S6DgCReZuTtMc1zy++MxQlqdn9WZLh0A0peNZKGmVwjeVy+8FkyzC3jX/Qcm+
ZLCqllqhBwDHDZ5qDTI2PVX1X3K7/cONxhvBbaU1/k1swdszUtjhflyFZ80RuQ3
qFC6vL/PGewy6SCf58duq/A0EksCAW1b+MD8QH9Yj7CFSmq1AgMBAAGjga8wgaww
DAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAawGCMCGSAFlAwIBMAEwHgYDVR0RBBcw
FYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNV
HQ8BAF8EBAMCBSAwHQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1Ud
IwQYMBaAFJewjnwHfWyn8QkoZTYaZxxodvRZMA0GCSqGSIB3DQEBDQUAA4IBAQCBSX
ignLEynBakDKU68roRsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsoX/Ht9
Ii6zyBVZjdaox644DsiloQEP4YMS7y4q94RFFdmdzEbDLyX9sfUhdTxDN00oHz5
3PYDBh4zE4Nar2inC0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/
eD0du+F2MvtluLihne0Bp1GUTkr0mJBol6dSYal8Hw8/ANHpyEx156BJABb744g
qoeuD9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz
lEc2tUpAr4vRhZjvD6FYMIIDzzCCARegAwIBAgITN0EFee11f0Kpolw69Phqzpq
1zANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLZWhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBVTIFJTSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTA9Fw0xOTExMjAwNjU0MTAhaG8yMDUyMDkyNzA2NTQxOFowOzENMAAG
A1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIEExv
dmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4fj5N
mn9PkrYo0jTkfCv4TfA/pd0/KLpZbJOAER0sI7Aja07B1GuMUFJeStulamNfCwDc
DkY63PQWl+DILs7GxVwXurhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMft
md+K04s+A8TCN012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8ggnhxBW2RZAeLqzJ
0MayCQtwS1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFec
N7836IPPdfTMSiPR+peCrhJZwLSebwXLJe3VMvbvQjoBmPEYlaJBUIKk01zQ1Pq
90njlsJL0wIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpq
hkgBZQMCAATABMB4GA1UdEQQXMBWBE2FsaWNlQHNTaW1lLmV4YW1wbGUwEwYDVR01
BAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0G
EhyXrllqkBDTIGZmczAfBgNVHSMEGDAwGBSRMI58BxcMp/EJKGU2GmccaHb0WTAN
BgkqhkiG9w0BAQ0FAA0CAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjJEEQ+v6BdP7
GKJ19naIs3BjJ0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd
6XaVWHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7a
gyHahIXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9Eiae6aCHHBh0iPU7IPkazg
PYgkLD59fk4PGHnYxs1Fhd06zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jM
hwFXLJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGww
VTENMA8GA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EGQ2VydgLmaWNhdG1vb1BBdXRob3JpdHkCEZdBXBntdX9C
qaJcOvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIB3
DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwMTUwOTAYWjAvBgkqhkiG9w0BCQQx
IgQgX3dsWdSmGjwXzejaB+kh8kzN0iNjkHpEtBXbJ8gjt5UwDQYJKoZIhvcNAQEB
BQAEggEASc6sf2io03Y7yV0zy/6sbjR6suLfigryPkva0vuh1aHCP/I071/j3LYL
nER9aCGoEFXzxXzI1aitjwLQp+Fg6qNz8avFRbSvecUpAsbihlRbb0SirvNwW6F4
McP6cbA4UR6M52M4mE8buxvDtwf6caf8gwtX9XbZy9a/FSr1YqQoB9ebotZDadDy
sh0hjzMTjvHbq6DTPytem6Dy7rBP7F32Z1SHNC1Wc2MaW4NKejRxubh4kKpopRvk
diHHADbm6WUwa3IsgU65HV7X/BkE4vQcYsWzYjqyA3WjpZZWlYus023kqug5sHX5
G5uhNtW6SURCqjN+d6PNa1820qCW3w==

C.3.1.2. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline
Message-ID: <smime-signed-enc-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:09:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-baseline@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:09:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.2. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8085 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 4968 bytes
    ↓ (unwraps to)
    └─ text/plain 414 bytes
```

Its contents are:

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:10:02 -0500
User-Agent: Sample MUA Version 1.0

MIIXTAYJKoZIhvcNAQcDoIIXPTCCFzkCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBE1FVEYxETAPBgNVBAsTCExBTBTVBTFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZm1jYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqSISb3DQEBQUABIIIBAf/SL+2acYbbnElaXwsZy3nS97+v4FjebWx
L8Q/BXPJQqFAqPwXiBMf2vbpBoVz/mq700wPiCUBgG6IT2e432SJ72N+FsZhC1LH
WSRu50QqqkFTrSzomm0iCcPEeU6dOL2THdDH01Ltp5zRarFzEFzXmjEIqVfHXFQH
2hm07af4Usxt8cJWSLaQ8px6hm4KqSpwKSLEeXK7kiDYKJDsL1VeSHDfqiJfkoCt
iajW1C0MfjBTvD6upSlusILp3/wju0Zr3Axxjr9svkyGBqkwQxUtNUev2JXxio+9m
A3xYUshLgDjVn1ImBN3q4yQfyTg7By15aS/WjdRZd4kBPoJ31AwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFUMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1UyYBSU0EgQ2Vydg1maWNhdG1vbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64Mv1sDXhpQwDQYJKoZIhvcNAQEBBQAEggEapi17wPDNLbvOE+snTdjrgHyQ
V4DGBR/WTMw8Tzd7Zm6nh6h4jX7x3FX8NkyE380HkFgzZ5yitz+kB7WtcMr2Gij2
VBdJi9ey3pZyTZ1TCkwnF5q4ghqD0vfoPmKXIOP0yQUP7Ak9+EXA91QPYaMcTRxM
jvibAzsbwQmmvnuuv1LhGqqDjv4woTJ8F/y0xrWaidf8nfWmCEZMP6kY14sDxFT
xxm329jXEQ0o1qYHzyIgYhRk1LW09h2TpC7T5Yov7NfWZyQZA0F4j4TW9gCfmcfb
pwP5tczbzxpc1kkl1BB1nbezpVEMbMsaLCcY5c5RDRLPJpDhYKcUztCeZKbei0jCC
FB4GCSqSISb3DQEHATAAdBg1ghkgBZQMEAAIEEHMz0B+KARgbNWCbbkfBkqqAghPw
J7tgZJiuXvnsaLW0qpJftfd1NW11Y6uUmPGbbp6ukBFi4Ri+coXutASHHc8pgQMD
In4vIs48XWLT1RUuotY2JfBWRq67pCjsfv/s5TyRzEaBDC/lwYV0m7UdWiko59tY
+y0Xqz0R5p/Rjj7U6REPNBv+QtQN0zXbECJxJ19IGEXL14ziddgXGejQcM0Juxk9
9AfoctdteTMV8H3Keg+LGhbUhwshHv+o9CQfWo/kEAQ90n20Zhb70RggCLRJSg3c
G1kdv+ph3umi/bGZVupvdpKqBQe5nSJazx2Ej9jkcbX+W58csvgTEME+bYexzK7X2
v5d/ut/lmd+Ah+P0kU+ZVYIAPHE5ORDrLSZjuUC3prtkshneNqx+DwA9MnjwRa4p
seLZWRCoeZgubftMk1zKBDRUJ9WCHxbvK7hLmpGRKpNHuHUAt4uBbHWERXBqvSG7
rmsN8r107panMefhNZAF2r1wc3dEVtwoV315RFboof5sPyVaitXkP3K1GC4JeKsn
3nqiP8sgN1kX8FLj2i6GDJYdcUCyzfURMGFGMqvwvtqFIgN1TYJW35gFCitJYCAvW
MhUseNGQz1qigkb0juHxSsgGt/OUwJf/5mhK5cV7KTYstnbF8tvxGT05MFaRJESh
s/WSxSQcr9P1T3i3bLQ31Y063j28cWvMzrt/vZ671WnpivPawpSQLMePPKH0qj9
ZLtf2iIc3Yn76ir3v8SSWpGs0BES8s1lhM/jEt1t5H8xUfVNz+WyhhnnL/3kdhv2
xXpnuSscxiQja9I4K0hqw5gHW0t//vnNZRRCXhWiVL5rEx0kK3UUnSJm63kkn+Q0
y/EykyK3sLCTSDQIwdbe3CoXq+smap61qDQeHgpBn0Sz0/Sp1PvPS09g6f0Wn6mj
ocXbrifW/y/uafC2Bs2rLEtfq7Tts0T96urE0BI95bEF530uYj9xLahALFmIH8p
DgHNaOymQcXwkooCT9JG5h4c/pZcM6Vbde1v0a4Nu9eoXC/ZIT7z1oVV7e7aYvEz
QXaABEmmmHaySmPpBC75SegSLUsHwRbpS/AGQb8LStZAX3mh3fsDfHqcWiKAKin/
QZ2TwDanvMca9DY1WFX3WeWte/fQk4uXEEQdPnLu6c6q3+ls3seauYpfg7pnr+bG
50msWCSg5HDBZqlsw07/cp8VXSXYLI0x0iKZ6gWFTkqcDkAEX44eYW90Q0V34fz8
yec/JTUTvLV0VRRjQCsg89Hx4dejSma2bKIjIdrF6HJfTwhs+XbDMxG5h4t2++/S
KFFDsmPtYjgcbQEas0ELKMDYtTWy5jq2L2nVLScheryfIN1vq1y2lUEPk33c4U8
vCp0aVaRvylCi6TaWKjh8JlfJ6e/Sx6/WGOY0wmN9pYeBbRsUmSkjtV6TofOodGf
9tp2VXt/2js02RbDCKp3cC/VNgttVU316H+R1Dvas0JIcVVeDVCQGiKnKLRaOuoQ
6Z0GLhfht0xSufMPUyVZUqmgbvWn40cQSYMajot6TCwQ6YSoN8L1H3CX1vZR1tCG
STXkEQ9BIL6TwQcyraRuBUnabv3oS45HNIZo6uWxBDFs7jHYgdvtJVko6rKc+yB
nXoB9MufZfK0Ra1SFG5n6hh6wh5DK1/5BLbWvym0Xwp55fhie182juyG6s5m4LFN
VpeDA1Xyu7yLIHwfMrKaKuzo1YWNu4mTjy1Y+v8WmVFlg3jiDLJGBN9XKsLV9tBp
chbN51co/RJh7A2Z5FUU71sLFwbBpmSdjK3/H9jtg61QwqozKwIAcPt+NCUDIZE/
DUz9L1u14qWd5FkoIUxVt7i6/FJUhtMwRP1xBtFXJDx1QQcYPgy9NRzJ07DpGWMK

XYB2aVif2gGHVoS103HGdqMJ/eciaRNUT0le35MkIpLh3Myv3gv8xIG2ue+uiiJ9
tG0tmbpsG4R310t/KV/L59Aa0X6y8dtrCo0IyD8SI5QburVh9FcXUxphMxgKle9h
scVHp+KYSLP6cx1z1E40MUL3ipU+ZLpDKCM12VQS6gdv8xyr38c2IGg23QCK8Vfw
DBmkJj32FaFJFgJmKcnEqpSJC2w3/i6odPJDNcV5k0QuQ6RTUaJpMLYcUTi1Vtiq
5wGVlXF0PR6va7B2IE4zrjst2pQ1e1wtQDjR3bwIQgL7/scNeTzmzgzcTwWP71HkL
+xSoCu5bCxALqG0zZp1c1/v/290M8sN8vDB10R78YM+dbxej64BzaGa0GDinIJeH
o9hjjif0UcwrKuVRifpTdc+rPpKXkXbI/IyFMEeVLx1JZTLi2i7BcChTy+JSUUV
Lb8RHEyRZcx/03i0+kVqfGUjaEw3S52A69A00/tvFDzE+Yxe/1M6RZrG7VanhtwC
WU3XzKhg2SkM8KNTcG/c7cRw7tzZVwHpXhH16at+9GoIsXA9tiT5keFKJvNWWdV1
U7EswrW557JnqSa0V9WwhWastP3LaAGDsMuseIRDCg65CUMEVC239q6eXX6YBE80
Fn1xN+WluVnp5Q2MAX3nTt0Z4B5R7E2qP5jBL1L6sqzChyIBM7BBi6Z9Enz91qzY
gLZTW7s0r2Gx9513voz5BbPyM8S9f+XzURH0LBbrhoIR9yk6QswNYS7RaGJREDL9
zv0Ird6mvTzRC8G471b0Y2q6TzU+SNVU1RVUdWj8X63SaU3p8F6HPqdItIfPc28C
NJDPeMiAoMFt/Zd9ewDUBCV4aPMniYUNQBhVvFX+CFbtSY3Nn8MVD8XN4jC9UB3
+sECAe1zD+hAG7j7vqvryKksejsX4tLrN8jIL+PhpU4bsTdC5kg3TAVQinf4Umc/
RcUaaMZItTuy+FG48sewznCd1E/6eBQxXRKfoHCnsBSgimiwqX2wvd+qvpgEzr7v
UTJgy+OMeTcbmnRz+UYIzUQRYYGGtg/vFYiKBM15xTu0qlGGWqC++15V/Af11lp6
4wYXNGSwNkUm1L6vqQJPgCfJs4L+onRRZLrzVkBKQfZVSs7jHUYiS9ivoYTP+I7+
zhiW0XYkQYf1dcIXwGmVYD78tdv7ip9S0sJTTQj+WdWfdWNP4BP7H3DGKq3rUbts
y+ti5/9I5Z+k84CBpS06cd6o2ByrHeAnqQ7Ti8GgM2IYvjij04YFDxKG1EJAvQVJ
MXKi0VIh54rT/7v75k4Dc+uysC3r/7o1BQESx0C9H6J7dHGLrPOAJh36rhh59S1U
J5ea5IZrsBkqLS+3xMy7h1VcVfhuKu84zwD70RftXUqoC4i7NCmmgGE1rQ14s0f
BkiiIqTgHEAr3A8bYFp/QVdx4UVQAwPsTKN0+Gslhj6WJpr+LHME8tesFg2pY4tt
YVMRWe52oVSH0FKmhZ6CR6DheUSiPbB9GZ7aYpodNZ1UgGB2iyl6qlBHZvH0scFQ
tupRY3EtFZGe26Rh2btS+xrSwph9n2/2apD3j1PCdJkj1yUA3iVybjD0Ks5NCsTB
7h0+V5xbMCHDb9PXHx8i9981YLIInLjfkGgDA5V4HfwTeZNSMHYpKLQYaFRFyn0ud
ecgQCvHXnC0amgU+bQfReBpMB+PI8ouxR/W4jIrovx2iArGVhvcLdl66Iv00/GF/
Bwa6nJ2VoAfmbH4DF0Q5U6KjJk1TCE6oGp0K140NKy5Kw6nVAmvIcONsYHLDVAY9
ba+0Tjoi+cZauKLMk4dXK3U2fMOb+TPqqomwaEkQVba9F81UYdX7wyvTWcqDS/X
h19CWPW3LK1W0LfmEfQWTwj87SCot5wF/thc0nm6GTAKwEmp94AbUfTb8kqUxAdq
yquvLk09tdab+ehAz5V2QZa70bwuvWmWGMU6g9i4zEXL4DTvrJJK9buA0SviZc9
v+0Ic+fEiF3KBH8vqbFhkYdACn8E1bAYPmDIVbdNGN4+sNmSpCWT+vet9xcTUcU6
17g88jgc4vEEaW01AA8G1khzRJNNzrbFZusDSGPE0CRpj0Eo3zu9/nfAN+yXKuBh
zgAXM3VJmCbCvd95NaaYaw/D9/mm+buZf39tMV1PdUY36pbwgQtT95hfoyw0SAIM
fo4GyIEpd4KgQZdXycC0JJd3T4WPV7SCla6ErduMwJ7qBa7MG9x8HfX0kPNGIGiu
V2UWih9UxvY7wNLfqnX2CV+XLW+iwaeJo3zYzKIAcuFEz55FE1++mELC04gwmAkd
Eexou8/Vig1Cv8y/S++bS2YwYm9qZFRHk13zMS2QdcUBkqaAGF+/dfBka41DLHVi
jqIAI5d5tXPq5120V3bJtqP5QNb1GvMw01HrXLgN+OocomZfUKY+XejI2mrgF2rR
QhPYDiUfQg/tjpsoZZLSjPfsqUkg3gCqbw7CX0gyU+Qi3o7u/p1cXeBdGDYbqfE
V8dG5owCq+LliK8PP/mi3M9hxvC8NizWmuI0MsRRZkcGB3R7E5MomZxKilhfZgSI
JRSPDYZmxwvtPdVo8kQPpVvbmJsLhp6AE4qoN9pGam8jEpFKD5ju1KoGGeN4Yrrv
3171UGMD8VdJJ/aNWucKViU3jYCNlcl/yOMy40M/KDT4pJt6ipol006ZXRDLnXB
X5wuv/nV6tc/Qa8kW8L0dqchYd94/Hyt2dtkepQVS3YB0dimvz1htXt1bR8XM07K
iYlF66cIm8dhfV93DhJcyInJhMRNCjSrTz3saDQZGeJPz0a2kI556YAazj1NgAQ/
+/fL/mDlDK+p9euwIevg3xe0110jqdpTqe9D0PjtjjnVWEW9y+0zv4tFESMh8g5t
q9W9RJ5oN/C1vEFS69BFkSNP8gGiMngv3uxEXDmDNJQUcfwoStlItXxcV+DjoS7
EDI3qU0h4Cdf53o2dfpc4+yjbnSSassRr85dH5GmuMoYQa95y07YhiZFS0VRasS
bpcNbTtrqYglt12WyyvWnmKS4+IZPeIePdn0tu33nh80ouE0srONNDQM2I8BWE/Z
PFRXHPt1IDrPqciGG13snBoGfzCbGI2IYrBONgaETvB1Ba7AV/in8I2oPCLWtMnR
LxzJzI7l6iRHKxT9SmLNAZ2kUno1E0B08+DWWyn6+bVmrBv16XbaZmo0JnTJbCsk
IIJGz+yG1XHaIPLdIn3/ouOKdwDtbRwCGdE6DgcH0TCGJ00A73vsXIym45HxZ74n
Mv1mdrduyIZr78JM5E01D1czqspcCM73XZnRgT1DAfJtDj1HT2z6jsrlepJHAzxo
pBrJikk151IkDlJp0IztwRa2a3Nscdr1KKd/FUKQEOj74ga3Lw8cSmOeYU9o3KQe
DzE02rVFbdFvgamhqYmdRiyKrXLUmI0IpOs+ftAXPwm2MDr0YM1FTIHppaVT6oB
ICc15ZDoUoDdLBBwFztNm2H8UcnplrXLIZQEHOYnS55s72RPM1WcIdIVdZt/+0d1
BDgtMBimGJ7PmN4Qhs26ZxQkAaZBuvceWkiL9ZziIDQGbZJ5cwGMAUGGzF9nhrBd
3bq0friQkI7KcDKwVnyh7sWBgWJfM3+tdRMPCaWDgJ68V8wpd+qvVSQFxoZpV59W
SePv7MwQddmvAVot+XtldairyZ291QtCGPxIPQzyqoke/f78R0UKqG9ugI0cB0By

```

UR2TcAlpcxwOpEApQBboziLpragIqhd5NtEj2RVD8e1dtOY4CD/jxiVQKqJTTrun
nWBBVWMZOB6pMwoqDJAqjjRP0uaTHBMgI93vj1lKfYIDcx0jZn2D21ey8J/LQJjn
rHL/XxJubai4EyhkxTmrafs4VZ1Ztoc2py99Za1zX90fu1dBXTQ3NdC2qmZ73Syk
SiNy7kOF8aCBcVmSbfcHfCZeKusCGe/KUeGbEUHqHxog8x0PJX0Zp9cMyc8W1hiK
Ky6x8BMTh6/GKHoi4ygdM+wcT06oh5pg8U+gJeDB0+m/TVQkDm9jWcPFqiTm6plb
48KuuU1jex09/WXIGjYP5r1rViBRIQ1kBCSs/ZGgT+xHyL/U/8YzNtZo48pLtfKx
eKN725KJxEziRXGjKRjDUitJtc0KCYeXWWkg1s2hQNkg3vFt+moLgV6UVnZwg+Tp
Kkk5A1XFBLDQUHIZKBYI6mmzJntMMhtLE7qR0S31w0LQxgR/KvClwJ41MfqXxS
ShSjgu3ZmAun4Tic5Er8xHtL2fw46cy8NMAAkMZgGRA5Lc0jcbgMWdqz868Uoumn
CABiaM/cw/fLIc9/MVDFrBM+m7GrJJJe+8+GaY9tV+psxo0SVGNI2kqoXVI0yrTJ
WhVik6d6oJaGviNjczaw4C5kuZ5bKHUCiMLv05uAtQ00yPidgdfZXymBoKCjndge
MNRBo4MxXU9cYHzi0umhauiw9I3UG4HAKH75L+1DFf1wbbgu165dCSIo2wVTIg0t
zr3Y03kTJJidcklYzP7o2d80EMGftQQ4uGyEtowWJbEn0yWhss35Vs3Fyy10mwGM
pncS4Tc1dVGyddkDXyAZ1JvfFzsXnoX+38R51I25aYHAbfij582/hv48FU1I3XoB
WXR/gIKr/hQ2cFLwHsiJLGRw6smfBG0zk/x4JhG7sCR2E0QmM9CYzmyhZAKX0RaX
Ur75d8x99mIJdE04uu4avHvaRouG6D9tPJWYIRioVDTDPD1AU6qirN32h0upGwcZ7
t8q70Jbv/tDpcLmLNx5VxsQzUfjpsGGvuz/Eq77raPG/TByissRMTjUuFv4BxS0x
wh//p9l2sJA4FWCA+Sr5YLFub1QqRF1C3Vv0h2YEEz+sFA44u4VMmcCwGBoJob1
4we46RXwzH3K7gRV/1tv2QB9pK4G8KxsBHXNV5RwVJ6xXI6JRvIJru3/w4nRPnrA
lRXXfx7senJDd2tXmXvYkA==

```

C.3.2.1. S/MIME Signed and Encrypted over a Simple Message, Header Protection with `hcb_baseline` (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"

```

```

MIIOfWYJKoZiHvcNAQCoII0CDDGQCAQEXDTALBglghkgBZQMEAgEwggRABgkq
hkiG9w0BBwGgggQxBIIELU1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVYLUVuY29kaW5nOia3Yml0DQpTdWJqZWN0OiaBzbWltZS1zaWduZWQtZW5jLWwh
LWJhc2VsaW5lLWxlZ2FjeQ0KTDVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbnMt
aHAtYmFzZWxpbmUtUtbGVnYWN5QG94YW1wbGU+DQpGcm9tOiaBBbGljZSA8YWxpY2VA
c21pbWUuZXhhbXBsZT4NC1RvOiBCb2IqPGJvYkZzbWltZS5leGFtcGxlPg0KRGF0
ZTogU2F0LCAyMCGZWIgMjAyMSAxMDoxMDowMiAtMDUwMA0KVXNlc1BZ2VudDog
U2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KSFAAT3V0ZXI6IFN1YmplY3Q6IFsuLi5d
DQpIUC1PdXRlcj0NCiBNZXNzYWdlLU1E0ia8c21pbWUtc2lbnmVklWVuYy1ocC1i
YXNlbGlzZS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVyOiaBGcm9tOiaBBbGljZSA8
YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiaBUBzogQm9iIDxib2JAc21p
bWUuZXhhbXBsZT4NCkhQLU91dGVyOiaBEYXR0iaBTYXQsIDlwIEZlYiAyMDIxIDEw
OjEwOjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlc1BZ2VudDogU2FtcGx1IE1VQSBW
ZXJzaW9uIDEuMA0KQ29udGVudC1UeXB1OiaB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1
dGYtOC17DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiOyBocD0iY2lwaGVyIG0KDQpT
dWJqZWN0OiaBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLWxlZ2FjeQ0KDQpU
aGlzIGlzIHRoZQ0Kc21pbWUtc2lbnmVklWVuYy1ocC1iYXNlbGlzZS1sZWdhY3kN
Cm1lc3NhZ2UuDQoNC1RoXMGaXMGYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBTL01J
TUUgBWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3B1ZERhdGEgYXJvdW5kIHNP
Z25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4NCm1lc3NhZ2Uu
IE10IHVzZXMGdGhlIEh1YWRlc1BQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIHRoZSBk
cmFmdA0Kd2l0aCB0aGUgaGwX2Jhc2VsaW5lIEh1YWRlc1BDb25maWRlbnRyYWxp
dHkgUG9saWN5IHdpdGggYQ0KIkx1Z2FjeSBEdXNwbGF5IiBwYXJ0Lg0KDQotLSAN
CkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQqgggemMIIIDzzCCAreAwIBAgIT
Dy0lvRE5l0rOQ1SHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJ
RVRGMREwDwYDVQQLLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBVTIFJT

```



```

QSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUy
MDkyNzA2NTQxOFowOzENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
FzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAmUp+ovBouOP6AFQJ+RpwODxXzY60n1lJ53pTeNSiJlWkwT/cx
Qq0t4uD2vWYB8g0UH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeu
Xq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7T
HNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmswqpS6oQcAx3We
ag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukg
n+fHbqvWdhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQC
MAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNT
aW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQDAgUg
MB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58
BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAguL4oJyxMpwWpAy1
OvK6NEbM1lgD5H14EC4Muxq1u0q2XgX0SBHI6DfX/4LDsfX7fSIus8gWVY3WqMeu
0A7IizkBD+gDEu8uKveERRXZncxGwy2Mfbh1Ib3U8QzTjqB8+dz2AwYeMxODWq9o
pwtA/lTOKRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4
oZ3tAadRlE5K9JiQaJYOnUmGpfb8PPwDR6chMZeegSQAW++0IKqHrg/WEh4yiuPf
qmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1nTXl85RHNrVKQK+L0YWY
1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcN
AQENBQAuVTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNV
BAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdG1vbiBBdXR0b3JpdHkwIBcn
MTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBE1FVEYx
ETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFjZTCCASiW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALt0iehY0BY+TZp/T5K2KNI05Hwr
+E3wP6XTvYi6WWyTgBK9LC0wI2juwdRrjFBSXkk7pWpjXwsA3A5G0tz0FpfgYc70
xsVcF7q4WHWZwleYXFKlQHJD73nQwXP968+A/3rBX7Ph00DBbZnfit0LPgPEwjTt
dg0VQQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH6syTjGsgkLcLNU5LZ
DQUdsGV+SA03nBdWCRYV+I65x8Kf4hCxxqmqjV3d/2NKRu0BXnDe/N+iDz3X0zEoj
0fqXgq4SWcC0nsG1llyXt1TL270I6ATKRgJWiQVCCpDtc0NT6vdJ45bCSzsCAwEA
Aa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQA4wDAYKYZIZIAWUDAgEwATAe
BgNVHREEFzAVGRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUF
BwMEMA4GA1UdDwEB/wQEAWIGwDAdBgNVHQ4EFggUu/bMsi0dBhIc164papAQ0yBm
ZnMwHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpHGH29FkwDQYJKoZIhvcNAQEN
BQADggEBAH0JoJanzqmgasN3/ggSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNUyTn
euK6AChwKfnNv0Fb8lV1iffRtF/KtmVEDMR/sYeqAH83KM5p3e12lVh40HhyI0qN
uz5oShNaACSioQ23WxHGvy9vsdVfnbhsplRw9NQ2WbpCmK+2oMh2oYl0Z/wvXmt
9cG6jbMvcdH4z0I0vg6mrYkKTM/RCGnumghxwYToj10yD5Gs4D2IJCw+fx50Dxh5
2MbNRYXTus2ZPRPM8JXNQC4Gwv4km3M4rKnJd6hnoQ9rNeozIcBVyybQYjfrgg4
DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMg
U1NBIElncnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+Gr0mqnX
MAsgCWCgsAF1AwQCAaBpMBGCSqGSIb3DQEJAZELBgkqhkiG9w0BBwEwHAYJKoZI
hvcNAQkFMQ8XDTIxMDIyMDE1MTAwMl0wLWYJKoZIhvcNAQkEMSIEBmb56ZODWgP
A1SVa8da67RsNidfHZ2zJVUWYLTkrF07MA0GCSqGSIb3DQEBAQUABIIBAAou3+Ck
FB6wTFWUvq1ABIBF3AFS+wBR2+mDSQKXxLVCnt/cfY07qKDX2YsVkj1uXq3I1PtW
6RHEtqtbY3iwAqB5pzgfcw7qZHDpRMMEwobNLzHBdSZwW+1jkQ3LvDAZao5c+Cmt
gSUCdnQ9Kvzdkl+xgtJQnjGGGNBiiWDb7NkZhlHYesV7QKNHTP+qP+awE1ZMR0P3
qBgIS1UH9nSNSm0fyTprD8MWOuKPKzF11YUyPByE/QKjdV245YvYuZjz0cqn4VvV
2Y6t9DI4EmJJhay+P4EJwiggtjH9mJeeXIHyKpyELVSC5KCaIghQpTHV/pIH+fNs
WxxyPU2C+RwECsI=

```

C.3.2.2. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-legacy
Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:10:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
  HP-Outer: From: Alice <alice@smime.example>
  HP-Outer: To: Bob <bob@smime.example>
  HP-Outer: Date: Sat, 20 Feb 2021 10:10:02 -0500
  HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8";
  hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-baseline-legacy

This is the
smime-signed-enc-hp-baseline-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.

--
Alice
alice@smime.example

```

C.3.3. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#).

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 7760 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 4732 bytes
    ↓ (unwraps to)
    └─ text/plain 319 bytes

```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:12:02 +0000
User-Agent: Sample MUA Version 1.0
```

```
MIIWXAYJKoZIhvcNAQcDoIIWTTCCFkkCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBTVBTFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqSqsIb3DQEBAQUABIIBAcnWkzPI3J1YHJzg+y81VoDKI7z5vg2c74uE
gBsxorvh95LsdB/zaB4nLdCgQhV+XW5s1srqRK0ioiQYbQi9txvMOzBb8ddZeIqw
1CGTLr70Xx5STs4flwJTYFBX0SrbAOYPGrWpHT1M+yIzD03oAWJRy0Q3eRJW900Y
bC5+YSAjTdzhMnn0483TQNYAun3CV1dTvQPEgrZUzi5/932YEN+sEA06SEPa8Dc
q8aH0843aTttnoRZGm+MGW0w3LWD/82EwRhucvLPhvusoKGIqGuEnvd0ETfTe3LV
CwoVEYotg57+Q1IW5dvio6fmXuvBARHVP0Ef9K1Jp4yKgJ0Cko0wggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1UyYBSU0EGQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64Mv1sDXhpQwDQYJKoZIhvcNAQEBBQAEggEAIYzFIRtcEwk97gg4g0bZn6Ui
HpU7Sa/VV4edmxdBj0dBx1BJzD0hwM1kUXSqPg0ZvRz9ehSGujeemC9uYfXhXo1J
AWf6ZW2i84zmQXkc23JlUwWajzraVfq6lJ17gy+iv//EtUvka/p874YRKnW6rDSl
PZzdYxcGK81dDmWRWcVvNQbyMT21EgvjWxm5/Ca77aSseERT2LjnonrKRvSfwsa
j6NZDC95Pd9GplsvgZD1GfNmPtymQaK1VhRy53D3+Ne1xHr97C77XYdJQefaZH/h
qIB2PKhjo3hLpP4dCvBDLI2TwC2wIphQ5azqH3Lcv/imBYuVqZM5UTJlPk58pTCC
Ey4GCSqSqsIb3DQEHATAdBglgkGbzQMEAAQIEEF5qWn/RJwrmJiPW9ewiei2AghMA
LYAJ/u8gGEAJbFuX0TnN0ztW+UHE3nWkbWmNf2rYdRCTRt6/DnH43242t/LkEbh
2fk2EOyffUFnrHglZsRWqfn4UT6dqMfMNDzgCIX4ZLqMUBkBRvn66S2/L/Sr1iM
wGZBfEAKhFo80ldzk1/aCaQUYVQfZkoI1clDg5ZxUGTVV55kirvTs0+PPir2ZVCT
aUhvZIZPsW0fJAqGjDxq29ByDe2hSxYftpiqequ+PHQuRLII7TEdUnZs8rOprswj
gn/BKPUiYKAuwIE/QCgd1gBW+TPZRY08TMeZHaFYx9F0MqDpOLjpgH5msFj973KK
cds0rJVZ2c3Ei/2VuxUvN0nEcRsd6Nfk+lny29hXuLCENLH5j+Ll012n59H81F5B
z0+29a1wRTJNT7ibVzrM/Bj9SDSPFzWrtaz98UjnAmhTx/4X409XS7gEZBdbveYy
+c6Zp/3cUcWFHp64gN9Fyug+cTV6U04Y8X+DzxbFEe0jKfx5nzCy0m2c045cchGx
54vtFwihMrs29C3SxfZTRFHBT/zTG4PXkqKgW+ZbQYG8917ej2UqNf5+EDdK17cY
r5HGLz709hDJ81MfDzfzW0PZ/60aE+OyvfZITL0Zto3fUHM82+kZt09p9Gd81fVu
o4mrRTW5CAfbeqv00pIKeHc4Buq0Cn0QyAIJ9W2AEzhr13DuEHBBB0hk1q+U01h
AfHC00arooIC5q7wc8sBLJju35A09msXje6mYGNewZkVZWLYYHlwURtYbEkonJh
nct0ZA37gL9Emwi/byUScChMlx6IhPrWdRCAuITWaJfmYR+Enq67wGrGPkU2U3eH
5XOLto815AtoouXP2C9nAvdGfwyHA8GvD28Ch8oDdof/xa4rZZGdLAsBxiUd70Js
CBBfbSusJqoPvC4yfeR+66GLtvVpFtmVZ+mTir1ZXtckkn5Dn+NakfV2wWvQGTFK
/dzk60Qlu/cCqWbt2/Rr3+Cny1SgJLYstMPWJezWK5ATzmtTKZZ9snyibsskWXlW
QDjZ048lgWaeK3hh+EZ9B1P7tsvgR/E3owHa0DrxmTgRGx/CCqlnZr0HPmPBg5h2
bSMYFybxr2CPgl0jr1NWvyZq9g8nFeVg3bqCncum0B57j1Rb4jtadlQRAHuvlpb0
mGcl/KzYqYUVq7/AcV/390/09mW7xLzgpD9F7KSpC3KxRutZPG+f5o+AGTT7moxD
hqVtwYnZYbYekNRU/dcakGieb4ksjyeVC40c39Xf8QTFQWm2u7cEjnfZ83D6kwrDv
701NCvs3VCyJahysjUnzA4gRXuKzTI+GJungjP5Pl0/DR2C3rimfQoEw+A6mpTga
SuTJQ6IruIlZTxfGAE411F5RLkyAsMkFOHLuDI faj6i7u/x1aDAY/9IDlwE+pA6s
IKx6dCyt4XIVTLNDkcQkjLMdl+i4B100eLJxanJdm3Ph+k50Xh1zNySbyy0NkmE9
uBJuE5gjjLCovq1o9rPR515YSZv0Rx6E2GuFkcbjCEh4Wc0ixb5CSDYgZSGZELGi
7smZ9W9WM1eadb8gCQIP00zdo1A7slnmG02ff03WAAXV1GYzg2c7UdgQdqhuL/eI
Q/eZhGeFFwA2m2e2H2tCIza1Ezmzd/xaeqChfjqxjanEUwBjtEuvi4B8hGGX4+0n
J8/7bKKnWibVQYHdEy+7fB716NJHrGTI7dzevIyq0WsZLIPYUihN1SP/02C+Y8bp
ChduQbWqUq/E0m+miVEI2z13i/wWR1vT1ripJP9U4tgENzcjyZBhzAIL2Ionf25
M17kjHqhxS54DGZJxiff5cxBWHG0vvuu4W9M+3zGPER4yWZML+5VrK5wNejz1PPW
```

5kt3i2QY5a15UjSL2NIKI81ZNJ9IkNGT38Hb+jSobs3pvkPdnUb1++TjAX1RwYgH
Bgr1XpD+ek8xoImLncymaJDqApW/Cs/9I1GvVlXIT6BQi3eA0uy7LpaECi2gWMRJ
a0R0lNt31UGHRez6rv8G1VthzVLNOXYlRKD8p2/NjN/Giaa1yJPGAu+z87G04j/P
Zg82+8SWYM3A4crGKjk9bBA1m7Hk3qTVu1SeyBA0dcNyuVH1LYInmzkvo+KGhDh1
rGuM3SVRQdVay286AqX27HUiYHZ39ebqJwMWY+qBVKSjwB0I6z19JOBrMuyB0dzV
TH2ck9dLF6+fQzfLLspnBjbrdc7KwbjuIX2Nj1R9DQLMC6JpnByGeo9ctrVeC3Z7
KE5MbppSG7gcXTMdqohjauu8Ru+PjxPggjtazUymKoEoMJFY0kaww5dqpYuPxtjE
YRgYyMfRFY07qnAU7+mdW2XzvGJAyV08o4RcHnaiXenlZs+TafQ0Gov0AKyBwrtw
ob8B35Z/XPp3tr1RuGgWaD7TDYSP9Sz3SvPhIpUBScCF1Hw+o5GsF5eoDGE63+g
N/ibjaJDNH3Dk1mIfMXAmErP8bqixSKXuPltf4U5L60pqhIsmk6rNdteKd1KBGi
/Xn3JXT4Qj2PicodzWDJDiaEjn9QK1FQy0XsScdT8Em5kfptHcc1RiNgsaIx0vpw
3RRsPNjG78iWQugl0XAK+HQUP2KxyGwWQX0e0ET7M5PLhPGhkya+ht14nuK3i0azy
ULFRctnSFowW+q81qmJYUufrcZ0QJf0ABVPbnVmLY9k0fG036N2NsPT1Q8a1EzVB
/CmoRmtntfJnKJUzubbgtvdqaQnH/mBTg8FiA8i4MZAeFBRJcSRLE+hfL54uA8GNf
6xr4D5eWIMXmvlWKiQd000DW5u/c3LeWzVyQFqm/Cw58cXnmTFE6mhTrWtkfFloX
S00QB/fzfKTuJuxiB0dFrPHuAIR8smUiWZiyz7NzXC2C7UI60t9FhpfQILHjAI+i
ktxm9EdGq5cix4RtG6o8lts8kJl/kBLTmuIH95sfyNkbHQ2dYi4LjPR7PKBAZjJV
UyFI6FDvIOMUA6TJfK0kyb3y2eTp+iRzuys1APhEY2sAskL2q02ZCzTldHNJfwm3
qpKciyG0LTg542SfC2GI0SSEh5jBVHy29liaw1R7ecM0Skjy8Z1MBiiHF50QXm
5hJ+T2xI/214rUvESBrcPykMTT8uKnAs6jRxoFvuK5Qxcu0VIab1ja+tXsft9FW0
5kSEL3cxfBoXRlWfcLpTty3Um6AukDGMmleopM6iQMoBpeUqdWPmvi4SB8jMJou0
rL2mZcna13w2tUe+eitwln6AIo5b0Mv14NkWcFeArnLyguvjkZ0aOE2nFvaI/rc5
54QCW9/VRU+Ku/S77gleCNSy0/FMOEiWFIWzc0Y4fnQxSGmp90Y1AmB5/eqPD5d
1f7wF40eNOUSKkCbX0A1VfmumJ+BzKdwZyjsxf5oDzMMfaShmnhtKz8lsfigHEic
1CFzuf0Wtjw3dnZrNmFIFhWBrcNtur3u8AMEqrmWCGHnATxL7BU0TiFvtkq1SUA
/Vq0k7gbvcAk3UdSVV4Ixr3AN3wiWHAx/Fmta4NJYM4xljrmWPL1nXUH0Nirv7aV
x0xHgZQOE8ftgIzkLjNqvQyuRaz5rJZzmHV20sxyKuK/GipCc8vx1kNrmUTjIjTS
0/9eyQw9I+efnBzydJRzDEoTwSh7Z/v7nJgMV9sxGy9MIX67z9WpCq0L3TuG+r1d
baCymEjF1Wf/015nknijswXyEglrgryCZkW0HHogwTAK+5efC+X7ZV0Uiyt8+HRJ
+63ZB86gTuKi8gM83p/ujliSjekCm0exPUeDu9LzIcPf+kkEDUZIBoKh558h/2nv
BWK+CVq0GFW+ztgLoGbDfr/iM/0YIUo71+gIR2GDZuVciMHm1wBrQK31BM/sfCcD
KCbcYf3a0JPOu9E44tHjA13pHy9d0uRHHAvLrPxRMCgDkDSi+xNrGeX0dDXfhCgi
iMvg2dxn3C09Pkz0YXUQPvtUua/qbZNXZW22sg1u3iKaQ0z4rgNLed6i4jHu9KBS
GjHrN0l4qKrr7C0sD0dl3MSL9M3IR1BJeJBLw43NW7+0X8EE58UWHB1vLemQ9vLS
AXsnXM5YHKBBWxlqXgXFsjIS041tTer2p122zdo+Um6cBu4h3mS9AoD8gKhq0q80
MU6ldCmyaZy+9E10HeNNyMt4GU917r+YuEq9CCb7AtpWtJokTCBv0Vr7tLt4Bov7
kinWnCF/JUuxx9QdjE0HzInkQiEq6XyxTkoUcjWM+FDRXF1KKc52JpaMYzeMV+Ln
VSJukwaVCmWMSEeKd0GUo2m/KQ06gX0DRoG7An9cDnTYP5LaNeP/KTliiBkLyaS
jddvEeTizcqKFHFjaanzeEYVavnFASxmd1D1jv06EBQZeovH7NkZ5T3QheRkr68m
lNyBDs4R1xLsd+PRZhdFg5fL/mgdzYcmYnu6P+rwgsQpQZpSbcu2rAu24fEbH9DN
RIe2Woz2tMIX6jTsA0BDRsDtXMWn/bqZ/lc5YaVuGsR0vFf6eWK9jJH3VkJZYK0E
ukwFrEZGSCWVP0d0epY19tIOU7o2BnQeVBA0as1jnr6gJWueoazZtgQHktiXo582
nzLC/zS+72a/9JaoChclM97ED534fqkND2SVHPkClxr/wRk0zqSb00kA/gLzis+s
RGZGMOsv9aCIMMUowMB3XKSn6qEXJvNHeN2uH8p5a0Em16gm5jyYqJlV0q5a1lhC
6vTbPbFXCWxJS1daqiZWtdVp5RK7qoUJY0CG8etYQGUDKsvUqr2J59RXJKA4mBR7
8beQL7SvDvioaHL7sgoY8Nx9sgCttww8MEAKvRnOkfD6tFURjivu8qz1tGAF/INQ+
RvGuw514o8giG+WU4Jcoz+QUMpL7SBSekiGnPE6iz5gHIXNtM3FUTgHTaCva87aL
Hh/idVK0/uV3Bj774fJhBrfLRxGfOPiaPwjdnE6W8p5colXpUw4MshD2zk27e2cH
W7hpS17FI427vSKU+9CYDmn71FNkb3JRP2Sy4uBWGBft0bmJKVvuwENpiL8D2QNh
f/tvY1zTXJTLZwWiV9vk82p12BKR6BdLY1hyUDEft+M0u1XR5hFmuPdbnEdDUX9G
pvvYvb9y9SdwjheYckd3F5R5TTEHTHDyf8+zYEbtCazNNmboKgpvd9z4Xy2RUJK0
4+BCmCC2n4VDN9Ztaf8zVnBCA6vxBf8kSCIoFyMXazCukX11pDN7qhvKQG+BomwJ
AK0UY20qhFKpBRcmiGkglpjaBeyDsX8Bd27lurTRuVry6/YR1cw9zAho0PPqE3bn
yFrSkQNaVCpAoqB1UitC8NWNsdCQ2h94w5Ai347vQf6S0R7SpT4zd5RNWXwV01FT
UkBkocfG9JIFks0apOpXeRc7J3quZEyo87to4U+12UGt1g77Q0aPT/n+StZJcNnu
MKQl1j6UB2yQjv0FWBtjwxay4Dn1CKbgLFBT5qntcPBJ3gRq/4Wa4M01kbDRdWVx0
LoLCgJRWI3aTR9FvjAmAIQju1vwCa8jNnwuX06Hf0Cgep2/uNeT6BBzn492brQUh
/cpZ1L0yvSY0gCDBGKfcmLXxbm6jVA835TQ456Qc3MX6EEVJvBv0zoqh3EqqGd2S

```
+fKIGwo1ruj6Pu7eRDzI5rNmIPbg640JVDnHxKCH0jhVFBkWGeI7EheYW49b7GPL
w1P3sM1A/67GXPJ67q9k0DZMPDxzTBw/iEnwT35vBaPp1RgW/dXXzdr6hS7kt6rd
Uxb5+ckIzCXX/BF1kh/yaXhQWAGNQy36g5uq77gWY5ypa97GXojuajqpjLrpPGom
P9TWl1raXH8W0zFaZXMa5xa3YoD9unQIzWRMW3ysobj0vIp+Fmj1gsI1grfbNI10
RJaC0WXXfX/3WuguukJzC8nAyTVM+Aj/bUZFoPgTCaZ37KXJy80RZjhUmZ7wMZWh0
lprC6iz0j7CUE+UyPUBDn1nIqWRc1ShIyUIvkGkvsqCPRseMR/K00bLk7PgHuq7G
VfDTv0YeMGVjrJUPxsydbA9zF6GzTmT6PWNfsL1r4wX38CQkKQzG/8IEGvYQ6xWT
kAdENyrFvVVE0diZgyCcybjTAI1LGj8n36DQBmfpYp1w6T/EyrznwS7PtRftaTm6
bI3eXQqn0+I1HCR6+1gqcS70LK+bX+Cw0sNzLaUy66XVm7/CxYJrohRkNRxTgkHy
cqFFL/wBx1TK/jhARfxm4kWk7Fsmo5t/ZRAv6jMA1YMjHdBF20HKMNDhZWtf/bC
mEV4/BERSfHB60aM6ZXWUzBlf486ffAvxsQy5qGjQ/yJIwAMN84qHZvqoA3NwIs
JThbTIFM0Xtux76AITxAyIhtB07ChxXrXC/owJ35oFve+sq1HQGH0fQIGTgtv60
tq82T7KL06ervK1UUVL6oxHkt/xbr3c6wu4wd2Vh+Kk3xn3wp7ShpT6sopk4GCdBv
mxxbUu50F7e7tlc/sxvCIU10bwiF6W0JH+7RUJEGmWpvt7eGFZSo/h8oLjnxvMk
Qyus5nGIWDZgKWYxxIGpQ==
```

C.3.3.1. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"

MIINawYJKoZIhvcNAQcCoIINXDCDDVgCAQExDTALBglghkgBZQMEAgEwggOUBgkq
hkiG9w0BBwGgggOFBIIIDgU1JTUUtVmVyc2l1bWVjogMS4wDQpDb250ZW50LVRyYW5z
ZmVylUUVuY29kaW5nOiaA3Yml0DQpTdWJqZWN00iBzbWltZS1zaWduZWQtZW5jLWWh
LXNoeQ0KTWVzc2FnZS1JRDOGPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1w
bGU+DQpGcm9t0iBBBGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NC1Rv0iBCb2Iq
PGJvYkZzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCMBCGZWIGMjAyMSAxMDox
MjowMiaAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0K
SFAtT3V0ZXI6IFN1YmpleY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDOG
PHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJv
bTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IFRv0iBib2JAc21pbWUu
ZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDlwMjEgMTU6MTI6
MDIgKzAwMDANCkhQLU91dGVy0iBvc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNp
b24gMS4wDQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04
IjsgaHA9ImNpcGhlciINCg0KVGHpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMt
aHAtc2h5DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lbnMvKlWLFuZC1lbmNyeXB0
ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUetDUYm3DQp1bnZlbG9wZWREYXRhIGFy
b3VuZCBzaWduZWREYXRhLiAgVGhlIHBBheWxvYWQgaXMgYSB0ZXh0L3BsYWluDQpt
ZXNzYWdlLiBjdB1c2VzIHRoZSBIZWFKZXIguUHJvdGVjdGlvbiBzY2h1bWUgZnJv
bSB0aGUgZHJhZnQNCndpdGggdGhlIGhjcF9zaHkgSGVhZGVyIENvbmZpZGVudG1h
bG10eSBQb25pY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUN
CqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmXS5CVIeh7j00Boq0MA0GCSqGSIb3
DQEBDQUAMFUDTALBgNVBAoTBELFVEYxETAPBgNVBAstCExBTVBTIFdHMTEwLWYD
VQQDEyhTYW1wbGUgTEFNUFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAX
DTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQQLEWhmQU1QUyBXRzEXMBUGA1UEAxMQWxpY2UgTG92ZWxhY2UwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCalsn6i8Gi44/oAVAn5Gnck4PH
HNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7m
ZjqQeb6FUH4i2Gmt4jse2Dqs165ernT905NLFf1HUjURca3ynqEBBV4DmhnZp8eD
hv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQlqdn9WZLh0A0peNZKGmVjveVy+8F
kyzC3jX/Qcm+ZLCq1LqhbWdHDz5qDTIIPVX1X3K7/cONxhvBbaU1/k1swdszUtj
hf1yFZ80RuQ3qFC6vL/PGewy6SCf58duq/A0EksCAW1b+MD8QH9Yj7CFsmq1AgMB
```

```

AAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAF1AwIBMAEw
HgYDVR0RBBCwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEF
BQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N
83cPMB8GA1UdIwQYMBAAfJEwnHFWyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEB
DQUAA4IBAQCBSXignLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjo
N9f/gsOx/Ht9Ii6zyBVjdaox644DsIL0QEP4YMS7y4q94RFFdmdzEbDLyX9sfUh
vdTxDN00oHz53PYDBh4zE4Nar2inC0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNU
RexTg+z3web/eD0du+F2MVtluLihne0Bp1GUTkr0mJBolG6dSYa18Hw8/ANHPyEx
156BJABb744gqoeuD9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w
06jaRzWdNeXz1Ec2tUpAr4vRhZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kp
o1w69Phqzpq1zANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLewhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBTBTIFJTQSBZJ0aWZp
Y2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjU0MTA0MDUyMDk5NzA2NTQx
OFowOzENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxZzAVBgNVBAMT
DkFsaWN1IEExvdmVsYWN1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
tPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pd0/KLpZbJOAer0sI7Aja07B1GuMUFJe
STulamNfCwDcDkY63PQWl+DILs7GxVwXurhYdZ1aV5hcUqVackPvedDBc/3rz4D/
esFfs+E7QMftmd+K04s+A8TCN012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnh
xBW2RZAeLqzJ0MayCQtwS1q7ktkNBR2wZX5ICjecF1YJfHX4jrnHwp/iELGqqaNX
d3/Y0pG7QFecN7836IPpdtTMSiPR+peCrhJZwLsewBWLJe3VMvbvQj0BMPeYlaJ
BUIKk01zQ1Pq90njlsJL0wIDAQABo4GvMIGSMawGA1UdEwEB/wQMAAwFwYDVR0g
BBAwDjAMBgpghkgBZQMCAATABMB4GA1UdEQQXMBWBE2FsaWN1QHNTaW11LmV4YW1w
bGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQW
BBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2
GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEA4miNqf0qaBpI3f+CpJDhxtuZ2P9
HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+x
h6oAfzc0zmd6XaVWHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD
01DZZukKYr7agyHahIXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHB
h0iPU7IPkazgPYgkLD59fk4PGHnYxs1Fhd06zZk9E8zwlc1ALgZa/iSbczisqckN
3qGehD2s16jMhwFXLJtBiN+uCdNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAw
ggH8AgEBMGwwVTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAv
BgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkC
EzdBBXntdX9CqaJc0vT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkD
MQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwMTUxMjUyMDk5NzA2NTQx
KoZIhvcNAQEBBQAEggEAmHzQqLkVTK18TKMaeYFFuU9fLrHZbg3aZ5eP+Zt30kIN
ErSsCBXE2V0u7yCmxk/PdfkTz0oSI9PW/seA5dd/W6yrCVX7EhqWWQx1vA+s+jtx
oZ+Fh5a1G09W7XmcQBvpjJQL0hyt78UzZt+CL0K5E5oueKj9CxCBkuKlgzzvwtP
XCAK6iYUzWGRWkxqdBaClu1xi20CEzu5mbpAUy8ra26hGGaExYIZRVbwNZ5uGjfCI
lsrsd5wFdxQbcW0F/M5QIjbed1Gz862IZxa0A/fRY126jdeJyG2VKdD/3XglLNx4
+6kU9F3BYb7itpwqnkY3MiKxLuofNQVx/ZQ1m9arww==

```

C.3.3.2. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy
Message-ID: <smime-signed-enc-hp-shy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:12:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:12:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="cipher"

```

This is the
smime-signed-enc-hp-shy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

```
--
Alice
alice@smime.example
```

C.3.4. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 8170 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5046 bytes
    ↓ (unwraps to)
    └─ text/plain 502 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-legacy@example>
From: alice@smime.example

```

To: bob@smime.example
Date: Sat, 20 Feb 2021 15:13:02 +0000
User-Agent: Sample MUA Version 1.0

MIIXjAYJKoZIhvcNAQcDoIIXfTCCF3kCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIEh7j00
Boq0MA0GCSqSISb3DQEBQUABIIBADmQPwawzwzPKIJbuLJ1LeeMRHXlIoG7j/r1
tvkHMO9bUUhT8jdexlAg11L7CKdQmfBxbMq/1AMUe8727BECAU/ZRqw9ZA+a71Y9
NfDivBgRdu0W1q1L0dcRiR3gU/TbvX5g9KEbQxT4sAqrVVJFBxPxKH1E3NPicFkM
2Cfe18+fM+o6+45xZgKrV3tT0+xsoJe00B0ghFEItp2p9q9+It0PnBCrFl1Mjed
B/5DmHDigcV/KcJqpQeZGifC9q/3uT5EIqoEq22gyTAg+q+SHASpbrUdtTAI00qM
MeS150u7Xr7oA++n5nn3KGm0NSbirWQ/luGC8txFEaEM1YCAHczwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAHFfMy82jaRS88AdeeTpXTcI5
eIWQXlgopLftZVNWouqoD0UNwE69mNURWUBUqND+ascj2aEc1SlzzZokWMzfAb8U
+HINE78pYcnd4PHC2EnMf6peasmfJwHgrNehJqy4J2WhaQpQD6em7S2wQXfCjxgW
UZdM8ouyXw7VMYd7CDQvY34VGxjWKooTwsSDriEL/CQ1ew2tjsXyznHDkfbFfpXQ
XtUciRQX+WHn6uZHDTGZ5/Parfp+hjsHmegmItt0N0Ggk50rh6Fw62+056k8W3jQ
Sgtlbqigw4/GnkEYBZ8iYF9dJuQpMV41S3tMcZzwM1FBTwLpW70gMeDtpj0JMDCC
FF4GCSqSISb3DQEHATAAdBglgkgBZQMEAQIEEG+d1PKP9Bv3wjYhP6kQiGSAGhQw
PgNipAh01AbBIDyP/wL0dgsWwC/KHSouWRESeutz2oMXMW6zDwFHWVVAHUX4uRmT
+ZZVEwiS+wzf3TAfd0Xs2kYHfhaiFkrJUxYirdyaqzuT11sVzKLt2F1+uxqud9JU
vLwZo7INJiiUYpredI3plWznCZd0NMhUHiWHv6qT2fBU1KPBEi00oZ3NZt0/ZnAV
jdM02PHAUwdnmqPLDNsLnsaNZ7i+b0rREgT1qeZ4xhRp0zSsjwvQn7d/WBCNDpC
9KKAP9P+Cr1216PTjQnFx4NrDNqpw2A6A+qv3NRq/ymn8zR8nm6zGLjje5RfftA
WVGQSajJNLTDIr5TUAtb3l07Cv1Zb8VQZhqxTJJrW3piWUTV9xjMiVL+h2sqdZ2
Lh0nQBNJmFHPukkdvkCPxbM+vy1JU04U+5ma+ZpD0BCgy5nWRgbQbFxcP5dpGkH
dZpcf164e23dKGNrYWK+gjVF0cp2VpEilgZCwJLJYgxnPH+tcoSIM7XfNe2IR1e0
L7pAhrzTrVWiBemph7271AXJM1tWhhgFL9GFWkbbQeJq2ndpGwz61K4Bk8Ri+9j7
fkXo8qt4xGECe7hjFHPiHcXr4FhjYRrk2h2bb4LPAeb7E56bE17XTT9hWCAoAT1I
lcfY8giqsny9xDeb8Bww/i7dVCzpFZCSNKxymnuWybTqu8kmnh4FQtTwJFvVDCoR
Xh2j6mM07DpzGx5v8E741f4cXwYKd10er0L7rBCT7worv50cH+Hf86Hgg5NzvWTn
ZdCioihv4Nh2w5EmLFWLcwP9tnMC+62jNFCih9k8EQ0s6uETEjN0vyFYWMM7aCIQ
JgF8fkEmAs690oU77Na5V4RrGvvyhKZv2EPGUTdwikls6YsYgEHRe0Q3hBVqrn/5
/Pm5m3Lke90D3ksmeasjTLBCf29RT+vYpHLLPYN1Jf1mTTKZmA6FjMi3yjlByJe1
TbrhXpmSx1oX6fHe0Mnq9JNqQEgrs2r17gyMULRxDRcVcSwPHYIkAjmjtYfR1Vb9
5XfK9/7bwNAH0qoXQ//tppHMFoyK59YyD/a0VvHAFyHvFxy/R63JkYd21X3AFevV
Ohk+a86S8/r1cSW5NMKMEGIR6d3sbUkoTKhVt8U/PNMqgTVbROv6oQQf6wB+VM7b
etSPPJciKCa0zF/m2FU/6HEU8s1DI0lioMgo+Q1YJrqWnAGLJ528Sdc2GTP0LKub
+zMRCZsrYzPHklw0PxuXa3hdyke/c6SZz890Nhh9jWhlk+1eju7NmNYhz3t9MjB
SumAvmHOMoLoY91dBwhcCnp+f4Y/Fx5NdIkj7VJVngCQiPQH/pi2LlgyYfcmqRld
n4ZwC4JZgjvz1U16Pd4iL6TTeHeQD/OtwxztqFqiQXZJyRNqbYYJyGZbBz3zFviq
aWahRK9rHYHVDqWKBy9SmyjiHmjVZluWXdK4zDkzWeqcwYHspKSYnymcBcrBneJZ
Hpy/bKK7RVNyU0E4V1duhaz6vUdkXG3KHIWCEppr3crlUHFB/H+CSQ3PXQAA7qNy
DvcD8jQ4TxDMhj3bWSaAKVL+SZiTBSVXX5A+OkGHoe57TDI9zKqJSmyh1dr6V8P
LiFdSfmGKA5sWuTsta9SMslWobVguXuvYTxE2V1S3zoHgB0p1efJ0IaNH0i+gqJR
NquG2fjiQpMQVYypG6942C6RXNUU1aLg3kH11ELT0mNRCw6EnL7xYA+xwwWQw72Q
6o9xUyrX9AqEv8cH4IMelIpkBue1hhf15eFpvB5y+cUlnv60jCaINXGXECNP1rw7
0mvTezWJXIyP1E+x438ZSFkN8EL5DqvbttkzH+0qcUCKwp2/RADofAsRwDdDuIOF
UQby6oDzqLTZHNWvrJiLkgquJ1iXWiKEWPApPgLc1pYzzBDFu0IKb//tjUznP015
lyCNpkazuJ2FGeDddz9jvWES5u3jATrG85wK4WTH2vjIh16Tk3210pwXeJP6M170
cG+NuQVPR2r6K1D1IZSG0f9/nsDVtnB5LePXycZIPtPoJYGx20Kt2IUyJj/00mxt
iGk3/KZsVJdukr8S6U/h5V70E/i5o3GYgG57iLX5DoA6uMTlxi5SEEv1qYMd/fw8
o0PCZw8N1kkkLxP4bKtMJJcAasns68CSu5kxC7bCynjEVR/Ea0Y07bAf6V+pDYyA
ABNLdZBQuYJ5r4G5TSS6YQQ/uh1z00g5tcUS3JPb3VYVXSthtpxaR6Z0bMv5tKC
ca4gleLxxv5qWetxcNTR054tCIREGX9qUX7HhIWV7cd3tiaN3N4RHU17nfy2mr5

geyQdfQRckTzuH66/a7czTq1VMUw/3oXNwqVVyxgyg4TJ7cHwfWx5Em6VCdUAeYA
r/pxcMM1wboDg3gsUuhwBPInGrbs7fQwe2LAJw0zXIjw61dGPF3Q6IJHZuStrGvF
3GH07/U/KW7P3aaVdBR484uaCf1QGVgkfZYLZntdAtH3uydDrhLot+DYUcD0RI5C
YIrZzUER0Wq2/HskDBh203LxGxAB+HABgzIw7od23AIzrTvwTeyGY0Fotnr8y6ag
a2TjAEHxSttZ7/YT/SiRHJVPDi1p8aptPKDQUZJS8P0yxCy3zNKANzcDkspdcT1N
R25mBS39o5ab7q6eKiNF6moGRxG1ZU1ghXYF0Tp6lHXv4YVpanOK2KKR3efly9x8
apD5Baaoo2t0mQ7Xb6d+NRT6RnrIIB2jUyqUSTADrnVQEsbz2nxd91+HFAChc+tu
7bn9swHrcgaBvC7ynFs1KIIx+UFPqEaOPwzbE0n5xGqja3+VFOEJ3hy0Q58N5Aw8
pgPavMZbWeBHwu8cos+FiTtRsNHY7KxYXPjirYRFU1d03jIwThwP3omjfs6cv0S0
wARwjaiLisgm4g8hj+7bAWjsXYNXbGhqeqbz3pYWYH5BQE0TIGdddXPjAFJs8hih
tn2b0XQqSuywiuX+RVXU0rPPoN8baZIqqLkxeAigsNzgFLhQoiS92hmoCsxgwoXK
EBGZdUd4Tq4V4BjhRXqdFf00E9jh5pY4xzslnYkxSmemSGqEbYUyJQKQntzx9SdC
gdwsNGOr57z00ySoHmwvChgw9RKZXDLF1MPp3BjIa0XwUhQP0aQPhXxSyogY28V+
j4cGogR4dSdR0YhVT7HeaqjCVHbpxC9BJD70XE19PEU6wBSInQVwddoYHgxJxEhS
o/GVU09kqqL3ygV75MtfA0SFu07RgkQY/geSQtdN6+DZ36LdP2xRdU43aICpyHku
fbUpAyIxpKYBndZakf/zvDSX67SvhIWRmSuv3VMYZSARw9WWifvQQ3RsYl6Z1hot
NbJyoRPEh0d+18Gj/Nyd2gR1TPzIsfz/jdQqfczTK9d8ewTCAQ11ddTaez1rmT+1
GInID99EIhouDeH97v46rJRtSTqRv5EtTfktlQHooHJWM/nRmvEFE62YqMrfT1c4
US4JkBJ8MBL/oB1I0F0SBo11SWex96Ab1T6XdZihJXStL2gGJgQNQ+0bj9GvFFYJ
uEv+LUP88Cv1MWHV50rCUXmUnuaGj6RLM27nL6pmXTQB8cf8CwkAlYP8pLzEn7I0
JigRcYCY6eevrctaIPkmmU7PKAB1RF/HUTdvelWzn60jF2idZKn00c0ks+o8IUpD
uoh14WwvAZnXbKZBWasPuw3VAKCniJxik4F8/7S3w75dW2AUmwamSFwNCpU6B5+X
9w083nMsnDbvRai7BHPmpsGmppuH9RHFMFHwiV66UR3Q0aapDoa1A6Xo6uFM3KtA
ytx8v1qaqmI9XyW02CySqGMR+d/Vu1opugr8jIrJCo1FGNhhj387FCeZsBGsKAo/
Lu6DgvgvN/DcipEafi108uJrNcqM34FGNL8IGDcWAZGxORNIyIZ3x7dnLpykaoS+
CkABKOMiUYHwEqER1BptchQ7za3nh2IzYFXbPs/dfkLEPE53+RMe7KiDoNDp64Qw
QrZqT8powhIZEVsacVKBe8ii0sFYK1KuAL11zfvSBFWfXJC3pHZ0JWqh1YjsATmD
FakLKn5FNuib4PXo52fcqz+EhlqxxxjXePjtIA3D1Iz0fH7IofCX/crana7PNGzU
5/KX+1e1srAhSMuy1PYSjJFeIQ+Hj63LkP0wisFSq5eAeSh6BbRqCat24xozeMs1
w5285nmwglBHXr9daIEyOZbn67Aa//9V+ANayy2sek4pdsTMyelCtYng/3e1+3yS
8eYxelFW4u/9xJs0g5zKwwKkxWUadRzRoYBBBjZJrwQj+/C/Ydl/xCXdCrzgX5tM
e7Nfgrs1Ed4yaAAG0KfRgOzmhinTnH9xwMk929d/zgcYtcpBh0LXnsbMCpc0sBlg
9YFQTAINMeIXRU5JXUs0xufbDR/XPbLy9bgyKBUUvSvypwEa8yvVaoJv01FxmC4K
Ne+843Wv0RR8M0QeTP3uDfqcw7Rc1if4Qa0fcZWpDGec5yqoiL8Rx6XpMUhxqZpm
KGw7waMxgP/wXouwXJNFvhUc12klVG00affvlt5IxJfLy6hckkGgsMaDrNduzziPn
j00ugt2EgVnAa7fDe9MRXF40PSwR2k62T+0dXRtC8Fvw5w1Qi9etWG0VGuwxPN
kMTVWt0HRPaaySRXw0hw1j2PGUBBJAb/bFfHAFHHLem3A2M32xWkkVo4y6bNGRq/
50XRISApwVZbpSum94VD1++LYrRk/u0XUBE0vHUEP16ICKKWXk6W4sFfAqisuPTS
JzqrIaQc0EEcn8c//Jyo4HtmFmqDdVeax6lkNeQekyJDoc9U87Gie9E8bJWZ9F9p
jXod0zX7SQjS+fQXA3vPeSixDq2+4rJhUzsF8aPxm3/HjutoLly1XTi7V1W15oh2
fpyHBPSp9E851ZLlf+c00X0A2HfixTjg7LVBwt7jTZhUt9P95PIYQJNu0BhCe2w
TOMcwNVigbKw0ZV63nSs5z0J7ZjMvr2eA0NIYCx5trzs1bplUMdspJVkTUp4bycv
qgAXgu0jMqxnS5ACuGIFiGRIyWMi6oVt/999wpSwJ71wV/rWZTgaAvU1h7lfqM/j
GxTHnuqVlpYPupUpNaHE97xbNbJoFTI77EnurLZssekD06jlzErtEkOvBZmj6KrF
StJMuCKE03KZo6Bm0agisDD6RF74fMxgQ2MyC3KeWpjbE+VoMEbNEEcQYW61kyUy
Qgt/TuY0WmMyrfyZJf6/xd90zn8tLRqev4Fv0tPxHE4qEGz1Rg3IMPkrdt0L/SI
B6nFxLwhsKLCzfoGY12npk4IaQsU2v5obj7b1SgNLhGGD//JQkbwNYP3UgToTsZL
QlpkEnAmardCEj4olwi0qwDWAZ0Cicf8PcvZYRuTl8yZVlpndx5eGvmCdEyEayU
2LCf3Iiaoeb5gF9BWQt9c0nFXb4iDjbcK4ijMbpw5IYRHaze1/GMnbkJJwzItJM2
LXbJSyVC8DvUYjyJsBu7CGJpd53lks2Mq03GFGVo3sDp8R1AUddX0qnvKj9je5Qe
pygvaBbAFn9NaHNQ0H0YRta9DEphGqMzjTgCtdQWhDHAUZ0P31fR2gcgBred6Cu0
gwoiXJxTyhx4Vqeb7G+dxq9/TpFgN0/M12p10Bz5yXuDPAP/D3InjewCSgw4rOrB
6/W13FnQfpngWY3Q/HvQRV1ArUbR0y/qf7amnQ79CPzYKUIW8xn6rD47ssNT/9i5
anPtUUrX02E8Wg5GeB3unBvqsRliK3tbS5u4pBCEHWrvHQuDJF3VenPdAag0pM/a
SRMsrI8ScXsz5XeZwRCckxIB/8GNwQuHsiVnKQ1tmBg9dn1DyxQfHyN25J4o5kSb
3hj/YtZk5pb0EtWvL0tMs+zBa83RaSWYaKn+sJESrx+pyU7YLxFKNmkbIVdB7m3l
4LXb9m0w5j+zXRPgvoY4hzVz1bTFqhXCKORncJjdm/2J1vNMjC/FioeA0d/oGwBx
/knz5VWDpbxcl0zeituHT/Y9iZ0TUwDncB3uS/sWn1F5yEIFrgd4emtibETOS0Xb

```
aweHBTxxZ0IuCYhtbyqFPv+P32bK9dAs07gVCCgrISA1TmTI9dRRJ7xE/P240BSZ
Zl2/8xJsMjaxDvcS63hfWeIbJRS3U1RRp9vZRBkggnutMrBu61NL/yLxPCS50R6q
HVw2Pr0MvkRvZx+RHQf9oT8tc9owYhxwGhweF9260M1HwsYW28K/IkyFIaMWw1UH
cxYnc2yPckCN5fftAdQXA8UNFBIBnSmartVGG5zxc1PoJCVax3Xz7Tgj+vISBaeA
HQHjNSzIa8APRIxE5jVMvz0fyvc6KtPLLgb0mvLmgYDC9rUVAuceV09oyLS1MsCV
g3j4RmMIsWPdagpYELQcwuek5e5ffD5bidL2Xn5B0XkMK7N2S11X1mWn215NZG55
PoIAeXjgNDjdMmCXSt/frUvTsF0PtcCA2JAcI/e2dsyAF3iIRvPpDPRfUsvEzSqe
gB60EFYkD0qcG7Lk9Hx5d78ZpJst+XViQAIDlgLHBpPuwkIvh900deP/XKLH/1lJ
y0Q9mQCfuTx6rBtj2216o2L920KFI27F/Ns4Lcir5VX0/6hrNe4/BlkAnexKn0gs
Ok3hIuQnB6C9Z2vtWt1P0InsemX+AhIJPtgRs6aGhMUnIwtvb8aZwFsS8WvaA6PG
uLKBuFuv5V+mjt5vNNlnkaaF9bMGQVq9NmK6mgkqjmjoaXP+8MbKHJ7cf2Kt1Bpc
PJ8uPBQ302Qv3PjpFk/YYdi3tmvaxb0lDkNCJ87xjn7Tlgd5jmbZRCdZxDBmb0s
1USxLB1yDN/k4soKAKL/Ze6rVusjC+GJ02TcWFQkS5eQjxoHNKIkU4fMDggw1vzJ
m5kyP5p5DST0+cko42Ae0yjn05T75MdYP0/1/I8YBes=
```

C.3.4.1. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="signed-data"
```

```
MII0UAYJKoZIhvcNAQcCoII0QTCCDj0CAQExDTALBglghkgBZQMEAgEwggR5Bgkq
hkiG9w0BBWGgggRqBIIIEZk1JTUUtVmVyc2l1bWVjogMS4wDQpDb250ZW50LVRyYW5z
ZmVYLUVuY29kaW5nOiaA3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwh
LXNoeS1sZWdhY3kNck1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWwhLXNo
eS1sZWdhY3lAZXhkbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFt
cGxlpG0KVg86IEJvYiA8Ym9iQHNTaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIw
IEZlYiAyMDIxIDEwOjEzOjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVB
IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogU3ViamVjdDogWy4uL10NCkhQLU91dGVy
OiBnZXNzYwdlLU1E0iaA8c21pbWUtc2l1bmVklWVUy1ocC1zaHktbGVnYWN5QGv4
YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhkbXBsZQ0KSFA
tT3V0ZXI6IFRvOiBib2JAc21pbWUuZXhkbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFN
hZCwgMjAgRmViIDlwMjEgMTU6MTM6MDIgKzAwMDANCkhQLU91dGVyOiBvc2VyLUF
nZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleH
VlcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7
IGhwPSJjaXB0ZXIiIDQoNClN1YmplY3Q6IHNTaW1lLXNpZ25lZC1lbmMtaHAte2h5
LWxlZ2FjeQ0KRnJvbTogQWxpY2UgPGFsaWNlQHNTaW1lLmV4YW1wbGU+DQpUbzog
Qm9iIDxib2JAc21pbWUuZXhkbXBsZT4NCkRhZGU6IFNhdCwgMjAgRmViIDlwMjEg
MTA6MTM6MDIgLTAlMDANCg0KVghpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmM
taHAte2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVghpcyBpcyBhIHNTaW1lLmV4YW1
wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uL10NCkhQLU91dGVyOiBvc2VyLUF
nZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleH
VlcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7
IGhwPSJjaXB0ZXIiIDQoNClN1YmplY3Q6IHNTaW1lLXNpZ25lZC1lbmMtaHAte2h5
LWxlZ2FjeQ0KRnJvbTogQWxpY2UgPGFsaWNlQHNTaW1lLmV4YW1wbGU+DQpUbzog
Qm9iIDxib2JAc21pbWUuZXhkbXBsZT4NCkRhZGU6IFNhdCwgMjAgRmViIDlwMjEg
MTA6MTM6MDIgLTAlMDANCg0KVghpcyBpcyBhIHNTaW1lLmV4YW1wbGU+DQpIUC1
PdXRlcjogU3ViamVjdDogWy4uL10NCkhQLU91dGVyOiBvc2VyLUFnZW50OiBTYW1
wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleHVlcGxhaW47IGNo
YXJzZXQ9InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXB0
ZXIiIDQoNClN1YmplY3Q6IHNTaW1lLXNpZ25lZC1lbmMtaHAte2h5LWxlZ2FjeQ0K
bWVzc2FnZS4NCg0KVghpcyBpcyBhIHNTaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjog
U3ViamVjdDogWy4uL10NCkhQLU91dGVyOiBvc2VyLUFnZW50OiBTYW1wbGUgTVVB
IFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleHVlcGxhaW47IGNoYXJzZXQ9
InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXB0ZXIiIDQo
NClN1YmplY3Q6IHNTaW1lLXNpZ25lZC1lbmMtaHAte2h5LWxlZ2FjeQ0KRnJvbTog
QWxpY2UgPGFsaWNlQHNTaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUu
ZXhkbXBsZT4NCkRhZGU6IFNhdCwgMjAgRmViIDlwMjEgMTA6MTM6MDIgLTAlMDANC
g0KVghpcyBpcyBhIHNTaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy
4uL10NCkhQLU91dGVyOiBvc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS
4wDQpDb250ZW50LVR5cGU6IHRleHVlcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiB
ocC1sZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXB0ZXIiIDQoNClN1YmplY3Q6IH
NTaW1lLXNpZ25lZC1lbmMtaHAte2h5LWxlZ2FjeQ0KRnJvbTogQWxpY2UgPGFsaWN
lQHNTaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhkbXBsZT4NCkRh
ZGU6IFNhdCwgMjAgRmViIDlwMjEgMTA6MTM6MDIgLTAlMDANCg0KVghpcyBpcyBhI
HNTaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uL10NCkhQLU91dG
VyOiBvc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR
5cGU6IHRleHVlcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzc
GxheT0iMSI7IGhwPSJjaXB0ZXIiIDQoNClN1YmplY3Q6IHNTaW1lLXNpZ25lZC1lb
mMtaHAte2h5LWxlZ2FjeQ0KRnJvbTogQWxpY2UgPGFsaWNlQHNTaW1lLmV4YW1wbG
U+DQpUbzogQm9iIDxib2JAc21pbWUuZXhkbXBsZT4NCkRhZGU6IFNhdCwgMjAgRmVi
IDlwMjEgMTA6MTM6MDIgLTAlMDANCg0KVghpcyBpcyBhIHNTaW1lLmV4YW1wbGU+DQ
pIUC1PdXRlcjogU3ViamVjdDogWy4uL10NCkhQLU91dGVyOiBvc2VyLUFnZW50OiB
T
```

```
LeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/N
kug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShp1cI3lcvvBZMswt41/0HJvmsw
qpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMhBm1LY4X5chWfNEbkN6hQ
ury/zxnlsukgn+fHbqvDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwG
A1UdEwEB/wQCAAwFwYDVR0gBBawDjAMBgpghkgBZQMCAATABMB4GA1UdEQQXMBWB
E2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0P
AQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSME
GDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgu14
oJyxMpwWpAy10vK6NEbM1gD5H14EC4Muxq1u0q2XgX0SBHI6DfX/4LDsfxf7fSIu
s8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2
AwYeMx0DWq9opwtA/1T0kRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gz
nbvhdjFbZbi4oZ3tAadR1E5K9JiQaJYOnUmGpFb8PPwDR6chMZeeGSAW++0IKqH
rg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1nTX185RH
NrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcw
DQYJKoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFmg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXRo
b3JpdHkwIBcNMTEwMDY1NDE4WHgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBTIFdHMRcwFQYDVQDEw5BbG1jZSBMbzZl
bGFjZTCCASIdQYJKoZIhvcNAQEBBQADgGEPADCCAQoCggEBALT0iehY0BY+TZp/
T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwdRrjFBSXkk7pWpjXwsA3A5G
0tz0PpfgyC70xsVcF7q4WHWZwleYXFK1QHJD73nQwXP968+A/3rBX7Ph00DBbZnf
it0LPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH16syTjG
sgkLcLcLau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxxqmqjV3d/2NKRu0BXnDe/
N+iDz3X0zEoj0fQXgq4SWcC0nsG1lyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ
45bCSzsCAwEAaA0BrzCBrdAMBGNVHRMBaf8EAjAAMBcGA1UdIAQMA4wDAYKYZI
AWUDAgEwATAeBgNVHREEFzAVGRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDADBGNVHQ4EFgQUu/bMsi0dBhIc
l64papAQ0yBmZnMwHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAH0JoJanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xi
idfZ2iLWYyTneuK6AChwKfnNvOFb8lV1iffRtF/KtmVEDMR/sYeqAH83KM5p3e12
lVh40HhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh
2oYl0Z/wvXmt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj10yD5Gs4D2I
JCw+fx50Dxh52MbNRYXTus2ZPRPM8JXNQ4GWv4km3M4rKnJDd6hnoQ9rNeozIcB
VyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUx
DTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTBTIFdHMTewLwYDVQQDEyhTYW1w
bGUgTEFNUFmgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/Qqmi
XDr0+Gr0mqnXMASGCWCGSAFlAwQCAaBpMBGCSqGSIb3DQEJAZELBgkqhkiG9w0B
BwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MTMwMlowLWYJKoZIhvcNAQkEMSIE
INdmPheiziYcbAwKeKaDpmu0QFmVMdAqPn4+xe0Fjp3NMA0GCSqGSIb3DQEBAQUA
BIIBAD0aQzYiNU8AycDkBBQVbuAjHzerZm027QlIZ47Cw9QfNcJ3w40RJAohR487
1NpkFskR79WY6aHuiLxC1WV0Jw/iuieAFfBZ8Z9t2h0t+F93M+9v1eoLzrgA7YZG
itp6r5zToKCdwN0c2futk/+dutbrTqYlFI8nnjLNqegBiGMMzVfateMc2fVnIVN+
7/4fyA8ASzseEis/HQTN7sejw0pUCvU4JvQy2klVYsaTZ04bdKXW86DHEWjoiweF
liiKSueA3WB1jeJRse2/g33dL+5++UUtQLY3kdKnM78705W0aFg03V57abGCp2r+
bgcHQNhfe0MXoJHKqYrnG++22tA=
```

C.3.4.2. S/MIME Signed and Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-legacy
Message-ID: <smime-signed-enc-hp-shy-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:13:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:13:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8";
    hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-shy-legacy
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:13:02 -0500

This is the
smime-signed-enc-hp-shy-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--
Alice
alice@smime.example

```

C.3.5. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#).

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 8300 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5136 bytes
    ↓ (unwraps to)
    └─ text/plain 335 bytes

```

Its contents are:

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline@example>
References: <smime-signed-enc-hp-baseline@example>

MIIX7AYJKoZIhvcNAQcDoIIX3TCCF9kCAQAxxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAAQIIBAGpRgu/+AsR287dW3Ygyjh1atM+H0IMy1LVi
g0Kr8xBysv4g5DuAWfNU5MC40hTQC/VzBNQEYq9XKLZojwJCSAz/doygseKYXqV1
I9Mwh3tWaoHHgLQxop1zY+AI7jWNIwSbTtn9W2YGTZCeZ0oV/7QY18nes26aNDgc
aRdEhx2jmlKxvhTcPfy7scICBSERea5SgN9uRAUihwsEvJRhx9vjngrlKwbGKMz7
ewpe0YcoY+gGRYqUYLKIvu6jyd5A/dDX2Tc8z2Zvv2MxYmMdP0okeAiie7diTHg+
ae9CTZN6HP7vbKHafTgcKcP7JT9x2PfoRLBagy1xFG9sy0DcqbogggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNMFUgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAN08bq23teHvwfECD/c01SAZq
OJ8aphPZfk0r4yftGe+uSLc/UUK5ipnFTHrUfmf78/BQmqSfaPRwHRhLREaZeFB6
aWgZN/DSe8BpkheW+2Y7L01NvmREQZLP69mwPg1WQ+phUc/NCUvz9XCMDbroiX5Z
XwauA4fjKKRhn25wdrb0EeVa5PRg2CjjpcFrLWUUTvDbEB1Qss0X467REyFg0QV
mSke9tdTh+M7IL2t2on4DILxJy9A+dVtwMgz8qd/bw6a5qGC+Hk6CgpskEfexANP
ypqf9iFQW/1lr1NhD0m80QLgm4PG+/L5nX/xsI3QkgBbpC7N6po06+W8Es5lgDCC
FL4GCSqGSIb3DQEHATAcBgglghkgBZQMEAAQIEEAYLQlnmoDE+1L9M+p4U5LSAghSQ
ukiRYivwnbEQfkBN8oIwjD6EBGHDfK53gjhPxRaaY43MwJqWoSjCQtJazc9to2DA
gFyL/s+lMGXxapd8DHwDXu9Sota0wZ94gJYSeNMBJy+QTjw0rkqMrurVqTr1Ds+v
55xulqMYc0w6WEAYdJwMz9TPsaHb9af7k+KNghTBUpteD+HGoZWGdOP/WN6I+zq6
HhwjXaEcideIxc32j8yT0bDHP3l242eFz1FNCHd42bcHtEDFGKFUTZZV02B54hcv
DRDqLSIIwAs4TmW7ajD+qcfM3ug5LRj3NJERbZyBjjxwXCDAA1P+3ERBc7KovqWC
0N0gBLcxQL97EA0YcnYuB9qZaNC4/Z9tnPdocCCMXViWkqGhfara1CHLSKbySV0QR
3lqLSr8S3lzQ5L9+GFw/om/Bto2VJp1AHWa7wdZk9CDdZKHk93eEGPHpMTbzcW/Y
L5kaD2Yw+vRFIM4ZYYgya+WkXh6SQYml+dAKlSXE1aG0nsTYk6odoanC6Jv9Az01
9FeNSeiH54hSyDNADjcuVg0Im8b64pZCiZ0c11qivK0mc//n3AmUT0k3+xvu/Icm
N+Jv2b1nYEF5jf73Hfv/xFm9ZuEfHLSxCtjtUcBmUyKh13vcoMw8iDU5gfUoTtD8
ceN5XkTFELM44cc9M5Kec28gWHYUM09wpyGiq9/Z1Q8qS+RgRZV210Yikz886Atb
v4+m6kciaI95EF5X790zgLjODR8JY5gS0fbCGdb94XtPouGASa2J0T003f9AAE7
rlytRgPHMJyY7G21NpSF81VhV1fY1RJZpPBbZ88tRvMENsyWQb+6+mMW/PrNy83L
ZxQ1E8gzA2oy018SIuRMgfYcSIGM831q/IiMTJI0cA80X5iVD4KnBloZLVcuQUwM
0WK/iGjJIgXDTsMLHNrlgZeulkfol/ryWU1M+CwJSetqorE3WBy4HxvUau8v20CO
pABkDZ29evve2X46KVmDDXGICE90+q+fanmX4ZFzMsVmPS81s3JQhECigYJ62IPI
hl5611XJzkC8lcp25Tcpcj jnvB3VGfdqDgTjmALJD4gDDgeGSWZHKWxEdIrzeXr
7yIoKC4H28y0tCwZ0UNqbeIVo6qcJjvTrSJ/ZD97L+jLQ5RMRwtGV0h1S5tTRC4
l3SmVX7qJbX3I/W1AKBGfCtvY2k/NqzMJ88td0RRmbVvNwFC7iioWYUCmU/97a6x
1v73Kqpc73L7DTkofya+zAgthQcRl0vZZ3Api3Spa83fYQc8kUA5n/Pq7P1LCbbq
yrv+2Y27If+bW0CNFP+4J8/hFdrQECTBhdGf5PtnizLORXFxCvZbqVdwN7jqocqW
U/gi745fcEOJjIMeECdhpY4sMsAaspFH21puSdUv/bx/i3Eaz4B2pgtL/t957pT
oATDNub1LFP8F/k+0Ml+LFFlg7YsbQG6l8Ki61xHyNp6HnK9Xjy1uLUIgTMV7KrB
DZwqyg17UJd1IIGBZL6tS5mX0Cv/k3Pe9raQR8MmCPNIuQynBB9JjiI8DqcCE17L
siRfTb0SPRR1GNmIIm+30H0B1IaPqPE470J9AprPe+tg2umKnD1MST8qOUQ2c/lt
eSBzmJBHJKp0S2GHIf0oDz6n6JvV1DUUtNi7LxJ0m/cjrTxoviMR5b8hc0Tvueh
nHtutZK2jr qGfMylRxpD06tRQ9cRv/svMlfXasc11apce0qwdGVUUVVxI8yvEwgl

MML9qVt8GIC3xMyU8UX1NhAC9iU3VHuU1i/mzIdVQmxXyKz/Csnvwe3jY44iW50z
dRkMrbr5JKf5HFGvucEsmz9Tiz8xzuiouxURAensZT8NastY2rmnHqAITbJc1TALo
cHow0MWUufyJRQgFoSVsQf5LP0IvSxj2dZ0k941MDjmH2M1Zm1ik9MQtbDwX4z3o
w6rlyBnUq9geh7Qt45nK1dyuoUaaue0oVq1HXt2qZ2w8f0DurR6XueEuakp15ty1
NrxDi3oKNc68s6jBnHbcRjlmqB3g1C/iA/D8gLZRcVDbM8kn+KGDMBJ0J/DHZN51
en1AddnXgI1sEo1NG1GWVFF1TCQuZpw2RohTcP1/+6yD3TS1BakjweiXKLahKNEn
t4yWxQiGurwT00d0VxUItt0d7s8idH4pxjayc652CK290v5Dz8ysKyqT+uIySPJB
yyWURsmPqYtoV80x1w11oWisBa/dpk6QhKSValX0U+RJre1p59WL7Bozte21Z09Z
g0uQEzaR38rByfeG1sExG1QJGcSgyELVUYV0FcdM6r5cfHlsqNjN2XmVw1Zry/W
JgJKuHaw6LCC6+1gmse1pXGkcpPLF02ZLBgDbC2AKZRT8e3T0j+SE53FQIyyZPbr
CjZ0ljtsWru+eWAlaaktJnRfokBpNCJ5GEyyd5asZu+oJXGIFZQNvQYe1FqLbrBY
Z4Rfdu+cMvz2Viw9f6kgAo4nDEBhkoJzAM7+1h0a5mGfaQEuL+kcMIRPVEbJ9kp
cWMOSE0M9TnLJ926fhtSIItZQOEItf0+Xs5y6K0JTLly02KdaCskyyIqju2AYA0hJ
UVdyzulqVURUIwIMCjyUh1jrmpCE7NtUx3/gXcxvEto9RjexlYHw++KCgoIZ5E4q
f/ZJjRMqBDu8CJpT7nHNv0pgRxp1Qg4x31A9ZDm6pdXF8U/ZNJrfSaSnaB0UUrLDF
wbeN7vdJsW/7JssBuyVRIEjx2vIfZ0U5y2yy/hbLjhh01jt2zkJZC2dxLBH64UFD
pGsL+lmQHSQpL3cf00dNyrx5h0wDoz8/rC5w4/axD70KijIbKcssgSHUCd1oWBn/
c+i1hdqXfT/obUCDhgFOMlbrbc9juoSz3Bs1EnjWft8unm+N8UaNuggTbCeujYvd
Mgh5eazSocQ82xqpwmIxvez7ahN4i0bLI58ZE70SyFME1yFL0/fnD7B/Dy0ooATT
wFWF+hBfeGaWdXpIbn0jTXjEpYchaWgN9nUon9DG1KYay4UpUSntUcnqI/CJEVI
U5FVWBaD5BY+nRymkTX9yxuB45z/AixvDMYBn69/LmcchIAYQeldMHwsy611it+T
cZUMtpemQoGqGdxP/uKkC0Pf5TFeq7v+1W9Q5ybxJh5nrHTAcupH5FJBsqnySg1
j0d3xIO/sQNTfCWBIjN0YuedORUKdieRYuJ6ygazkCBQCr1k7/r/sQio+F5PD1LB
J26sP0Ly+WXruQ00yA9tTRYiRgwqx/sjcv1D186kKMMKBNCVLYudFPsgjToIhsti
DASDRZXEW1XfAJSwT+dyaDz+H00twOH6In8SNr6UPnSsoXofE2Kh4U7DNTot9k39
s1AQBG6FtYfFE2qZ+r7oaHCWfkrkUUCgBUUJcKaGv7mZptf3BS9WEKSHBZboAxse
yOfszNnagB0qVPK6Yi9JLleXEBNSa0CQuXuLDzEadDNL1tcEKt/CWWXYcq4Mkqej
FyGNnNGoFRJy/ExL+IbaMVg9wmAhYLR7vmPFQ0me59CYtbaNr5y8818Gvu5EHba
g7ZEubaE4qFnGX+jQ5te7cgoJ4aR0Aeq6fcV9mwBK3Cs60eJpCv60LYjDXrX5a/w
PMhFtY+KCV0yfgIG69vDh+MSSsRKe7VxIawTJyhD0miF+iW/LA4zJKXgDdSXk0wB
+hECKChBT1BqF2SHE+8s80olKv3wbNp91cY4m4MV6+Rjo1x5eP28tGQOG/nx3Cs8
f/uvxTv0ijAc43i307H11HJTY0keEzEVcmXh7eEhASYJxAELpLPXCVDMuohNIAIH
VUCx+jiWESllycm9QmCf7ItjnyyI+cQFjzS5hVQDpSVLm3NJVR3hcJey800I43FW
gTpB41MR9jVDN/eQ+za+T9wNN16yKNKr1WXcT4Z6j4fMzoUdAmSVITjGGqy2vNX6
jZFI21ne81gZifabkpxmmCig6pDkTlHsHA9dB0lywBq0o3KQ6E7t6TIiJ15ULr1
Rr1vxE9jw09DtSIqJfK670/ERJtIVRwHCeyBgLz7vV/IWcYeYtVyIjhuMpWtPuoL
BUf/Dnmd22fJh/o8fYrNG/OFwWX805gqsP9gwzN7TySxw51nmeE9ggr1M8R9+qxY
hv3NK2I5rcbgraRT83X9qugiFFQtIAN0SZmP2Heo3YJ9MQURarmvkMOXytKhBI7a
+WAm3VxW44u1SoduDQl1tkKV1bEwqDzVp5RSRMNiN0RSNP+RLYmQFpK8UD4cZb2lw
uEmx7rvvQMLsmfmjHEnQfh610CXt0q/gtnvZNLcbAPkY4m2T0czYuA9cL2yWArZM
Ya84vxqvCvXwqlwIK18UxhOyGfYEUCUfPc2vrHPWt0iu/dTLdzYCo8gfA7aWK2MC
DUg66Skfqx127pFIUuZ96RbXyR0tG9F6mM0dWgyuqZU5Mr4S0yDyI1r+1ynQV6b
exdCUobNN+CaRyI7qktV362GBebe0iEe06wjrAAELXqLCbEs1Xg5myl0jVm+t+1K
2R+Jv8zcFsUCK9XfAK/029qELZZPc715bcXS+Fukyfr9wKvaRKc6u6WRJE02LzVZ
0ty5yfA0xFDKjxbYV/xfduUvIKVA1Z7mMKkgk951zD4yUJYfgP4NKw2IRXTIEi+0
DSRfmEPIj0FHn5Ae9asKmXp+jfnvA0v9sKezmrrsmMsWpFoFAGyuSy5ZyXgjIEnm
TnW1kJwqDYMiNgzTM/X+Grac7oXYZq9Lw8vvDSPdn34Zuveu12Q6G1I98UfC500H
V/76smknnphD5Smk6VJEP7bvfvTfJvPQJ0/xIoPP0LFFa5+iZ4x5XsnHkhNXTLb3
6sDsZ1VX/jpMZRO0Xpb04jNIV4e1CNHaBk7+UC50axW4KtMteG4F1mML/6yK+f4I
601UDiEcxxPvJfUDpkhSPSfoWLE43eJgbr0Arm4YKjdLYA2j+jAD1aqXNv81gh8f
7H1RVh+yiZ+bADj+Y2bYP98ppwMu9+zNEGUMBY7dG2r2WbzHrDBciTKQvy3ZsxFS
vXc04p7Y++Zirsxum+o1/sXi3Mz8uIigzE3fUVmbysVJ4ZYWBhS+/Nwv0t3ufxvo
Y3Ns9Ba1JD/ljbZGSEvFhpgClyNWHZLy0FFpZRvpCzWvV8pKmkbs4dyPFRp+cgKF
dXmkWfqf1CNh1GDg+0mW0+V1NticcM2aTdWjWR4itvpBPZir41YeSIYCT7blzoCx
NtlSnxNik0VaYAGNjYL53HS3kfGJuVpu6vwxCWJ6PIhkvJMW0/nrfdrrBLKrj5RO
NANnLc81IOci0EqE7GDP8c4HD2HxrFYY9CqrGJJAMDFuhAB+CNv4c5nqYBmkYefu
l/W1N3klgyxJoYP1m09J78zDhv8ZS9M36ofAwya7Wv8JE6UHE/1E1qgxg6vycFEH
zt0gM6uk7do50yHE3YVufmsulKXKdZdCEmGxtkFEC4pUN1Tn9sRe3d2CW4MFtriF

cHRlZCBTL01JTUUGbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNPZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4N
Cm1lc3NhZ2UuIEl0IHVzZXMGdGh1IEh1YWRlciBQcm90ZWNoaW9uIHNjaGVtZSBm
cm9tIHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX2Jhc2VsaW5lIEh1YWRlciBDb25m
aWRlbnRyYWxpdkHkgUG9saWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5l
eGFtcGx1DQqgggemMIIDzzCCAreAwIBAgITDy0lvRE5l0rOQ1SHoe49NAaKtDAN
BgkqhkiG9w0BAQ0FAFBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eTAqFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMASGA1UE
ChMESUVURjERMA8GA1UECzMITEFNUFUMgV0cxZAVBgNVBAMTDkFsaWNlIExvdmVs
YWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBou0P6AFQ
J+RwpwODxxzY60n1lJ53pTeNSiJlWkwT/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+a
uzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVe
A5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShp
lcI3lcvvBZMswt41/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5
NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvDhJLAgFpW/jA/EB/WI+w
hUpqtQIDAQABo4GvMIGsMAAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAdJAMBgpghkgB
ZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8
ASpw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAyl0vK6NEbMl1gD5H14EC4Muxq1u0q2
XgXOSBHI6dFX/4LDsfX7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxG
wy2Mfbh1Ib3U8QzTjqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuivZfg/m5fFo/Qs
h1HNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJY0nUmGpFB8
PPwDR6chMZeegSQAw++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K45
9CyqbqG+sN0o2kc1nTXl85RHNRVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdB
BXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMASGA1UEChMESUVU
RjERMA8GA1UECzMITEFNUFUMgV0cxMTAvBgNVBAMTKFNhbXBzSBMQU1QUyBSU0Eg
Q2VydGlmawNhdGlvbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5
MjcWnJlU0MThaMDsxDTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMRcw
FYQDVQQDEw5BbGljZSBMb3ZlbGJfZjZTCASiWdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2ju
wdRrjFBSXkk7pWpjXwsA3A5G0tz0FpfgYc70xsVcF7q4WHWZWleYXFKlQHJD73nQ
wXP968+A/3rBX7Ph00DBBznfitOLPgPEWjTtdg0VQ6Wz+CRQ/YbHPKaw7aRphZ0
63dKvIKp4cQVtkWQH16syTjGsgkLcLNU5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf
4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I
6ATKRJWJiQVCCpDtc0NT6vdJ45bCSzsCAwEAAa0BrzCBrdAMBGNVHRMBAf8EAjAA
MBcGA1UdIAQMA4wDAYKIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5l
eGFtcGx1MBMGA1UdJQMMMAoGCCsGAQUFBWEMEMA4GA1UdDwEB/wQEAwIGwDAD
BgNVHQ4EFgQUu/bMsi0dBhIc16papAQ0yBmZnMhWYDVR0jBBGwFoAukTC0fAcX
DKfxCSHlNhpNHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgaSN3/gqS
Q4cbbmdj/R40BEPr+gXT+xiidfZ2iLWYyTneuk6AChwKfnNv0Fb8lV1iffRtF/K
tmVEDMR/sYeqAH83KM5p3e12lVh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVf
nbhsp1rWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/R
CGnumghxwYToj10yD5Gs4D2IJCw+fX50Dxh52MbNRYXTus2ZPRPM8JXNQc4Gwv4k
m3M4rKnJdD6hnoQ9rNeozIcBVyybQYjfrgg4DRvW9Ksk220H4ConlB8f7R7s1LM2
cSYxggIAMiIB/AIBATBsMFUxDTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExBTvBT
IFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFUMgUlnBIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5AHM3QQV57XV/QqmiXDr0+Gr0mqnXMASGCWCGSAFlAwQCAaBpMBgGCSqG
SIb3DQEJAZELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDEMTUw
MlowLwYJKoZIhvcNAQkEMSIEIKHPvLfnw9dsDhrKZlaFW3+cbW6ewBQ6mkp22q7y
BhI9MA0GCSqGSiB3DQEBAQUABIIBAH3cRn5L0a7nqW8Z/czFCRpkU6j2e8xqaw7/
eCh6GvC4emq/eAgKhqpbhw+QwEOYZCMmTe7GFb/eS182QjB+zYaR+pGgVhBH57Zp
IOtobnzB0EsgzmUKakI2iaAuQBtOxMPqDRTRjMPLMhc6ddIRBqNeDpC3hm+s0Xrj
r8rQAMDBJTck7psP72DTyDWDeVPw7BRMSnxz7FwSbW1CXFeiJ6mWhZ0Va1YgDpJK
Ic2uW2Tq/ob8jTjnPrVIQhq0ZxKOiWsHTMfzxRnH3xyYt/c/huu0DtcF9P3j9Gwa
a23tU+PDSpfcpG5MJPe9DBzExWII7Z50Om8g6tZETD0+p0jNTAg=

C.3.5.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-reply
Message-ID: <smime-signed-enc-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline@example>
References: <smime-signed-enc-hp-baseline@example>
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-hp-baseline-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:15:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-baseline@example>
HP-Outer: References: <smime-signed-enc-hp-baseline@example>
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-baseline-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.6. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8625 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5368 bytes
    ↓ (unwraps to)
    └─ text/plain 426 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
References: <smime-signed-enc-hp-baseline-legacy@example>

MIIY3AYJKoZIhvcNAQcDoIIYzTCCGMkCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTewLWYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElnRnRzZm1jYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACjyNrxVYj1Xb+ACrx0kFuDPNhExlQkEjbJj
EZ3Az3gK6rWKIcIfSUIlwhqWJn4Vqa80/fHS0WRKaYuLRR+WBB0XszR6j+cEhHwa
MHYVoJ14YCg9+AmGbU1s2GNSrxqPFRFbrLVHCHdM26+7mpjWx6NhbtPTsZ/+mFc
BPmKu1F7rImdumm8nkaqdenbvp+AjPA82P38Ah6FTMUeC5ItSqr0WnvVMvcL6NA7
8BX/WlxEYVmcIL9B/EfRmC9f4nDYudwfMytHElddT9Gv7MejEqOB8B2+b2K0+z7F
DqxBUK3h5dXgIDoPadGkvunqnTLFak1JJyIeXftPK1GCnglXI30wggGEAgEAMGww
VTENMA5GA1UEChMESUVURjERMA8GA1UECXMITEFNUFUMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1UyBSU0EgQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEABvIWkrAM7mEjQFyBhNeJwopi
KUcL2wEHZJkKZxQcx1nzWdNXGhF+JCY5H0KmZw3fbcH4VnGPB0o1qC1yarSiLuH0
dfaZB0ioUwzLUKobv5u3gJ53vd7LwDvZnadXAWdwSXuxbp5XCRnK3UFE00/djZ6k
K037U5tydzJtCi484Yd5BfaQwF8UPW3/JNxFs9Kw+jmVGjWJxDToZAh1KNzILmk
nj20eZcUyQoCtmzXmpTHDENz60IJZJ9KvblhCpJ6owwM7818kOn/69ffTYR8dV39
Liy0KUISCODAVtTAsioyQQV/wBgwkmE5iTiLa6WKPogsbxWmGTjItDQm5Ty3NDCC
Fa4GCSqGSIb3DQEHAzAdBgglghkgBZQMEAAQIEEIZLVXkwIIv1TRvYBsWvNdWAgHWA
/OKrDfplfnq8JqXGW2x4c7ag9bUaeknbqenFEWbtYUXuUs/qEjYEnwuGoxs4KoP
14FjMC15o/IFDzURsGR644EvdxjKTgdzDIJ03SoUIz+RgdNgGCKGbGoBbl3t2PQV
645X+7uSfUqCpTceJ5zFyIZKoYlkdP+nqMSKQItXPydmaw01ipeVizufHb09Fqz
FZxZthU8041z2G1r9y8y8PDHD7EpgZpNa1n4vpma+612G06aIuVfoIxmJmi+Zbbb
yRfJcypPR/iY0M1H09ZvR3za35m3ffSBdE4P/Be13CBhE06kRQ8Wpvg3Hk5vKo3
0/FMT9+Ef4BZ01IkzUxK7BEZ0VsLK89KC96P1Jsp9PDe18/XbyW1bLsuLdMfCld
XDq+Obdtv236mRpDeAR5TNtcFelr35ZZf2KxFHnnNV1/OI+UEX7ki1w48m8CSvKm
KumQRm5+oQtDIYTqm0hiIog0mw73q5pS8oXbR+Am6sGu/fbt4ucE9qpU0jk0IkHL
4rLHAj4Tg2N0ecFBTECN+Ce/QMPQSQ0mBsoPnJ00dWt4veyxFlIxlkty33PsQv
ulcAF6c6Pvef61FSHx65KJVUUtzb66h2/LYb5zkV80ICa0UQxGX5hMg1METHvYb
108IwQ2eGbCyHBlErwWsUY4xca7WvTEOmYIDcEtIKwL3HYauTjn2qUkhzfXkrARI
eizjTTkxP2fPFCMRPrMD28nD0bKqS8ChYX0gy2U4WY9DyiZ8iKu6C3itXCFW7vkZ
Po+Isc1wXmwEqMotPMsjxuMtS4LTy8Wb/KUK4gY70QeBEp+u3zIBUN12b8LQ6ZLr
7ktrD9GrEx514eGfoNZZNC7+27Hh0wzFjHLSnAH095iilKTly7iwhcuu4bHNyOE
rq63jKdaABkDoktAaMcb9EYkXBmX31W3/rGtKK3NnjiImstxu44aTcGthbF30to
dcKyZrK2s/6/LDYfwyt2zljaoQ1F+ozCpcx2Lv0oR/Qq4M2DY9YekJ33aAD3QsdA
+JhTVNpWvXykQp/UzHzjff5J2XNGZrJtz7KHzXTATk0b3imqx1ct13J7kyuaKTem
HY1H51UegRyRef0VjAS9rft4fbelCUwzX8Mc1bLH9buDB0tIZafLHDjhlhLHaYsF
PmYFSDy7NsLPUjrHuxpyY355es2aKpvz3u+38N4ykveAY1Rhh4Z9HNMnSssSnyBe
TWn8LogACMHGp7QZuXqhchJMJZIH9QX3mxs4hrXliXivQ6vpsNnZDEBapEpcfckR
riuJD6mQV6y3mE+wjTiLaC9ZakKosB9W6465ca8F+bmlKuaaH0rJOLf4I9mJw5fV
7IFN6uXMLEb532cUE5bixUrIqWPyeX7mHfr6E0v94bLcuAss9dT9ny/TXLY/Fsm9
4DjbaaP7MtF5R00MyBS3p094dEF6lSkcZykIWMtJsqa7qIynZOBPOKjGgrwMkNee
llwFFD81SESUC/GS0Vr6I3WgMp7ZydaZ7KR7p96Gx78j6ZL19HsbauToON6TI/uW
kTSKVzZW8spUz45pzGDVKBnvD7he2d03poQJ16VS8YAPrPgbAewmqSA6vYU9TuUy
```

D8lGbx+THB7U7eY08t/PHCsD5MbJNBcmxX2PBjgPUqWIjz4oush8aJ17z12jkTn
yXecwDQAKk4CH7QqHlYgtam4+mK/A9YyDp0bCnPQK6KAvGLfNoJEKxe5KUfBP4D
+uzUiTu/Ws1ArHTABROsrnidewhpeUwCZYv5g2gc/i3stk5Dj/M5hAd+TDohWY19
9kYPRMvEfSMVR0rwwS1wv7gBZnyy+Ovby0sk0PgoojnbrQyb8tS0TTeCfXyQ2T9
1HIzR1cdC/58VaM80zQUuajYyMa7JshY1/xz01ynL1YY1uBuGpBIW3Wb+0TTtnbh
CHCo4/NvnSd2eDJPC8/n1Qzy04R7ML0wQATBARLtd2L2DqDJT1Kw4ZRrXX7qvwY
B4VUjtAwCnoR20mzPeioI7dYSf/dIfg11IoDHct++g26TRPW6RVoaVkPMFEqoaFp
L0nor7UoQ5o/pa1RgE4b0QdJ2PRZ/EvaAams7LkHrb/3HWhBSZ0Z3k1N7M5FFjPV
Euez74xXPkhYnpLFNc72RJ3tqjkAUbhbgvp9Nx7CC3T094iyy1R70ZhRnZhrvcv+R
9PsovDR+HvrFvxIQnFBC5rrkBXKcPMIobPLDDoawun1LJEq1D380u91BUupkMkvz
fdkRr4zGfW5x0FiIHMtoukrWPxad7Gy0jb/thROWPdSvbtNEKpfvWtEIovNio/H
BheLoM/6dbkvdagKwg4RhI674DXH1P1YKGTYPKjcoGrn3aYLAkDKK50E16NQSNAF
4j/CkJE8DHVye7Cx7ehNfqmBfgDXCi9pZpqeJq4U0CArNV3/zmMAKQMHfyXGzpq
7JsZz0E0KhwP8HbLHsV9qpq5ZUjZ3wnvtuGq0Be/itv8DTI5ezuOpX3cemiy9INT
hbFpRvDeGHeq9lwtgkWNZIS1x7BtvYce8dsDZM9tN/t2d6J1DtpIb7AjpWn7ke2
W1TN19C3MVMbXn83mwGyHfTW2wfZ0JxROWNfDssCGfS0BRodMsm4LRqQnc8MNK+4
A/6g2pMxj0wikABBMke/+Ygw1AEt+VKGcIexo/LOAoQDpG+hI2dRGfZnrKz7Hc4r
R1v6gaCqqErVonHFPNX8bGYUPrEwBxPwzjzj8bbAczwC0Y4KsZqfABysXUzQ0n0n
4JQ491uuydJJSbjgP0QR2ZuBpuRKf/m8NamX3LEZUfeixvSNzh1eNVL/98EhdoEas
nT1bfFNSbg5+UmaiQJs2z9tGJokUXtPp1PYKLgr6DfoPqUe2yNtrBn0SxDLZwN0h
RU7CoxoKKHQY8QtYdwXQioh5PGFGCzRloeUaYq4KDYr6d0D20k4Yu0NxxqYrkp5
RyBXAI/p3wpBK1p6lnHmybbpb2gpSY5HGmKDDq54yLZjDHM//A4I6T35Nx47uWS1
Ix/5McCzZP1gFHxjndRU+7Mdj20kBsSpdVZ0+OemrEtjJGUpXJoC5xHN/cxLQ8jA
gJtbK6WuZ7ShAFey946Z7r5xFtDhNqFTl3q8oHoiFPDW4qafryKcC9faC1KiP8
TDBkQZ3qngiTEvSrVkfASJEKFHfNSl4dgVK41YkUTMT9y04C0rvMBxHGhgxEVFC
eRuWXBV/RPa5y1RT7N1iaMDt10pBrW2Qq/BLw1jma42QybmDhsfGtgi902NBPdyG
SjgsMNQORHNQ4dUh+kTsDxaz09s9QDASGa/ePVbEPMsBVftbIphOWNkvwpC6+k10
oJZgx6dqxRoJPLXLF8qdaVq9sZJL9ISaLJqFZXflx8541shyy0zP03s8pzAGh9e+
u9oYtl+DwvBB+GoGqBK4zwGDReXBLQ5aJbq8QhzoHPnhlpfXsvssPXIZRX7Trq1d
z7J3iMJav9bDaAbuGWvP5jbmJ5GVypnjgbaDG094YxkScou2yW+t696iVJaMvadQ
bm+N2pgJDiC2yCCzbEiWGTemoW1irHPLnBugPxQinB4KQ+n0g6v4K1VbgZk Wuafe
LbQb9+bwhiz0YNinzaQ20fEf7qtEUvtJ1P3UkZzW/MD+eFRLHJoN40RDe10PaP2r
aM0wa8Fs2Fp0/8Y6t1GSEfZ4USeiivrd6vw2JWs8jKV+5E0SJwzeCmvi6uNqe8L
iJkkA684/Exp90W/ASQk1nEy8MvDrypH4UdQ02+Iyef9uk0L1wID7u3BChaikbdw
211Ph9caHNGSMxr3CJU98mQo7NytCSHv9tD6BJe+Ilt+s5NwxVg9JD++hEN/agKS
NsYFRdOAW6XPZSN55zA1ypsVHGGuWASMSvLogx1VDLzBzpnTXsidHavUwHI09fsn
LrD5FXDjjk3iU80/ara4Vkg7y5UI8RS5SnU/N2MYVvP17Mt83/ax0D+J+hXKRJ48
fk8TP859Ec9g2LMZPUCsK0K85adKh5/ETjNo8stdhWk0fdapisSg3vkdCT1Btr2f
kTrT7z8mX620vENI4EBP03tX6V9waWeQXA7ogDZ+arjh9eThdS+QZj3SpkAPPy3X
/FbPCaFm1IU07V8N5qCmPlb2iarjvGVbtNF1TosbBYQuJ/ztsPZcF8lQ+ukTw90F
4PxZmGtU/bmDGg/nwmIIZuLiAKBQ8MTViWe4nk6r4fdr7cpNph7TiRhG8fM9zwVY
QqJP0tvy454q73DqhIbMZixjINeyq4C7HpFp85/m0/cSgGdqfyDjVTV4koQb/RPG
XEEpOSx72k0MVUoRF1h083f/QiXZWdfIDTBbgjxZMtW4o8qG5xigFfAwptzy25GX
l+EMbxgD+YSf7N1zdV7zWBy2UgV90dFkWyD5J30ThaDJ+j6DsDRawz132INUWA00
WFBWH/jspgzIbCThPwt5E91flhm11qrIakJi9ivVjP0ZWGVm+L37CA8PxK5cWfg1
v+5a+HuU5k2I5w02C6qvqLhAhQ9jX2Vtvu0ej3eLNoFb0YrJ8M7ZbRemcitso64r
6rdbFn72FwTiGQdgKp7p+jkSIIdK+GWT61WVQ2ZPHYREZOMPGeZDtTW8JzjfjS6ca
DpxURVz1VUEwQYxd9uCtjjslmInatBKUmWyoRmMMuYWEzsr6RkjZo00qP0CzNSMz
PJGuRCrU8uv06/xFu7wnk19500sqAS2n0He6Ek3Y24JerOYwua0sLeEymWt+KSzn
uG5LWvVpgot9yfyE1HJ9bIvQ1/7qxKbXkK1l7c1U+WzMpFQ1IW10gi25n00Mr+H
YcYr6KdXizAhuPAjRQ17UFKIht7D0qxHh8e7+gEhX94XPX1B9PJsdSq2lm3kvK2n
f8/MRKW1RphqZdXHKe7QtRanyZMxbC0+Mz85U3iCkkJqfzTnXYorvFndTC5YBLQS
PFdlrhtUBgx82G1MC/OnDgF5RwIRBZs1+oZ46cgJxVjr0A0pWmYVfQ2mUmV6gqQx
k00WwRGs1cXN0KKfRITPbrIge/+68dwtR0ftuYMPZ5wmCCna2LbvQYGcKZ8NRtQu
Q3/fDGSZMMQo3FC1XHVDV1BRg2qLapJe9VZM08RVx2vBcB5IIVceNPwkZDPATtMd
lPBVNpwHnb5JIM8xiDHomjhPL8P0AuuMMDcmUsj10JsgwyqJaRI/JlhoFsMUh9NL
7jNcPyuk2YzizC5A0YUoa4X0pwLVmRSHQ5reedn8v2oIch9KuIT6dewcELGQHdHR
0Y7UCwOsQYwXCIYu3Njkss07+xrmqrffdgJdq7sf8tXZpBqh0QBtmrqydbnx96JQ

```

HRTzPwk+X2Lc1d2jd5jfQmyk+m6MyB11rMS47CGs39qWyXs5rMr6cFyHnQYfaXR4
o8rLT1A1f+K70A6JrEM65Ka8YkeUzSiNKDgPq/0ThItAFe04GH3UpdBpoiT2oezy
rPL2ddLfMr0oiYIHJwSXPDLHdIYvbfXveZUJoAZcE0USPxnKvYb1A0G7rRj1ahw
bRdQ/v0q0LQh+STRCZiFhws6JbGfFiKLH06TB737Qo4E4XxZegQFIbwgg7Irc/XU
F4fdteW5pMhEpGC8Im02j6QCs2Ls9cJEZo0LAqyJYXTxWgUATvy9gIoG/99AuG80
wGnqMQmYrX+swf8QAK9wLxE4wSs1ZGyc8oWqyF9mfwdLSx4cfa1R94930CgI6hBS
MEFA1TBVDKvEr21D74f1S/8Ya+pUD8Gxxnp4MDWtHEs1s9w+0c4UDgq6S4gcMMAE
sTry3u/D/hFZqRX8M2y7W7Adj21FyvC8Mm30YCbX0GHF1bie4AQ1wSiS+fjEvvvt
XSzRoZuULU9HIjemb/oLmVzs3Bx/U5n0If5ucCbUxCOA+016rHNMMmYQHwpu4rbu
+d7wMRrtVWLEShy5awYotV9XLI7chZUB+pXh0BljGA9h4DChE9cwwHJGCEwf0utm
63/6T8uNwI90I0LAPbbbABSR8na9qzrpV0STxuG2TQ9Qh7cCHRnIfE+QRJuy6Xfc
rVhLZB24G1CEPf0kys4RPfrcHFbFC/rAdiF/KIjD2vw3oXdcdd2gdn0FrJ9fFPfM
ZMWKFZKSB0vUFUFAyg90jMS+J0MoG1Dnmk9ZtddhLjh/IiTInTdrWU+T02XG6V1b
/qNEFKIw6vbaPwoLzowSepVWptogqTnfCaQPPFuv70+14mNTL6wi0ufinwhHtF5
fvuhUkekixn5M61+uE7czfflyZnxoXTzI8YhSdRnVCCrJ+9AV5dyx7Cr3ELipGLB
20KWNHz8V/GddKLN2Wu+ls0CPiss/bCKW+UJb4wtXJz/fHp5gkH6qc3EqZ7i5crJ
ozY9n7Up6WSZgvgzWET0JCbcHsL2+wStkSaRlhTycZB52cNJTACi6uXEYy19om8M
7BWQ2FvDTEUJDawB+rBm+XzyL95ySrXhLhTN9N71U+Jk1CDBf/zJXVbu+NDPhEpY
7hTg/P/u83DbXkUR8w0Ja1nSjA8ze+Fxt3fbtNPSzG/bC7Ut+rGkJsnzBBYpTUjt
dbDoEdjj0cj2z8B7LSLdEdtlueLKLtIdYFPDdca5CjoEzja+4I3mNU8FxF/CC7Ci
KIGaRgwy1JW9Lsi3Z0QM1jnugR0RgsLisIU4yX9pog09EvWmo00wj7kuM40VGggg
y2/c8YlJji3JvyBayMj22CrUtBv59fPz+biFloYe1nHh6jGJB+zxSobKpEZ0UMGk
1Q8k6PKznMicR0M8cummltrtNcwK13470zy0VCisjIq4j7YLFskUH2Wo+3WgHdpN
wUaSTXpE2HR9Amg17u0U7qBqBkCC4nbArddaw9d/Jv6IxfSgX5kyDK1X8Nkalqvh
wT59c0w3GXz0eS3eIfvu5R09o+d2mfRH+77sRkvPIX0kM/bDwZH3cPtT+YEveqOK
8RJTQDeLMqSX71o1+VC+975x2Wsv1z1LBpWiW68tXLj4De9Pp805BXnfBS80vJFY
JMBtAg6MIVIQyblv+QxnYX09CGCxxjqka1PehmYpafcP100UfU5tSqJb4k87MyUj
NRn6yYcJXJBAt1LMRG1LDkUTN/mswR5Bzy4NnzThZb62sUZ23xwKJV0oApexfBVK
rJRaEUaDx1upyGfMEVuiImlCT1aYIXBb3f/W2zK5219f2dbAFU0goYTKJoohBzGL
tJ3/d05jLgje9H1AgZS22UVUI+FQo8uG8ApJgts3AW91fjohjzzYCP7T/zR7x4h
UERWGFMG2fHYje5/QuyobVCKt8QfG2DhVSiMDPB7KH07bXJdEmUwb/aSeggmDCp
LHK2foRU983nLGdDrp2q4TWC0MGVSm0wBasUjVhiUA8=

```

C.3.6.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="signed-data"

```

```

MIIP0wYJKoZIhvcNAQcCoIIPLDCCDygCAQExDTALBglghkgBZQMEAgEwggVkBgkq
hkiG9w0BBwGgggVVBIIIFU01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUUuY29kaW5nOia3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtdW5jLWwh
LWJhc2VsaW51LWxlZ2FjeS1yZXBseQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ251
ZC1lbmMtaHAtYmFzZWxpbmUtbnVnYWN5LXJlcGx5QGV4YW1wbGU+DQpGcm9tOiBB
bG1jZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NC1RvOiBCb2IjPGJvYkZzbWltZS51
eGFtcGx1Pg0KRGF0ZTogU2F0LCAyMCGZWIgMjAyMSAxMDoxNjowMiAtMDUwMA0K
VXNlc1BZ2VudDogU2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86
IDxzbWltZS1zaWduZWQtdW5jLWwhLWJhc2VsaW51LWxlZ2FjeUBleGFtcGx1Pg0K
UmVmZXJlbmNlczogPHNtaW1lLXNpZ251ZC1lbmMtaHAtYmFzZWxpbmUtbnVnYWN5
QGV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uL10NCKhQLU91dGVyOg0K
IE1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtdW5jLWwhLWJhc2VsaW51LWxlZ2Fj
eS1yZXBseUBleGFtcGx1Pg0KSFA0T3V0ZXI6IEZyb206IEFsaWN1IDxhbG1jZUBz
bWltZS5leGFtcGx1Pg0KSFA0T3V0ZXI6IEFRvOiBCb2IjPGJvYkZzbWltZS5leGFt

```

cGx1Pg0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTA6MTY6MDIg
LTA1MDANCkhQLU91dGVyOjBvc2VyLUFnZW50iBTYW1wbGUgTVVBIFZlcnNpb24g
MS4wDQpIUC1PdXRlcjoNCiBJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbnMt
aHAtYmFzZWxpbmUtbgVnYWN5QGV4YW1wbGU+DQpIUC1PdXRlcjoNCiBSZWZlcmVu
Y2VzOjA8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1sZWdhY3lAZXhhbXBs
ZT4NCkNvbRlbnQtVHlwZTogdGV4dC9wbGFpbjsGy2hhcnNldD0idXRmLTgi0w0K
IGhwLWx1Z2FjeS1kaXNwbGF5PSIxIjsgaHA9ImNpcGhlciINCg0KU3ViamVjdDog
c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1sZWdhY3ktcmVwbHkNCg0KVgph
cyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbnMtTaHAtYmFzZWxpbmUtbgVnYWN5LXJl
cGx5DQptZXNzYWdlLlg0KDQpUaGlzIGlzIGEgc2lnbmVklWFuZC1lbnNyeXB0ZWQg
Uy9NSU1FIG1lc3NhZ2UgdXNpbmcgUeTduYm3DQp1bnZlbG9wZWREYXRhIGFyb3Vu
ZCBzaWduZWREYXRhLiAgVGhlIHBeWxvYWQgaXMGYSB0ZXh0L3BsYWluDQptZXNz
YWdlLiBJdCB1c2VzIHRoZSBIZWfkZXIghUjvdGVjdGlvbiBzY2h1bWUgZnJvbSB0
aGUgZjHjZnQNCndpdGggdGhlIGhjcF9iYXNlbGluZSBIZWfkZXIghQ29uZmlkZW50
aWFSaXR5IFBvbGljesB3aXR0IGENCiJMZWdhY3kgRG1zcGxheSIgcGFydC4NCg0K
LS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KoIIHjCCA88wggK3oAMC
AQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECXMITEFNUFMcGv0cMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkwIBcNMtkxMTIwMDY1NDE4WhgP
MjA1MjA5MjcwNjU0MTaMDsxDTALBgNVBAoTBE1FEVEYxETAPBgNVBAsTCExBTvBT
IFdHMRcwFQYDVQDEw5BbGljZSBMb3ZlbGfjZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBABJqVKfLwLjj+gBUCfkackTg8cc20tJ9Sed6U3jUoiZVpM
LcP3MUKtLeLg9r1mAfIDlB/wlbmadXPmrszyidmbuZmOpB5voVQfLiLYy3i0x7Y
0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0aGdmnx40G/e3p1fIKM0dPzZLo0AJF
5m500xzXPL74zFCWp2f1ZkuE4A6l41koaZXCn5XL7wWTLMLenF9Byb5ksKqUuqEH
AMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z
5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAA0BrzCBrdAMBgNVHRMB
Af8EAjAAMBcGA1UdIAQQMA4wDAYKYZIAWUDAgEwATAeBgNVHREEFzAVGRNhbGlj
ZUBzbWltZS5leGFtcGx1MBMGA1UdJQMMa0GCCsGAQUFBwMEMA4GA1UdDwEB/wQE
AwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj80e0r83zdw8wHwYDVR0jBBgwFoAU
kTCOfAcXDKfXcShlNhpHGH29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCsTKc
FqQMPTryuJRgzJdYA+R9eBAuDLsatbkt14FzkGRy0g31/+Cw7H8e30iLrPIF1WN
1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMT
g1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PFb5v94M5274XYx
W2W4uKGd7QGnUZROsvSYKgiWdp1JhqXwFdz8A0enITGXnoEkAFvvjiCqh64P1hIe
Morj36pgL19oWZD6YrZSWHuZ1F00juyu0fQsqm6hvrDTqNpHNZ015fOURza1SkCv
i9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqG
SIb3DQEBDQUAMFUxDTALBgNVBAoTBE1FEVEYxETAPBgNVBAsTCExBTvBTIFdHMTew
LWYDVQDEYhTYW1wbGUgTEFNUFMcGU1NB1EN1cnRpZmljYXRpb24gQXV0aG9yaXR5
MCAXDTE5MTYyMDQxOjF0YDZlWNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJ
RVRGMRewDwYDVQQLewhMQU1QUyBXRzEXMBUGA1UEAxMQQWxpY2UgTG92ZWxhY2Uw
ggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijS
NOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHUA4xQU15J06VqY18LANwORjrc9BaX
4MguzsbFXBe6uFh1mVpXmFfXSpUBQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4D
xMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3SryCqeHEFbZfKb4urMk4xrIJC3Cz
WruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog891
9MxKI9H6l4KuElNaTJ7BtZcs17dUy9u9C0gEyKriVokFQgqQ7XNDU+r3Se0Wwks7
AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAAGCmCGSAFlAwIB
MAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggr
BgEFBQCDBDA0BgNVHQ8BAf8EBAMCBsAwHQYDVR00BBYEFLv2zLItHQYSHJeuKWqQ
ENMgZmZzMB8GA1UdIwQYMBaAFJEwnHFWyn8QkoZTYaZxxodvRZMA0GCSqGSIb3
DQEBDQUAA4IBAQBziaI2p86poGkj4Kkk0HG25nY/0eNARD6/of0/sYonX2doiz
cGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAZef7GHqgB/Nyj0ad3pdpVYeDh4
ciNKjbs+aEoTWgAkoqEnt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf
8L1zLFXBuo2zL3HR+M9CDr40pq2JCKzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+
Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI
364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEWbDBVMQ0wCwYD
VQKEwRJRVRGMRewDwYDVQQLewhMQU1QUyBXRzEXMC8GA1UEAxMoU2FtcGx1IEExB

```
TVBTIFJTQSBZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phq
zpq1zALBg1ghkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwG
CSqGSib3DQEJBTepFw0yMTAyMjAxNTE2MDJhM08GCSqGSib3DQEJBDEiBCD1m+B5
0QBs78N2wRl0kf1Exib4redr1foUWvF3vmcyCTANBgkqhkiG9w0BAQEFAASCAQBc
m0fLRAACOYr8JymCYS4CYBWzMuTqh1D0at4MTroQLeNXvV8NijRWYdbHFcL1hrdy
uLBoqHTkv29eG3Lp5+Ah+uYLcPeamzoxWgfiLgPBaFSQU8ZyxPqVRj2xLq2EqG16
IW5DfieHgVN0bv9P+gmRdKdzG8+hiZcZXBm2aJtN8oifP/ahgTzePiBiHK4Qvecy
q+Cr1gFwVlT+1t/2M01tGqif6R14NCmUaHze0vzEpJs1H1E8W7yUjBdrS3my9KW1
fAv+chp5rIXeSrZGTg7ZhNLcq/ug1H9IpgnYvRXN/f6WhggdVUZ5BJwPqbNcCJF1
zAP8CJk3IK1fzZulSebk
```

C.3.6.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-legacy-reply
Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
References: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:16:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
  In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer:
  References: <smime-signed-enc-hp-baseline-legacy@example>
Content-Type: text/plain; charset="utf-8";
  hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-baseline-legacy-reply

This is the
smime-signed-enc-hp-baseline-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.

--
Alice
alice@smime.example
```

C.3.7. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#).

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8190 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5054 bytes
    ↓ (unwraps to)
    └─ text/plain 325 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:18:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy@example>
References: <smime-signed-enc-hp-shy@example>
```

```
MIIxNAAYJKoZIhvcNAQcDoIIXjTCCF4kCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTExLWYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBQUABIIIBAFak5Jw4mFC+UC84fvpvWVuVYa7lz/mqUPw1
jVB8JIsTrvGAeVoW5Jm9cei83og4JLMUOIxM9WAUJEUBUApScNRBgW0vSyl0qB8E
4VdNXWLA0Hsh2LYySirv0yxb0cGuvoWdgGx1q1UmgoHMcwcr3o0F9Y8HenqQkE/L
aplaZ7E1TW40GmDmuxxUHUHPER5QcS3UKFHM0rQga7Ecnagzlw7SLiIoFNw0FhMb
oqAbKADbMdgn27Th0oroxT3z02GDIHLaYa6uP9Ive/ysFPQTqjKZhd+6TETLh1/p
0SMix7NDaUnm9YiZYIzsqSqwKTCWYqgBh17uZ0MrrooZNQn1rQwggGEAgEAMGww
VTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMcV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EGQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEACpVIIC327M39MPcp0ozCdnwC
eLqFcDb59GdezAghfnnv5LE38ZBa8cl4Hq010yIE0CQ1bpW0NRbQ4qa62PEHsRaHC
hJlBhkOSs5xw/C108RRPsQz01t2j5hA1F9Khe8z+OC+TaLBFVjXm7v6S0np0GHSi
Rcy2QPTCU2xj/4u0wGNQ5SMxMg9v0RmnKs7I5fLHJDTgBQ2p+YLGp55LAIPQIA3Q
QD4TjlsZrCYCK1RK/qj2/0p+1lf9X51VPUE0kttJ2qu+1PWJXQ2+FyB/zh244v5K
fnD5DGok2NK96pr3HT0JTRgTTRgA6wKF/6t1E00BZHRqr1xhUL/d4ZMkfsjpdDCC
FG4GCSqGSIb3DQEHATAcBglgkgBZQMEAEIEEJua4/oTK5pBnB0FVr+FDv2AghRA
Nff06MgeUXY60oPjjAtWmKdtLrY3CCr/ii0Po04wnBngRfEHJQNkqJ01g0Scq1+w
eFP5u+7znmTLC7ib9Y7Wed8Kp0bxTISfyLmd/xByN1fIuDyd+mejL3c509Lnc1I/
Kng0VGLxbQekkITS14iBrwgIv0SsNDBAKsVpyQDvq2gk0yR+e3fTAKFtDpEovs63
48iKvZu922TkdxTjyp/wQjtB91VlWqPDnHr+boJ2TjGZomEIAwat3mA4+ESIb0kR
0qPjglFqu1mH/XA7dvW5y7PqN8WiUKf6dBnesRIjv9Vhq0a30FqdzYdKy9KpnXU
zI3o2GWC3xdGJ2WhX0L+J5hvW22k+CIGrB02Y+1ddESmC4gsr4Lq0Sz71er1r7cR
```

qSc7URaQqefd240iNaJfKv3pkTzUYXBncIlovijegtz+ypzbv9h4Ejr6CyETCqwV
+HNC9216ptAGhG4aobQ4cEgMx6AYgVWk21gXe8/ZsXm7xWmkdqAwCNNBUExd0QNw
cSFAVI+0IsyPSOUBTyA9CL5oQkODjviiy4lvswBqjJYuQEGQnNZffMuuNKESJpA30
kwBPtVhEba6fK0HpW2XStVzhpg0jr/J80Hqfw4aTWFuH0cZb0qNQ424FSAZdNbsb
mUQWOCpVzdM4tGM27T2MbC0z/ux9PXRqola5/YcLkjm0ji5hntITDmBTY2XgvEgC
yr8UoUFJ5xEWFGQMcyUkN/WNF9MdGRvMqKpyKimRqn+1Y3imYD0Q1GDbXsufJAEj
9tFbxG58inPfQ19m+oQ4KnMGH1/wZisxJGzZT4mkB17155+wfATa2Vk35gnHZJ04
8CrdW4k3y0L3Av5uDk4XIOWBrK5xMUF+ESceQ32NGd/PXaifDe8P5NnxBYw+5Sr
+3+Ws14v1CUZoDAEvCipqNKIT5MV8wrSADE8WC91DYsTeRWx7dxeTdiIOQzKhaUL
8rjgmWF2+Smm0HL8eX3ibROVzN14r6V3BKGJrbztHT9kKXRCPsOmpA5XLsObNCXP
vqcPKIk4XkzLvPgZ/znIa9bhnPKY3BqphyLDMVU5p/1Wp4UIztLmiqEGZLkphCM
pa5zd3r/C7Lk8EqOGIA8TmwY0iuiWZX3+Zegs155QYs0BmSS2/2XKyPGI9+QPond
SOeyEJaxUhtJtXt9mqae9doxL4jzLfc2IW8Sau+WmdVXmyZtxPxDP9fZc5pME/dD
uL9RE774krvPtGvpI45BIAIKVxPpaliCEURf2U8QpDBcCA03hml9nY8t5nPGV1nm
gkV6DVWiWJkLPCS13a6l3faIQUWR/ERLku0omu5zFToe1Xq8oxN/fQeVETMNasiTQ
n+ReCFvdcMbR3aD0yoC2obz5BImvIXwde7Tw7VWYRuu0gngluf6C1sv+uvURHj9C
eu7asNze8hCdhvkeVpE02ow+ou3nstMsbTo2xdjXPG1Ia1F0/kbZj0A1V/6E9GhG
6eSV36R177bj6pJW+XIkyM0UHUNNZoSrxwX6EuL/+P0nVA72tyP6T0ZubuJtSSk9
IeWI7Tt614PGdFj0UT22v8QXbfSFXXSH3A+A6DUX0Qn2Foe+pB5sLQBdrD3iJmBpv
j6hN2rZCd+N5WjRANUpToD9f82BE39fm8Cx/Dd1ZTSsBy7QA5a/Ho4Emu3mt00za
gUPPgru48T+/qZs2TAZ0i3Sv1Rv2orXrbUW9UWYv/T8bD5ICggHVRmisFbZyN1h/
ZBKZCA00vVq7hbPOAYC1b5/Fc8bHXk4iK1WCt1+4agzA/TjPZmN+6V4DFdJBLf3L
EPvWW381ejEIIeGx9wgMWiDxc7QZAIGIF7n9yKrtUeGgz8D2NF6P5cweiFJ1U5zz
VoqIyxwE0yySPz1ItRl6rkztn69yDBfzUZTaX4oWxLyVW7Lv+F5Hn17HC4H/I8By
3aWPHbYUXuSXvXvXC+R287Rj0yNi0efGQm+kKA0n6386fsw7MvJ0tCGIzLwdhWMf
TZtKSTOQ7753xxcQVx+4YDp6TaPx+qgT5MjS6baHVaUR7YX+oFQkY60bhh34fmzw
q5WA0MQH+310MbhadPvC6CcDtdz37iHhaGbMf9fc20JY2VMMJx/unT9KTtYh/avZ
OD/7sLgkVCKkLbtpHchfHpGvJkTA9cx0/LEyXKTb5VLo+pC5+x9CdoGvuI/hWve
igy5BF3wxfGK61pusCXS6VRCJuG+ohtg1iQK5NRJA0W2JX60AlKaiRJawB0IFQu
XUrr1leiCD4zJHNixDMkawai7X5TtcvKj0fhiRGifRULn73UFLl6tAo8Fy/hWGC
qYIFACU8RjrlvDPVjLiFPQCsDuPrxe5Nst7bI+C8LzeqI73pYGaK4kSNTSMYk0E7
Ls1jxKcRVh602gA2sNoRRxirScQsF2UW0BKWpKXIunzvL4SgzHo4yuS0U1H44M9E
kbR86G/K1jXKBNvNw1H/ou90s5GgCbJn76TxVRzpeRWAKOX5AhU20QYCB0MxZ19
wRD7Ehsv68CzE8Dw4VBIjMku4D2jRov3fu2LGmreQG4MJEQjwUNx4xyHNTfr7BDp
5Z87q/rCa/GNZX8zDXi+FrEy/4JjM8j8V7MC6cGMnbAd8fqQPVPQLtcHUQgGbuV
Db9gQF573Ss8ttWm6n55pb5eUU7wLgcH9YbXdLLQEntJ62HTxeKY/HD206bCEQfA
zqb3/MWYIElvUiIci9hGZCowzcTm9+JCry3/JBr3hkZ8+0Svor/x1HRjRqt1YW3c
EvuyYXFJ7/dD6yHrqdwJG7AhJbzbq47Y4SUTWpDtpM+WHGaQFj1B7JVP2iYtxsDa
nTLg7Ym6GHTH5ZwizjKZLDR9WBwaOPgpkn3JMbI2pYLz8p/69fdOkMwud14iE9+
iThb9nf2Z6iVhZzxpSei1EGh/5EMQHGLIfcrZwIu/vuk6GGIGYF/ktUAdHbdengs
PqRYP0tEaNQF40nG8RPLPi0PiUlxvOKU14+7ChD0so5Y8fVDRlgK7GCJ8lfi4LoU
DLGF3sto76A3RgpmCjSh7fSk7IYRiZm92KwTGssRhFPnABqskxw7rXtDcA0g8uU5
sND5d41btT6GqAQHwiYrfAQN8cIZd2WBSiGZG1w7/KPRxcoiatkGD1YJd017ytbH
QI2C3m9v1GpykX3b4sYN3SkHU9GSkeAJHHA3bnXlzbmsudhAL4Q19YayagABbdA5
VwzGFIZ/43ybp+MQYx5nB19y7RwxDd2N/kZXXaqq+9aBKLvhpOpngBbxrv0jiuH
e4SaMN9a0xJ1oiYufu7+azgIcQia6cDTLr8jgYXACpUvZkZQAwkmAvQ1IvLjhv2X
01nogIyWfhNYxJqpxrWexbtg9TYHDnr9JxAdi0dfrMIDx+r10MmF0Sd+Cp/LFMxD
jaR0Z1Gug4CAuydpdypVnif+a3FiltDvtjIwaziKG8J5Qcm1X7+7gv+RtqcLnsaxv
70Gd7o1XbiAhNvEUWbM2wxSM+T7zgFdHI8cEjU15MAT3Vf2gKxGfQibD8z9vmW9r
HZV9eN37q1QY1MS+r02De5jCLdi6WcMP4CxPaRbbzXPmUm3bDesOf2CZihf+HLru
RPNI4Mg+xy1N9VcMVsx11S1N1r4yMJdQubdzS722gw7GpIaxVjTQbr6qAtE0xon0
pUmaRwABerAeiFU61t+uAGeP7dCG5MkfL69YrBBVf+jvZeHzcnBNtBuNvBhQy9er
SHL6Gst/Uydbdc+VCboDX0FNb7FgDzD9sN8tkBhP2vYEu1pe0QZeVZBIvJpipaSO
PJ0VaqpP6Z8Yj/afEIf15GY7+10tKiFew4gTIYAtDEUqc935yC9dvH2wjVv/OVSu
yfIpxao0AcjGCRdByH/yhl2cwvydVlCjdVjnFi8r0NWjuBozKcjb9urpJvdj0boZ
GHE8L8NGsjGQxzT7oAiTY5VfYnmMLPehsKXNJ84YYsRvK0P1fFk+YG7AATKrQQRc
K/R8v7ymePqfC88281jZkVA9deNoHgRdjZDx155vjH5+DX36K8DtS1ANLavnZLi
uvl1tHl0pT0zPd3XpFyqz1iZUZe+M305EBpbDn7VayM75MwF02gJhlyKEG0BFAA


```

2XyrE182tQ58q0pRZy5jW8jcaZhn84NuJGIwhmAoytcW5dqVnDvKmbQZbqiN/nhu
yJ57eMnAfr4p13MtFbI6zAZLnsZ2Re0m0TgNk62F7QR+pg370MYNvp/P6Gong8zs
3+hDKpj8kfG1GgDf0PNzdnRGsnEcKDX5DpeaR7o43PQAPjIv8ESov7Xrbd+zilQ2
E1haaVh4NWRPT91FApiDLQY9KFSGHeb/Xu3s+p7xZWmqgML4jgDXzcKCKPTuKDL0
qg+CVAeFLOG95pGrdTo30iUV232E0DV+Ozh0F67B5GbDu4M27cAaCJoZN39wlz5Z
C80bYjd3XAJfGiBRWRSriu+HugTDUHS47oe3bJMSRd+qrQaU0y9cCqw0EgvQm+9u
rm1uTM3aeDjZQ8oToV5tc720xvNRdv0d6sZP0StUD07u6IXSN+S2eSxw+jB10jQ4
lSkXBKppi2HW9Zvm/PuDdWA5cYRlgre+rxvztbg7KMzRheKJE9tz52FPybJftvyZ
1J3j+g6u8DC9WLetCA0/HXw3aiGF+vuBeaJM48jMNRxZGd3dRmwALHsRV53mFa5S
d4f8F4kTtXrqBa0Di9qPMKznp8Z+BbXtI602Lv3IdPEaboyFBVJyGMfXINDmuyIt
B3fWbEC8ZsZ6AxZN1nemckf1MEkyhNC4pwZx73nQ/qNleRVsbjXTX6qiGlRtaK0c
PZ5dPJFJuNeoCTtowqnsK7eElb/qKWr9SbjUq/Kmnl3aFWxo4+P1goFnaZmacfEH
mhs4vTDHsgKmbB6rkIeUAxxolb6TzLD1ZqUS/EWAJCA0gGJSctdh7W17CwtRuL67
vygwTQqekNi4P7/DGo45zhCj0sABBAQZ+0i9fVwAP9rTc3MFgb72jTfEizqDSfzo
h0FE+9X5ssuYZUyPUi3VFC0m4Qxv/LVFCUKa3CskcssjhUQkbXVX4gltDigPRFms
7xV95x9/ME06RzEZTy5IRmWVImePuKn7lH+TCotJDxpHC+BmGxuMkuS0qYSLwlxD
wu00876bUHHdfaJ+JfAs1c1aC76AmL44AfI0eBMOqPxaCD+VdCKDsTbU+vEA0ZPe
gi6f6ta4DNMDGk2unqrGGYacY6n8ZOWowI40/Qtyq4AgQLT1TtVq7CYq3K+vNVc
vRvbsqwQHVKEwSA5iVV50kb6YD+q1obEcjJRN+zHNC20jFDZMPaPRJiu5hk/JLTx
71IRKblxaYqfb0/TSNwlRezonDJWTQqvIt5erHXjjGmSYTddadf+dVsaLbuQv7u9
W/XFZZA/zZz+mhGHYeiRmMZ01eyxXCXiLKvc2DnXwT6+MMo10SpdgHgApfpd0uV0
yeiwtlTGUD+cJJcnqk3rd0v8rm76ew3TpixPYh4xg9HBeeJKhkpiVowg9ihgUge
/L3zH1iMiSk1+fPbqFGmfXbLJ0sy2G83sIgvE4/88MrA4+mKGB8zORJhYdZ8TxuZ
r8GNW3hoXh6ov5v6jEYoGd3XJwsYcJJTtWNTpWmZua+u234unR2sAxwYw3q+w8yX
LjsK9n0XuhcZNTZyGIUEJVOBeb67nMK/UhNiFRYQAKEXJTv08vAh+gzFgDlHr4+k
z23Z9v6Z2v1zwxAheWcYNER+Jyk04FiP8toA1qYPhx1jttaiFfXxdHJWs+soQjv3
/mGD8vTogVJdGjyaJmab7jLTbp2zvMMLKqkN1bybjZRhaH7rftMxoD06zG9Ca52
ehAhFfsiEjUjZzcUx9ynvBXsEyV4rpRzCREUA6NsL7zrYWIGSVeLn8pDBkk3gigF
JVg2mN9P0ZYS1Zlctw90h0UXhCViHM5+dceyMcIEUmMyFgN8yDe86sPSnXqJ6cYQ
xAB/TzIsoWddbLUNNZK1WnRaarXx7tU/2iEH9iR3A192b4pZ1126JfURFwhECP/M
cY1Q3lHSMB20o9RRWYvlpSgck011EcMwLYYIYxK50RtsmoL7PF10FK1mYnTvPTyb
NntoJ/mem/T3rnmXTFP1THxs545BoUFj2fCYjWsxXALJSht5gH7rQ7cFFmNu3Rv
4dYWF0R9Cb5+JpY7MoAhXk9k4PqgQwn84XUuqdIYPNU/PmB280bGb3e3zvihZvK5
nHjaAs/k6Z40gQZaAEBFD08yKlMTYYH0F/I0/Aey+mJe1n8SvWTVG0XTFZHM459z
kb9o2JKJmBKTH0PHFOI/dDXfm4kbHvn6T1y70Vke30RySdHxxTXoEEchkJ65rT01
gJ/cA7EJSIzJ4DpcU1Kk+HBVmv10HX63NSTBEEfWrsWdoEUaktVHmTTFxnvrtoH
LPnNUdEXJae+0kE+EyEWce9MbSPjsNFddHADNpxthy04hbvQx6/YrUrK0BHGtzDI
lIdeatVgx1Ib6XS3UzfS/DqHx6+FCGZ75ZYM5/IwlyXkNzXXibin6xqAL3UFAGob
kGeAoKE1bo4d4TJdoYafa+9KxU8DH8fQvMrFFBtS9327I4qWfV4fzPG81opU/+d9
kkK0Ovwf99h4aMfflT0Y1bs8/mLmABnZiYpDe4ZDIwoicqGsQg01u/dRD7pHWt
J9Hv77iPBZMmURHGirKk0hBxYlRGUFZm/6/Y/aX4vG/1K+A8l2ksWdLpQXRQpcuD
kqIBlcn++x8pyWyY1STA0F9w1IFp5wBHH1fy07yNBDj/xKMufz9j6hrYWQV8bjWV
TK3cb8Ar2Qr80TrUUCjyu+d+37kcsi2uMDkiRD/avJbLPwepFTuJZe7nZYdA1A2s
hxnJyBasTI4iMlxH11JYuMGHouu24u5BbCILf6541R+BIQ1d2ogA41eHP1Z7x3H7

```

C.3.7.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"

MII0VQYJKoZIhvcNAQcCoIIORjCCDkICAQExDTALBg1ghkgBZQMEAgEwggR+Bgkq
hkiG9w0BBWGgggRvBIIEa01JTUUtVmVyc2l1b2JogMS4wDQpDb250ZW50LVRYYW5z

```

Page 135

```
WTANBgkqhkiG9w0BAQ0FAAQAQEAcmiNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6
BdP7GKJ19naIs3BjJ0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+XH6oAfzco
zmnd6XaVWHg4eHiJSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukK
Yr7agyHahIXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIAe6aCHHBh0iPU7IP
kazgPYgkLD59fk4PGHnYxs1Fhd06zZk9E8zwlclALgZa/iSbczsqckN3qGehD2s
16jMhwFXLJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEB
MGwwVTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMT
KFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvb1BbdXR0b3JpdHkCEzdBBXnt
dX9CQaJcOvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsQg
SIB3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwMTUxODAyWjAvBgkqhkiG9w0B
CQQxIgQgMahPfXerTJKDWjCE/01lScBMuyD7DptAxoKsAmAzBdgwDQYJKoZIhvcN
AQEBBQAEggEASJuMfoErHP+bowktPN/yJI1tnTlZUibkbJxhHPhR5EgNnn3JyMoW
l0yP6nJyH3sBQ2/CIBkmMSXmg+A0PFv3w40fUtX2oKVzT5TKnNsIDtv2Z7J5JRI3
TbATMRmw8VItmPGFCJsD9nXRc4cEgvrvojXSfv6bWp5hCO+8WNadiiGZNdoZduiL
rWNSwO9nQSXuNkqNo+wwaXF9Rynh1ZcazsVopBB4s5XuJ/Zcbbsaci1w34ywNCHw
5xx9Cgj+6+yUsFp33P2YVgdfK4beyo0ZK27Rm9e7Mpi6QxUi+BCR/8DB9svZBwob
K7iaKJzRBDx14Qt/m6VHxtvkTXjkOOD+7g==
```

C.3.7.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-reply
Message-ID: <smime-signed-enc-hp-shy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:18:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy@example>
References: <smime-signed-enc-hp-shy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:18:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-shy@example>
HP-Outer: References: <smime-signed-enc-hp-shy@example>
Content-Type: text/plain; charset="utf-8"; hp="cipher"
```

This is the
smime-signed-enc-hp-shy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

```
--
Alice
alice@smime.example
```

C.3.8. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8690 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5418 bytes
    ↓ (unwraps to)
    └─ text/plain 514 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:19:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
References: <smime-signed-enc-hp-shy-legacy@example>
```

```
MIIZDAYJKoZIhvcNAQcDoIIY/TCGPGKCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUjNBIEUENlcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBQUABIIIBACdv0XrIiYw0QFiCZ4pb4VxZQfPk+g7Kb7bD
45v1z22kXF1sbp0rdYsJCfyleCEN88RhU/gzDpyLHY4ESXAJ6fEvKWJn/1kRZEX0
LFVzbE3f5F1N0x0cLKa7r7Au0ryY8P8fvBM0Z1sgZTo0L135JiiKm3RD7IKXCLxg
onz7kgGCrkby51sdsGAQgJ6rvFJlmvPQLdmi9Y00YpKiIR6wfAUu2mH0gBdEtsot
k7UfAlOQ+AZXA61VSejFBwEWwKMSk1NiAj6S9Nppn+b0zEI/1qQsVJcNNcdA5kE0
BWRzQFs2f8HzaoitaeLQuI4UPjnasy86sX3kl+xK9MCE9iSASZwwggGEAgEAMGww
VTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFNgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EgQ2Vydg1maWNhdGlvb1BbdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEACFBy5UfVv+8iNnM1Zr1MISJ
ygBuy12da1yDyv3d5J9E131g6QoJP1lmkSC81oxIYPQGdAZ10IEDBWW6bkgPGnZP
tL07RkYkNTAUwLJ5Ug2tKADNfKkWOZ4bNa8SbxKDMgx5CtleG2/u3X6xw0DEA5N6
m0s9vDa218FWKbe5wSKAA5mToCzWxE0zLLLKHL/a/7p5njtYxneRj2iRPSA0FmU6
uZ1c2UJDmd58b2JlRuxTxYf1+jJguej0/j2YannWR0w8LcF/jEXrMUn66Cux0LoZ
JdFTc5SmrHnJrjuE0U0jw6SW/R/IIF32XXEX7/4VF1tbjzD8Xr/Meoch17hTdjCC
Fd4GCSqGSIb3DQEHATAcBg1ghkgBZQMEASIAIEEH1amtLrDCmloM6pbsnGLNuAghWw
x8bEDtMcmKRFac1sZQSooeU5PEKfwtYxagFordfhGUM8tkgm+ZIGq7mujmTz9AmR
rwvoKTU7j43XdwbT4QPzFwNZm12ay7z3qQm13q1R1wNNQgmH/KWiku3iFYzvF9g
017Io10kAfgcH02XtPxPUhKxNjxw2fSpELB4o1SyET1qpHQyrCf+4m4BK19M6sa
AwqBO+gj/hv2L5TNq21dqsAsTe7uNpM0++gJZqm8MQ0dmTQrd0f1wxr3J6KRIB5o
JAFyLHikD5fKyzLaWfLaUPp361rISZPOHodnHwYYQUuRZaZ30yABi/5KmpXu978A
ad7SagBqg3ni8VrVKHPz7b8SngjPVWYOn1CjUC9jQ1XZ0z2mGeaP9ShiW0+0h4HC
```

Czm9z6RJ+4B2pkkDtnPvxZnbB7VeMmuJYW88GfAka4HxSdMU34PQioy+egjdcPm1
0wIQ059A+mZBDhEYdaNxLjHvBL7SBrV+Asfuwm0UmGgTXVnzRbd3qRqRt8UIU10+
H/vMN1W/HKeWvjsg3RAjFCY5B01CJO/+bp0I7JBQZn2p2Ke1hNTGThUCAvBX+0A3
9ivwOwws48WoynTr6M2upt62lpFqI4FaXwv6/M7UoprWrtppSMdlpFv5Cun8RPb2
ZlOGKcrHxEZJjbCA5uzPu8VrBAj9f0pM4pIcyXBtpboRBRWct1FH+7N6WFN0dojk
yu0Dty7pRnbpaZyl16GjzByf0hUssuWbPp7V7moqTYqIMfkr0WW18j9G/Ri5LNU/
gpuGBREBhW3VDmya1axW3MegAFu25WTxtJ8lIeE+BIKIdtEE3jhFp146KsG9IPc5
6Ctb4kGm2sI+106EvkP4CvMo8/ZGwCSYLCsLwi60X1RA4LbAHgwCx/UsXNcYXRAS
oEmVh1N9C4exEvVW380B9KGIjX7ViCxjwaXpPhrnLNxLWQLBAPm58+4DgEa/jlN
rHL3c11S0/HFbJ+3RxA3jCE/CVFe0foszrUnz/tSLqeoLxyeGixIEutTwIag+5RX
WuIa/vtBI9om6v2Uqwgvi jipC1aFwBZBjZXRDXzj04wbDgzmXT9uGKSLwgrn0wRM
Y/k0SITHuRKMAYAnRqTj0xtQdiUznIMLKCRt1r qe jCLREGUuTowoJGgpYlMq10dPr
Qx10qrTEG8pCMFm/GS2kdMXvSnINDYFKiJUKVoIDEzjm43DhpIN5KGQwcfChAGX2
gf4T0PPGHVokXsurrqpLc7Uy3gSajfc9/4VWrALDRfBPh7NsXgWf1Mc0p5eIU8FG
i3pzph/J29SSN1+JAiIfeSoIdX3k5oHMGHwhKY4+H7U1RX/XEdNsM/twQpeC5Ri1
9WPx7ZcaQKRVT0vBmIlGJFYBJY45emZcPaKMcN+hPue9Yt2+gQXD8xKnh4IGbZy
a6K+v1koEpb9VrRhGjSarX8CzsnDlGTyJEfFru+qbYN8XYT8mtSUxbLYsnRo/skn
BcT3tHz4hi3MS6KjJkcXw98dyH1IkJgYACsv2GjyEGEZPR3wadJP6Jcig9xX8Ga
f10uyyDwTM4ZsMj8PiB+wd0KN/JmgGU5b1wkTcc8cV1RCmiN0UuqNAHsC04pn2Qh
yhfdZU0518m0cmsZQ6fRu3UbVu1HjZZH1eGjxiPwtGutBo8mh0QNOCPb04a2sza
QBOMx5uVsZoqB//p6oQFQZdv18nOah4T8JhoSoSn0br2NgJYSgLER/WzucP4zk5s
o7LgRt1b+IfTYnw9FLUvOHLs8AB8TWTpkk8Pto+K3CcUyJMKYjbg/57teYT0T/U
/aYB+CuAatM7H0c03C0XcvfJuZsXExSdu0NuW/VYSwibXS7tgIu/w8TsfgZqAdEz
k+mCDx3NeCukg/t4/7ju3NPe8RqhU3lBer4r94jNoPG1VkCve09bUQw/6PAVmpes
FkbJsAB1UTSCimrgZlUxQAnndDFZCdU/rmc8ogRCmHtxrgzGyHt803jd1EBQ6Ct/
rb4PcotIHQALRsc3dyL8BkxwW0N+nuB3S1xfr4oo0v71EeAvZn/nizGGlxynFynB
DSeXi1NnMt+8ZeX+jQbPDQnNAONz1QG7LoxUXS/7AIEf1V5MmWsgen0SL128tj
8xVC0X1NUvTGVKcW73AXZ8V7oI7sVee/waRo7Sd4T4yzg0lSEzvRepNecB10smdnM
Z7VPXoazVhQJN5QpodedrL0dRD5Kwifgru1JsDNHxsM1+cLYm8rx7ajyhof0rk
Och2PNRyu14o9ts7jpPhghyqwg0P2A18RNHB7YcsPiy1MUftIRExzUZ2VCyYRK40
DTCK6zatynXBEbr9o1QdeQJHAYUF+D53RUJzDD/vTD1TpW35D6xY5s7PxajLaybc
4WMcZwJcLt2u+VznKgwLRCADESBE1XqScu7mfoB3jpc3pepdApHcnj4T+vBX/OwW
L5Icn7wcMRzdcfP1XlHii+WriJk4GM8Xn8HY4iK15csC1F5TxbPIT6r4SVdRoCFX
zpxEoYa3JvpAP2ek5LX+nTd2TZU4WcbSLG/Nn6y4K3KJNR+SuinwLqNrwXbXtKu8
BM7+bshaz35e6klKXyKksXECPS+qPjVkkMSVYoqg6go1VixqDvPhtlr9IvKjWK7B
4mSWU4ZTaw61bTRw96bAjrjQA50/pY7+RGxxAU6K3G1BKzL0z4rGCACokU7i/n+1
Rj2iyF0a9Qf37CLg5TQXqoDS+zx2qb2YTos9MQj8jSd9HKS2B7VIXWJgTJf0ZE8
rlxZZUUX0BwehWBo9fJ1ysBQ/ZCYLV5i0hY5/93Jst8Q42ohT/Jjo/vxsYbruUdr
tGjePoIs0zY2i6pAhfx816/x5ULolpKBAhtVNByiP2TMDZ8FVSM6JmciNs81nn1V
AjDixrjl5PCY5sfW/qGhVp+h6PUorjTXS+ybbJAzkVn7BAHli2sdw70vS64yJfxn
2+nj3J+VpMrnH0YbaDzIck6G1cCN7UaZo1UcFgPdYQKdzogyRxBYgr3eAMEUwmrk
Gu1TLsRltloSb+w/+mkQDg5LkidqVPpRz7Iq1DhWVuZXI5ntzEhY+7DWJEocKSkf
n8vpIecLWn5wHTaGsjTzvwgZma/o4QDJrNH+pcFj56DBxVR0B9DyUiSB0rZGU/kk
ts1F0aFYGBg6xvk0S9qFfevizRZ4DTY+VZBtLpk/tvYU864FnSkff3ps3W+bEm1b
MgvVAW4UpLgVGe20V2z6QmUm+DRmF4/MXSmRJTIEv2eonDZQXZ2/16KaxL6RUTNP
d+ZgU1ZJfdvesVgoZCZQ/F31sD1SR0qDgufQsaxvzb0eVCTgSEoITfN+99AA6p7t
xmBblraAIfax15zG0VQAveBhWZzqkJzdKRr57RUW/UV0qBKgYegKxBtTjdXHGRE4
pwr1kW1CDqF8GUjC4JX6oc57tQ+Wf6G0db51+jQoJ+XexKUCgyJFj942795Du47E
tzLS+GswkD0kD2JBz9fXj9iAg06RvN6c1JhSt0Fj7Ila/6DfL+GoV5d3TCN1Z4g
lYv+hUmiW8RPpZMSGChWdTIrp160fte7fpHR/M0cNB06zB42HtXWgJzGyr3TZ54L
FmfUEnklbvExdmZN/0G7eI04ZIZvQKZQYl8pSMQ4kZ/8hEHf7BkeHznadb5FGpS6
+ZTKy/pT5/ulpeyMUDlu0e3p4axhwGGAUnEpNRdU0hFT4jiil/hZz01GN4GCBDSJ
Ok258Bo9xVH0eyDneHVbn6FKWkgASGBzbJJwCybiEJIM/ixWgd36jg7Ipb035Fj
YPZYomQjYGyyuq+PoNPlCj6k6jU3wYIbRoNpXso6eacAq1z62121WDQBdSSNReCq
gXeX/8S/qVXEGAR4Kju/MiR0ou9yx8TvWamJ5RHai0kDHDfVxRFbXjf4GrVMypaz
gVLgFuvn3Imt78IY0u0rb53GazUYix9qEa6fdWAHK2RXrgJW0YKt1DRfZTYgjVOY
cdf5kQhYRSaktDOSB4LncLCTY6KDhrkrMshWgCOYgikhoe44enEPXKhWM9y1BVTO
ZvcjYR2uQ4ryIVnpinFhPhT8kZwqdia2mfiJpXmDMCLDX+XV3TWTsMWrZ2c93miv

```

0KfaMJDOiFWK+zh1QrJ3aKpa1iR/+M0YkrxKxx1q0Gz4LW0rCn1b2hHjW64fq/5
rJRFcC1SQM/vYqtk0U6yUeImlfIoRIIUH++f8vd/7Uv6Am00sgKEYp+pkht12nPQ
MtZ1NHw7oNmLi4TeJbtLRU2M/7mChrL9C6BVDp6CZx7F310RNkxQ7wHapVSiU+A
LmL59uxWzXSyESQYojaV4hcM4pDjzP98X/N/qNwJpNy4K/LVackBz8GZxi3K0EBa
nWxVl0f8RRpvi0AQB/t48FVGAVzC2RvfG3MMvrmKMv8SXh/Vj2IsYuhDME9ns1P+
eJs9DCLp9YwJYpntS6MRT9xcPwWAHT5PwQbqT1TFvAJgKL/UjxY1sjwP0Fa/aCk
CNlSMVHVgQSSAbaR6CN89Yok0tnDJ5VSG4X8CKbVQved21D2UBXPSocSnuvgw3/y
jc9n7EyD+JsgmIZpbvQmJcoqv01gxjmxPmFuM6Q4R08VIY5FHoQZiArHo40brgZw
gpn4WjpGkyWBvunGsBX/WEhNoPlpvNDZHSmH2/j1cG5QWrv0x0ZRsQ/J/cpi0Sj0
Ez4ib/yQaZWdKYtGd9SBBvPm4Ss10aLm6eSLy88bBDJCRd8j77RMgjZVYzEMkjCV
0A9GHBX1yPcY5X3bxS3+D8QsyjUPNDDk1rwY4MNby6MsEsdwoZ+qFFWLXjz1LW1p
wHYCM+MH+vXwNlxBQE35FCIoNrBgZsuGonDoiawtcZ17LBnHLu90+mZ0w5E89ukj
NvqBY+Xea1jc1RjwAjD/aM+GKL1V7Io0sFwHZYSVADcwrjWBEbqu8Uaahb7YCh+D
5cY36IlaKvWircrjG4ZRLzI79e+lutD6JWASaQMfpJwP0FrY3Rt+KdSf1vXS/EaZ
bI+C3h6JxG1c0W11JHG0u8rWVNQKN7uYVsw5IBDgUSIr015No5hcFbMrs1F5X5XQ
1A/4tGJjT8tZVuksk2+P8Sq80Zs67BsQ2J9envNQIe/zXiBac0fpteUnQ0BjH7Q4
dTz+Nn00bH4fQwg2jPMjArUvRgjexG0DpC/hbBTX1PEhez2djJxjbsbEoS5N7MwI
PLrI1F9yBhU4I/ZPVVqEXl0rSbgKyyKxzX95jXrfFp1FVW+ch3RxPFGVklgVvRUi
GmwNAjVQzU8rzJtzGKI8aWnQUfwpvEVBsXFwzn816oQxwfZR1aIHHKRQ+aTXyzr0
u+20U0DJP5ibVwSANUbbEcXG0vh1hJDbPGa+zhy+aWIWbAiZFZPHENPG4g//iww8
o19NavfvvZMhaWNX5jfBr3j4mMCbRfmfQ/ZgLTiCfQUXKraVQRDxSVWqzxSGMGm0
iQH0KKE008DUvFQ6YlJse1N6MxQnL1tUKKPeTE90mXescLZsUg61f1Z2NaBIVN0G
4UMKGJ1adzn0KWVGZxBr/GBcQDA9OYT00q/yLxG0hZetGix0GQYBsJx3U9fdDWYm
4o+nmEFhH1sr5QvSAEKho8uCXzTXx3zxh547nzzCibuG26uhGpZ/xbFA/PpFvkai
6tXDze0uK2rlz+gf8yRn1Yl++Lq3SFNRk/hisAGY2P3vYSa7p3k7cI4lfsacX7AR
gmkpCfY3gLDLHftoE+XHHFGNwoWo0mkiF/gViRv+rj2m23jtzs2RKckiDpHPryBD
6aktHPrs7ie+4e4Gj/8LEdp/czOG1r+QdhMYANSn2TlS4lQNu72i0B0BeVBszUaI
A1bEyVW7e0XQy1dqTkhTkF4YgoWbxi041p1E1hjGs3lkRuaSkbhW/JDJ+pWEMjwx
EX598fgRN/fnedEElqn99ob4iifPbRWl4gk0n6Gb2R12yzx81U1AJesPAPzwDiPd
rfp/JM69QgRUEs0ady10Xi/LOXehg6BBqcpVLPXtQykK1Vh2n2m1G0szjI2AHxWl
k5EDLicoBwUdp6UqqZIt2W0tP1o/KT6xvb7oUBbHTDUt5gYrB0wNx+FSAW3MEI/k
zA4zZRgl9cPTSG30m5dd7WejVxw7YLCd3HULW0CYb38id9//QmEPxAZaEemEFs1K
WAEwKbqoiFi2fKTPjZlV+4a3wor+ZpjR8itnknFqMkRGewklmA4Q1hH8cW4L+TJK
50A1HI8vTeigu3vog0nd8w1Rr3hy0zNLR5b1QtpAfv+m3gaqn2DjHnXHU7aYsna/
+fZ5I2Kx4ja4vyDcx+vIE0iJVZ0SabINF4hsAyyF18xdo90x/rapKhF4HZcTGi74
YHw30ig+ddtvtRrdpFuZKW80rEVgmvhIc6Yj/oVc/1Tf1J5BEZA/pU45dH3NLWWo
gWqivq05ncRgBqPVNJyY6XBELWWonQesu0TTq4PGESxKGeSBE9h4S21tYNhm6Un
SDm33C36ART01juvdELav8B1wqJNCjNU/PCUI23txYMQP41M6RkPWjNd9Z59Zpn
hgHXs4nF7ZWnNxEhnG8MN7D+kXG8UjBdQwyAGwxU10wPEbMcwkj0bmBVMevWUFG
5MoJjt952bgNTa4tNu0UDzKg/eirLXmnlxgWE75ZHeMWYj70JmD127UDA2zy2o/U
gU5j1ovrtdMqsLtd2g62ccKDlZDJCVn9gP6nN/KXhKBQRhLATgo6a1lmyd3GNA12
CGizsLjg+UImbJkFUWp4eEZr9E7RcdJ6lC/Gs93K4aq/XbhJMdjfQXWLM03ndF9/
r7Cp3Z7TW2emivxYYCk7airnd0WeIdZrwxoACNTQ+6IeD0LSet6iMP2EiLRRgf0B
2eU6X7yMWvTwRYbByybrKpqsM2moy4IpMS+DgaThSVxVHf3RbFvIXPumhRCFFkS4
1mm2czKN9wUaBLKcmeynBpRaunt9n0uFyWjgSbekqw3cet82vu9MOPsmM2h36UV
WgJDktehhr/gi230N4kavEwGngVIv1q+Emm0SuUmKacqda0MATxUHL92IA93L9pm
RvT6xARWsy0DrG/r362C6PDwp1fsTOQju6LkhFA0AvqDPKk+HOIjgBtkynHUPGwv
8EN9Gx2SWwDJahAjPoz2t9kByC7PdG9qyGAAAEU6G/wXjshmzgw3jdw/PRmfSdNs
gbky/4GGewN106WC9c+6qN4ldDff+m83ABgWonCuamerjlaIFFbfBJEGX/CBz7GQ
QpfXuAEbhi11U1oM77povWS5C18e0GSD2t2mt7E0aLgMT+L2TZXQx81ZmN8sWQq7
cP6aK8FpkDhidLIc9fneWucvMH5BKXx8em3ug4B18MUABR4K03ebuTLfDH+FGkD0
HNeqqUVBSzDveFday1cw2HkJpm8D9BoC3Y0n/MMW5VE=

```

C.3.8.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

MIPXgYJKoZiHvcNAQCcCoIIPTzCCD0sCAQEXDTALBglghkgBZQMEAgEwggWHBqkq
hkiG9w0BBwGgggV4BIIIFdE1JTUUtVmVyc2l1b3JogMS4wDQpDb250ZW50LVRyYW5z
ZmVYLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtdW5jLWwh
LXNoeS1sZWdhY3ktcmVwbHkNCK1lc3NhZ2U2SUQ6IDxzbWltZS1zaWduZWQtdW5j
LWwhLXNoeS1sZWdhY3ktcmVwbHIAZxhhbXBsZT4NCKZyb206IEFsaWNlIDxhbGJj
ZUBzbWltZS5leGFtcGx1Pg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpE
YXRl0iBTYXQsIDIwIEZlYyIyNmMDIxIDEwQjE5Qj0yAic0bWNTAwDQpvc2VyLUFuFwZ50
OibTYW1wbGUgTVVBIFZlcnBm24gMS4wDQpJbi1SZXBseS1Ub3JogPHNTaW1lLXNo
Z25lZC1lbmMtaHAtc2h5LWxlZ2ZfjeUBleGFtcGx1Pg0KUMVmZXJlbmNlc3JogPHNT
aW1lLXNoZ25lZC1lbmMtaHAtc2h5LWxlZ2ZfjeUBleGFtcGx1Pg0KSFAAtT3V0ZXI6
IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcj0NCiBNZXNzYWdlLlU1E0ia8c21pbWU
c2l1bmVklWVUyY1ocC1zaHktbGVnYWN5LXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRl
cjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IFRvOiBib2JA
c21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTU6MTk6MDIgcAwMDANCkhQU91dGvY0iBVc2VyLUFuFwZ50iBTYW1wbGUgTVVB
IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogSW4tUmVwbHktVG86IDxzbWltZS1zaWdu
ZWQtdW5jLWwhLXNoeS1sZWdhY3R1AZxhhbXBsZT4NCKhQU91dGvY0iBSZWLzcmVU
Y2VzOia8c21pbWUtdC2l1bmVklWVUyY1ocC1zaHktbGVnYWN5QGV4YW1wbGU+DQpD
b250ZW50LVR5cGU6IHRleHQvcGxhaW47IGN0YXJzZXQ9InV0Zi04IjsNCiBocC1s
ZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXB0ZXIiDQoNC1N1YmplY3Q6IHNtaW1l
LXNoZ25lZC1lbmMtaHAtc2h5LWxlZ2ZfjeS1yZXBseQ0KRnJvbTogQWxpY2UgPGFs
aWNlQHNtaW1lLmV4YW1wbGU+DQpUb3JogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4N
CKRhhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTk6MDIglTA1MDANCg0KVGHpcyBp
cyB0aGUNCnNtaW1lLXNoZ25lZC1lbmMtaHAtc2h5LWxlZ2ZfjeS1yZXBseQ0KbWVz
c2FnZS4NCg0KVGHpcyBpcyBhIHNPZ25lZC1lbmQtdW5jcn1wdGvYkXfMvTULNRSBT
ZXNzYWdlIHVzaW5nIFBLQ1MjNwOjZ5ZW50ZWxvcGVkRGF0YSBhcm91bmQgc2l1bmVkl
RGF0YS4gIFRoZSBwYXlsb2FkIGlzlIGEgdGV4dC9wbGFpbG0KbWVzc2FnZS4gSXQg
dXN1cyB0aGUGSGVhZGVyIFB5b3R1Y3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0
DQp3aXRoIHRoZSB0Y3Bfc2h5IEhlYWRLciBDb25maWRlbnRpYWxpdkHkgUG9saWN5
IHdpdGggYSaITGVnYWN5DQpEaXNwbGF5IiBwYXJ0Lg0KDQo0tLSANCKfSaWNlDQph
bGJjZUBzbWltZS5leGFtcGx1dDQggggemMIIDZzCCAregAwIBAgITDy01vRE5l0r0
QlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FAADBVMQ0wCwYDVQQKEwRJRVRGRmREwDwYD
VQLLEwhMUQ1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBvIFJDTQSBdXJ0aAwZp
Y2F0aW9uIEF1dGhvcml0eTAuGfW0x0XTEwMjAgMTA8YMDUyYMDYyMDYyMDYyMDYyMDYy
OFowOzENMAsGA1UEChMESUVURiERMA8GA1UECzMITEFNUFNGv0cxFzAVBgNVBAMT
DKfSaWNlIEExvdmVsYWNlMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mpUp+ovBou0P6AFQJ+RppwODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB
8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5
R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJan
Z/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvMswqS6oQcAx3Weag0yCNj1V9V9
yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukng+fHbqvWdhJL
AgFpw/jA/Eb/WI+whUpqtQIDAQABo4GvMIGSMAwGA1UdEwEB+wQCNAAwFwYDVR0g
BBAwPjAMBgpghkgBZQMCAATABMBA4A1UEQjQXMBWBE2FsaWNlQHNtaW1lLmV4YW1w
bGUwEwYDVR0lBAwwCgYIKwYBBQUHAAwQwDgYDVR0PAQH/BAQDAgUGMB0GA1UdDgQW
BBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAwGBSRMI58BxcMp/EJKGU2
GmccaHb0WTANBgkqhkiG9w0BAQ0FAA0CAQEAguL4oJyxMpwWpAy10vK6NEbM1gd
5H14EC4Muxq1u0q2XgX0SBHI6dF/x/4LDsfxf7fSIus8gWVY3WqMeu0A7IizkBD+GD
Eu8uKVeERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/1T0kRg8
uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K
9JiQaJYONUmGpfB8PPwDR6chMZeegSQaw++OIKqHrg/WEh4yiuPfqaAvX2hZkPpi
vNJYdTPUXTS07K459Cyqbqg+sNO02k1NtX185RHnrvVKQx+L0YwY1Q+hWDCCA88w
ggK3oAMCAQICEZdBXNtdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTEN
MA8GA1UEChMESUVURiERMA8GA1UECzMITEFNUFNGv0cxMTAvBaNvBAMTKFNhbXBs

```

ZSBMQU1QUyBSU0EgQ2VydGlmWNhdGlvbiBBdXRob3JpdHkwIBcNMtkxMTIwMDY1
NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBE1FVEYxETAPBgNVBAsT
CExBTVBTIFdHMRcwFQYDVQDEw5BbGljZSBMb3Z1bGFjZTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6
WWyTgBK9LC0wI2juwdRrjFBSXkk7pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZ
WleYXFK1QHJD73nQwXP968+A/3rBX7Ph00DBbZnfit0LPgPEwjTtdg0VQQ6Wz+CR
Q/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH6syTjGsgkLcLNau5LZDQudsGV+SAo3
nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0
nsG1llyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAa0BrzCBrdAM
BgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYZIAWUDAgEwATAeBgNVHREEFzAV
gRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGwDAdBgNVHQ4EFgQuu/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0j
BBgwFoAUKTCOfAcXDKfxCSH1NhpNHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0J
oJanzqmgasN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnN
v0Fb81V1iffRTF/KtmVEDMR/sYeqAH83KM5p3e121Vh40HhyI0qNuz5oShNaACSi
oQ23WxHGvy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4
z0IOvg6mrYkKTM/RCGnumghxwYToj10yD5Gs4D2IJCw+fx50Dxh52MbNRYXTus2Z
PRPM8JXNQ4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H
4Con1B8f7R7s1LM2cSYxggIAMiIB/AIBATBsMFUxDTALBgNVBAoTBE1FVEYxETAP
BgNVBAsTCExBTVBTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NBIEN1cnRp
Zml1YXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+Gr0mqnXMAsgCWCGSAF1
AwQCAaBpMBGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8X
DTIxMDIyMDE1MTkwMlowLwYJKoZIhvcNAQkEMSIEIDUC1bNj9mKYodH3vCGfNVpZ
jSSWg3QZ6u/dLxbyfbvEMA0GCSqGSIb3DQEBAQUABIIBAHqRG2dp61WFSKrkBcj7
sVy7Sms11IQU013E023T5h4PcL8PjggAJi/GHWaEsGviQEdS0QAb1jEnzd2wjgn0
QDtLBAfpQtQR0byQGTzpg7y9Lt5WnuxQaZxsBPvENqeYSFesUV1W1JrJGXcqLH7U
cu1+bdDLEe0p2ITtazvmgJ5NvoHkucBk1v8fwW6uliGJCZC0Gf9WJDP1qay2Jexy
/TUzmr2Egnxq71W1AVq12kfU0fZkgALFRzhaHtonrST83I1sLK9ZxB8ZX8vJX56v
5hHRzhuQQyAVg0eVz7skKIb50DfBHqJ1vEzvCjf72BgQLYGEzR6hmPXW1M14vXtV
lIw=

```

C.3.8.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with `hcp_shy` (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:


```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-legacy-reply
Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:19:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
References: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:19:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: References: <smime-signed-enc-hp-shy-legacy@example>
Content-Type: text/plain; charset="utf-8";
  hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-shy-legacy-reply
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:19:02 -0500

This is the
smime-signed-enc-hp-shy-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--
Alice
alice@smime.example
```

C.3.9. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#).

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 10035 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6412 bytes
    ↓ (unwraps to)
    └─ multipart/mixed 2054 bytes
      └─ multipart/alternative 1124 bytes
        └─ text/plain 383 bytes
          └─ text/html 478 bytes
            └─ image/png inline 236 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:09:02 -0500
User-Agent: Sample MUA Version 1.0

```

```

MIIc7AYJKoZIhvcNAQcDoIIc3TCCHNkCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBTFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFGU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBADDPZm+dVU61KX+lmXLEuKI+W/hu1Uw0QmHq
Vi5HfM9uo9AMrXV17PG2YzA75ItxhcJmJf8TwnK1A0YbrwGnhJAodi9MHCR+nqdY
A413rxKHU1hcJLn8oWck8ypYwzs3NBDJi7F+8aBmfEolG8xn42o5B1FLKcNkM1Ng
NBTQpqrUld+n6iin0vGFPTJV7PBDdcE0VVeqiIoDAsZaTp25PYqEKSsnC010zRF5
8v2BEAX6h8EpjqE5PX65JKus2NAjnJioN9eUjCQ6mn1XPBw4UYJEUqc834+17HcG
FjwDXIoJY7XuSND2brm9JFYSmlyR6gzz3bRgIUqWYgjQhqu1CRswggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECXMITEFNUFGUv0cxMTAvBgNVBAMTKFNh
bXBzZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAmxXv7vLaS7vcshZyoM5wgRsY
IUf4iPK6n1BuzbCZnexPwW5TGghgs08zxA64/hzzqEwbVneZIfcooIij4bdQZx17
nbYpLBCC1Y35+gtSiLGgCyUvqymH9jg7znq617FNqgD6v+0ui70F4ZX3t072I+4I
HDjffLryn939vUwMpmTPUQ5Y1ZqkTNjM2jdDQ5/1J5ndGYcC/wi1hiZt5mz44LvF
npGAXVRn7bcYUtDRsFuuSmHbckCnbeI4C2yU0c2G6fmyHuOnpy5LL5US0h0Dca9
pMV9dn6cJH5T9bks12eYiPGS9CrixOL/U+fXHmVKsyzm5cRU/CB3rwUDnLen0zCC
Gb4GCSqGSIb3DQEHAQAdBgglghkgBZQMEAAQIEEBzMZlGxbLgauF9sIia9KrGAGhmQ
avkXlQ62LNzHi7NtNtPLsiqIrji1UwDWe8cYPupsu+3hxQZRVMDHjC1ygNsK8BWA
P86t5gJaORrI4Avy0//4bEzZM267YRWiC3RgXm+p3DB161vETc1cXjZu+7qKJMdE
LbSH9iLue/iNi+xQxD0tGYVzuYPwHypts8br+Cs3Yda3aWK1ipJQUuCILbDCGv17
ZC5eizwGufBEhej17iJkgVDyU6sAY10E38YFL/saDHjtryJLp+c0cV7R02UEmDPC
Jf/BfdCknCdo7gEu4lZitlkcr2T1h56IAyK46iyPLXZaZua5R8He6/MEdC5Ys2a7
gw3FwSgzjUlx0zIrTgWcQdk5dc1Up7PL0meZ5PLaQglwB8fXYDkv9f/T/Sh0uJ40
xc/pcK5yjrCpFr0pVzcPVurzBpWtKwRNjiRnwFGHjafPfldxJf96WtgkkZcJNDmW
11y05SwWHRUd50pVvffdqipm88nL9tVfp31Jy3jbFR+7XTRPUy3QJ1l7d97a03p+
aZLKXhgvMWN9R1MzqtF6wihpmPccLOX3Bd8bIwuGFeyZA4FR6ixicdql7nXWDSzw
1Zakf4e4EbKRg0yrRb9X9iMaUBoScwByEopp4j1Gex0hGD5omujbvrD/tpR5amqN
Q+cY/J33oo8v5auCWQiBdr3NK9jG6dAyfXrhcvpVi/Ay9sSMGwApCTXkRRibbNS
jY+2sZt81uo2Nfp4FWr36rfNmE7KmBHxWTs9U7ZW5yYJvBVG9VZDGk+7vt/KxNqh
JEXdQlW/g8XmuYDqtnx9VL+vAZqHvKkBqvSZsQsTrEh0IJ69e4wTu+2/f5Kv5DYlw
pas+TKxRN2VZgGaLx10Jp10TkyY846t4iud8pVR1v3MxuMSzS3JF6R+Ynk1uTmtD
x27uKFT5LwS5+jvL0y/a6zk104pr5SvA/EnGJrVn0D0+Rszw2JWXRdiE2Cejk1X

```

zXgLIIdVrF/tytRNN2U0hypvsdkZdjRT+MrT26ypkJSPEA9a/0LdiylkRJuFW0Fh
FDYIZ4T1jFMkedTktD+038TNVFE42LBF5dTm/ATz0Be00YQgRC+QSE604NEnCZhX
Xppkk1sFoPjvA8AAZANQyZ10wQuFZA/8S/6mJ/15Fh/pr8c/NU4NyM/vC1T6Pg5f
ZMFx/anra7iUCSyn6Muo7t3vyevh+QX0wn6aHWWe90NPsuLFd25EDYWrokrPo57t
/538uPU47RPCRktG0tqmuNplh/8HshhP3e9082WKPyFaFixGaVvmhMjzU9+CFGQa
d6oJag2uudjv+e2mpwX5Zm41R01I00QH3ubhaHz9ZCU5S5Hckwb2yIvk81gFqmm3
/ykRWX30g11J4tfb4+WpbcJWYsckwc8mvGizDEQTu6oStblDBqJXzeB+PdX1LZQZ
xsbAc6xRFyD8CJBEhAEzwQ/y9tVG3hLbNhg8IQ1XMcRvP3EypwDRdDEIDnIP2HUS
Iub26/ZnAXwzCT7jt5WGjsM73XHMruil/4nwSGv+px7Zw59U+D7w3bxncqaJHUpe
jUxBIJadRSUKK0UgIMkshAQsCB6GyTcvddolFZF+keE+cyvn1wKa/pUPBYh1Hwmy
LZ5Niko2jqyuufTAgB+u686Z7c36E3N+1xGUS6BQIoTKuLEXmuvCdwC1xjmC9Hi
uHKb8tv1FaHfsp/Ilo2v8GgIL+pkJsZeHww6cM80qtuJKMMGz35SmdrMbInYK+4U
OdiJbSBB2tCk7m5aRn6HVff14RBZDsQN+5xtuPYaE5Wmie/NMT01Khvuc9Yp+Xl1
rvIe02kKZ5FjPYW5BQJuj3gJl3G6Z7Z9qrEpgqK6XtkMvEjxUbzd5PuhFDklPd9q
PbXD48D8L03q1rLScuHgrRTaSXy9XfYRvBaNuGrGfD07ucM9LqS3Ugu6MPyV4wPs
2bvQkybHmuav5M+szPnyUVnYvS9LmPlCg3IX5YshrCyVYz2w6zZRF4J+hI3zIkla
huJgUoGumLSlea7qTwr1GS2MuaUfe5PZMn16q0aqaXTMk68yEM4ugI9a6033MJK1o
OTkWQvXFRQpb36NWAVHx5rGlk5+LG0idxGFjyI/AUcpoe14h98QtYR0jas6U0IDm
/CVjFKsrzCsyWPjlxL1mLoe+0J8ErFY5X0ZHGYIP2AvgpTMZGRc9X5FZKeAs1Ny
WjiqUjjsxW7f15ynVpdHH2Z7M5rZgTdClC+sxn6qPq2ua0AGeMY5hQR8MfPX+aWk
4I62uThf14lDECunGX22nIcsgpRfuW6ylmGlkpNZDNGf/ngreKQEj4uK7CBx75Z9
jNubdl+HYWUQEEF2I+Gp665beYQuF4tpmI2Bh5TTFyF5+0Uj/DeEB30l6opPG29i
b4+cuKXFbF4F2ShtKqy0033vVeWKMdyB1TfcmWJx6Z/feQKrVRKJsOIp9KrsNVYo
K+xBtHHnnPuJiQM6HUsA7ttPtTCjQkMWz12trAvG0EcKaXAATfQ/upTBuk3NoiAo
q60bS80irMm1/W63hgPILubiXlMF0H1pQ/1k6FoxJfT8jlcXM8xyNxufux00/uz4
aTstfUW85RzFba98hoVGJrg/bKXH1Ffc84Z2cc7VMqsAZZcyKjzGIBso0MFTMN2E
JsTY0HtF3hzUcV/KrEU+4m3mSSauUpudyR4yLeFmPN5Fc4l4MYhh+vU+S/k4AQwE
QChthYZmWcmhTu3Nmb8IINWLpUT8m6upYy9/YlVApQP4b4HosKdFb9ZTW8FXhhB
ASzt5f4G/cJhw+V2TahvFNyWGMskArE0srv7Sg9GNRv7IBSGCB7g+c5A3cWBWGt6
xIy+HlHz2wxaIip+A7Rflw0pLZjAxRq9hCtMEXM7pq4FK6MUzs+zVR7ZjFD7Xp15
SB1Lkr9Shfo915mGbAvjT0/zNj87yPu/6IiZ3BXTF4mXJFh8LjRSf3WaFLmDGeZt
iX6y0U7wsLbkGLH0HvwMDCm7an8fUyCTzpOC6RwiV6gT3Q0Fhxj250yTzwIuETXW
3oNSq37nLwZxXzj58jgsDcjPysfngGTld7PxZdRS3B0Ik3YbDhCgYXYsy/Z43zmD
AqDqdoh8ab1foLtuifBYQC+0ns9eAjbLzqdRzXJMyzKWQXkmzNM03TYx5Sto+G8D
tkv2bPbImfD4ElirDT7nquY6hBG3p107qUiFs0jq6RS4wb/v8TW2NqXwGoCp1SHK
zg9MuzT+srDCY6qSAePqy2HZ3JnAYsk3Bs0oB79yWYLXkYzgeMZADP3C+ees7oK5
sA7X+LV9eA+dIjRSdXsAlnzviEhM7zSq+82V65GqcvNNFZYqkxsl167Kciy12XxU
pKYAc54MdvrrJurCWVp3tWvKsqwdXXlZyrx3/a/fdzsiTD1k++REYhRTEwGkyZsK7
okSoR+ZkVAIRv4vto69DpkPmUX+M+56Wn/nmV3XZQ7IQ5CuF1XutC9NXF5mvnnnI
jIAf9HiDAV8Xf3+ru0WzMXGzVtkW8qzz5jqJtDpYIa/IJDRC9DRLWaqJ6a3+c7B+
zbqggQd1Sikha96oqoQ0C6ulcjWt+MuFvzjcICERkjFpCAgsCAAt8C1a+5ImnlDt
VNfZwvhhnfICwV2BRQDZl00f1QwJTLsijK3cR000cgogL28a4ydWqVD07Zmp/0bs
CRUckUdhmLd/vq4ctF+nsR0bmtYQ8+By+QoH2NmWkiIyKatniZLBNnoWmQV4rqkz
X4MJxJlQkHznpxxYVJNvvBmjokw90FeSkwfoAEWUzIi3WgY2TKAMI1kKj0XCSPSh
eFcnh7+HFHGACmBcpJp07nWQzbIZNQzXFAdmI/jLTJ15SfDiJi/xfKLb8i6Vrf0q
6tk+90HRy44Mni6wCvg8fVJ+fY/UHGpwdWc33r5W/1lLJbo2QugsGkNB00m18Mz6
IerbrP659NsQYgfXf1GzXQ5ySkkHL/YB0taljpMiF+MYTLbGu/DlxMG65nGyNADD
wbTOY0s6PeeKKvc69LzjugHlA9hgFhdGraNq0LIjX90P00kWBwFsmijELEgbbsspV
UI7Oy+0z8iptfSN9P05V5b1SYEx0KK7C96tKXcJgCmZlTnu0HJueoaUW18s3lBPk
WFX840R0rfcxNHxVn62SQZJLP9fmoAHW5w44ZND5n32U/U7gqNXPZw9bbhsIWufjc
UsHZQns2Zoy9z+2D1f6zXRouU4DxkhJtLZDubYqyF0/yuYeG7P/1nmIzcmQXUX6J
G1BSZGcoFAuurvfJ00CKi6E90pmXPfxd0l0kMMXWfdnDiAa1ND4HpWKC09SevZsx
0dxl6xFbBNm+ryjTm0pqzPHPo9E0wUdko10LuYL/pLFE9t2LlGu20ILRp/gZsN0m
GNpTZkP3aNZ8y9tg/I04DbwbDqYJfYEKmuZUjxxdxYBNj4TW4Ih/HisVfsByRjN4e
yMGexDmMrxXTetCfMAISTPGk00hPFZRLUXn0k0gefXlN25xk2XqpqHFqKf8zSHk
9Ke2joNowVQjqvxJ+0VYgX0a+JjNS/x8p6g32HH6ajzHxQDzV9VFqHqdiYFB+ZkI
6ZTSLZesnOjxDmWYH2DQXJLw05FBeioLJniUq3BzbVcilEZg9erp9KCuM8dZ6mkQ
oLZXmAYkG5Vsr5Fw3NFTctFZ29gFABkmAXHannZsGogAoA0TVegTgR8m9+jNNE1b

SBKUxEny1EUtLLH4KaxDZqzHQtwjLldq+b7XZ5Qs0G5aoq7UhbPkQboJZesYtqEv
+Xaqccw8InSNzUhXcgo20m16C70ux1BhF46kxcccWj0G2sKAL8t4tp825bvJMmy
fE3b+DH120zVQ6AfX4ZRpjDk0Xxc/5h3SX2Cmbk05kedoJrh+US02uVYMT/TAaww
BlbYwr3R0ikSF7dZK07vnDsvXV1MDZ+6iQHnLkXRmQxMYvcMoyp5uKdSca3hb8c7
lrePfaI8PG5+RQ47JbYjjg91cRZA8GC/170KU0naxalgvf9FSs18PLCjmCNuoS57
FB4+JC2u37iGmsDu94eU0DwwzrBxzM3I6HZDALhqTrABLztww9E/+qc43F/L+mgv
ndic5HuFseCHRilbLq/SrQdzWH/t7FYuke9mwqJ5fMozW/TGIGJy6kYcMWx4NGcs
Sgq4H9waeqVdpUCYi2rnBobfxwPp+iFzJLFCyYLYjKB41PAZdn49PI00o2cXXMKA
l+B5qMwIumPe5tx10ETUes8wW6Ma2BuuRjpX9YK/mwICAY0CmrUQ9P3hCaKdvkuZ
oW0h9bdZutmK9/eByk8ecjc1aYLuFcAzuLc2UHNhvNpqDntEhcxF0Lhg06FBQVry
n7j7NSc3tTR/PoyMmDXHIubDi8ACm126ju5ioyVxep7/DUzfXAAXY+XI1Vkt1M+D
xwG+OZQK1h1600FqypmjEhcALxUcD3jXJcmnA00oYNNV+j+CQj2xi+To+fY1gMTT8
6BCg6dT2VwAJoYVa0zBFnFvQ2190vR2EFWnJuLBg28XExos4/4MS9Z6t9thWcu0J
uVoDVjkGdeQcyuG3Ey1YwSnKxapj+ZtQn7m7rR2YTGndDqVLypXZn0SQYrcamlgD
C0/+iW7fbnUevaruDyyXaz+Mlxv2KCPHP62qeAInbwWMdxkVBL7cWLYmUZb6i+A0
HkraXcLbadGGjmd7sgoZRVDQzxj0on1B4iIgWigZ3RS+4QLf8L5Dmr3tnvslYEg9
OvtsdJaTJ+jGtUE1BZ6ny0usf1L1k+t/PGrkBtv1AFsLu2YWvxnP50b1HsD84YXv
XA7ieDsgXXDSwn63VAUhoaMr1hhEF1+2JFwqDx9v1ZMwnmNANJUPT3J0DYKVjBe1
nRZe0ePzpYQGxXJapZhYshsMNjQpHieqm/yyU61i+NXuap6Cyqifab7xRSc2TQza
txISAuRxxg1pfTu+anSmF33157w3YFttJx/KzjAImNvVHYvAg3AYd11s2gaI7H2bh
MHvkXs2wcBimKSqanMmzZ2Ds8K10YsECcvqY7172xEvxG2yhETAwiuXXgRHY88L
WnftnPJ+x8aWISWCoY7iGiDWTX9nqgd2fvPx76ZMgKDYyhUFU6jhr18HwQQozesK
2qgMXY+tsMm06pIK+dtsJX5vtr4FHVq12dE/2VsHqzf0u/dfJSkTYP4qsLZw9RRX
NfFCAnV+ZSrCMzQNS2B/1d6Aa92PC42QYxGtQebmPnzSvBpSbGAaFoQDVF4wCaY6
iRUegB4a52zfjEGmCj0Y1110W89ep113frCrqdua15qPKQw3XvAtQg9taTGM1RW/
kqSlw2ThmmPdik4/JriXTJYBP80b80FQBYFxbR03H+6cxD9F8YcYcNQQ6RngA6xL
ZPGH+gaLIYFnp9s0X9iguS+r37pBoPWfUfXIrzZpoY0KL2npgjf9/qdWTF1MzMDZ
PbavWCdW0k4ZUksf8Q1kXEoa8Rao87yUhxvyofcKNoX7UE2Pbanu0BnvsGJZQq/y
6u9nNm+aB8gSzGaC/FQ5mRXvUU+3SmLW9oWrOD38HEQe7wtVUchez+NQukZfDf8G
uOuE6vBtXtHixn3vZa21Yp+rWpR7i2B0sKGMUzKLsg9UvZkvfwnP4+zuZvffr58
82nMbLStjTB0ZnqNDkLhIZueXGJgGx095kkqowlWv8QYyp5XQy2HaGjaULGB0Yt
VyCF+7RErQXvNDycnIc3aumJ7yJ5wygor3/z+SgEqV0E4iEkjaSvsRKard6vVdCK
KQG3LL6fKwgGDTdP+08KKXLYhZMs18TtGLjye722CQ5w17dfQex1L/vnHN5avW8B
Qdq+TEQowywTJC5qTe2EtwmRiCcBc1PnebQFM3cT2rX45c16iiFz3zM2EYvTQBYf
LKKLudvH/4vd8oFWS8oKY6mzPtZKwZ4XgM9gxCsN59HZ/+CsrNFOEx1kTPVRpfD0
rgr/sfNpVKSS7E4hagMUbeLSU9G1cyxX6DYoy0sx23Erc0i+/D19MLNAny9+x0+
IpIyP9dVbeUCSLBbzQIH57FN64h3iHXx6Q/JNnkmLNkWMXNIi+ekE6e/ikZLSBhg
cMrTtZ0+G6P/7bQK0KYxIkdaofRL6qkqKqzTbHXM9F0X1xcjBP4EhfSzS4zTk2PP
oQs9iebTozmbk2x6xjkw8/D27fmWfbWdjCLjCN2Z4xWkmkkXonwrdesjw40RGxwk
AsS1VHW5akXeR0xHx6wjS9y6sGftYWI5fgh1JTxxvvaSjBY+13BvLZboKLAw0/0j
5JiyQAB/t22zUaHvi/YEWL1aHtpgY/PUEatbHmU09kt7PY+3jiURxPHjae4CelqL
D3dFJ/I6DGPuLhLgxCuKTDXGDbReugmNA9rM0z/aS/yQuwRh+0iNLsJd+iifaX5p
VldYRq6gOkRej31j08fPKEHNDLgTToHbDzDhUTBKGCjePhMH0//JrOkH3izTpSWR
6IEfM6Jo8HvcZGPq00Ra5HS0BPcQ/rEr5GiEtbeUqkJ3PonMEYe1K2buI5Lw5sUt
W8/wt9YLuXap20L4jNVAJrflf5n3f0Pm4F9mCPCzBCNzBv2U+cuASVh9HA4E8+dG
KqR4FEeqv7Mo5DONHdfYk8Sdw5IYx+XGahqk/qvrqR+QXPBb06oeXLmbI17TZKus
nqAg6PoENnx68R3jPwrZ0c11jasz0L6zQ6yVQTxlX/Jj3CbzhkYEHh6sU5EPkWu
H2B81Fifdxkn8CIs+cdWcSyVxJlYRU8qwwdUudsXbcFn6bW41/V43yrz4BozVuB8
N3vOTqoDZeLRRaebCaFGRmUGWW03/Wv0qqdzMc3UFxBiMDol0Gyr/3tKff2kf/dY
KaHssQYIIC2hh+f5l+Ekp3XjaX6GFtAjM/scJlC0ftupzk9tJG3scEUTbK8MwUxT
pJ59+cj3CtdJHxMVic904PlPqsocHzK5CpqQD5Clvqj1jFc+eZ9BICZ+s880Ie9B
bFpW1S8AN9UyH16nCbl1D0azUIhdRh5goDv1FRv47Wtr+zZCseGzIJ7oCAE38KDZ
u6QdAe2a16qibKGe0KaZEVm1DDIae6YCIUJZw/PDm05Bf8NkRSz2atY8UzyxSxi
K9HYKPDly0ILMF+aQzqv36IittNYQ22nqN1XVCmYF0HFPnS6RFyDXU+wa9RATL1p
u/kW8TWMOBveXstkJU8TbHx5TDEftg+Y+tyDNb4n4xwpuishLd/pMck6LNK3f03
c0aQssUWkpjJSzSeedcA4oonnq833DXP6SPF1ksXlArsDVWB4at1FRqbaUKKrpv
Hinhb+MUjANUW+TcAEznbtYHFvEuNCIX7WU7S10glcrEjJzGnJZC24+10KzxF3ed
7PndgDs1LmJc4ExhALrKGFw57Muvy1UNd4f6W7AEraj/54FIozZDRH+R/owcjuik

dGlVbjogaW5saW5lDQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBUQFV
Q0FZQUFBQ05pUjB0QUFBQWNfbEVVRVlI0MnVWVE94YkENCK1BZ1M3MzluTzNUcFJ3
MjBkcXBizkFSUUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3
a1oNCnNncnmpY3FWTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWHbZlRQUmljaWhB
ZjVZSnJ3N3ZqdjBaV1JXTS91bGkNCnZkUGYxUVoya0RE0XhwcGQ4d0FBQUFCslJV
NUVya0pnZ2c9PQ0KDQotLWUwMy0tDQggggemMIIDzzCCAregAwIBAgITDy0lvRE5
l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREw
DwYDVQQLEWhmQUU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTvBTIFJTQSDZXJ0
aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2
NTQxOFowOzENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxZfzAVBgNV
BAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAmpUp+ovBou0P6AFQJ+Rpw0DxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2
vWYB8gOUH/CvT2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuT
SxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjM
UJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmswqpS6oQcAx3Weag0yCNj1
V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvw
DhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCAAwFwYD
VR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNTaW1lLmV4
YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVDR0PAQH/BAQDAgUgMB0GA1Ud
DgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJ
KGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAguL4oJyxMpwWpAy10vK6NEbM
l1gD5H14EC4Muxq1u0q2XgX0SBHI6DfX/4LDsfX7fSIus8gWVY3WqMeu0A7IizkB
D+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lT0
kRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR
lE5K9JiQaJY0UmGpFb8PPwDR6chMZeegSQAW++0IKqHrg/WEh4yiuPfqmAvX2hZ
kPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCC
A88wggK3oAMCAQICEzdBBXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAw
VTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkwIBcNMtKxMTIw
MDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNV
BAStCEExBTvBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3ZlbgFjZTCCASiWdQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XT
vYi6WWyTgBK9LC0wI2juwdRrjFBSXk7pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4
WHWZwleYXFKlQHJD73nQwXP968+A/3rBX7Ph00DBBznfit0LPgPEwjTtdg0VQq6W
z+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH16syTjGsgkLcLNau5LZDQudsGV+
SAo3nBdWCRYV+I65x8Kf4hCxxqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fQXgq4S
WcC0nsG1lyYxt1TL270I6ATKRgJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAaA0BrzCB
rDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQA4wDAYKYZIAWUDAgEwATAeBgNVHREE
FzAVGrNhbG1jZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4G
A1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYD
VR0jBBgwFoAUkTC0fAcXDKfxCSHlNhpNHGh29FkWdQYJKoZIhvcNAQENBQADggEB
AH0JoJanzqmgasN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChw
KfnNvOfb8lV1iffRtF/KtmVEDMR/sYeqAH83KM5p3el2lVh40HhyI0qNuz5oShNa
ACSioQ23WxHGvy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMv
cdH4z0I0vg6mrYkKTM/RCGnumghxwYtoJ10yD5Gs4D2IJCw+fX50Dxh52MbNRYXT
us2ZPRPM8JXNQ4Gwv4km3M4rKnJD6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk
220H4ConlB8f7R7s1LM2cSYxggIAMiIB/AIBATBsMFUxDtALBgNVBAoTBElFVEYx
ETAPBgNVBAStCEExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NBIEENl
cnRpZm1jYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmgnXMASGCWCG
SAF1AwQCAaBpMBGCSGSiB3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkF
MQ8XDTIxMDIyMDE3MDkwMlowLwYJKoZIhvcNAQkEMSIEIFP0mRBiI1gpSbRbrEhT
xW8uQ+V/G/cm0B6495mnsKVeMA0GCSqGSiB3DQEBAAQUABIIBADgh7UByrX+esUzQ
I9zNqk4LnbgdQoUdeJtdY2Jvy16d1V8cfIFNgn8IluuJI48a5yJwYG3060AkVF
JC/hq7sSBClZNVb9UioTixGi+4nGB2iRb7TKsfamuyh5Zdjg40rN8N1H4rwUQ1K4
Sis2TCi5/TSc+UYG7rH+YyIRSeVxNCII3rEA8E+dDRg6R5bq0THxInQbBvG9q19e
peIntJeSxvRSOSYwcoNGXenZ6S7eqfB3iln65d0gURSV7hPSfZwh1QSZa47egE7V
9Dge5pbZYQgeB27mLBCpsgRgYKbQ/+NBPBexT6Kxixd4sND++AZ6kUie+AvUpXo
+kGun/Q=

C.3.9.2. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline
Message-ID: <smime-signed-enc-complex-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:09:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-complex-hp-baseline@example>
  HP-Outer: From: Alice <alice@smime.example>
  HP-Outer: To: Bob <bob@smime.example>
  HP-Outer: Date: Sat, 20 Feb 2021 12:09:02 -0500
  HP-Outer: User-Agent: Sample MUA Version 1.0
  Content-Type: multipart/mixed; boundary="e03"; hp="cipher"

--e03
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="799"

--799
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
--799
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-baseline</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.</p>
```

```
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--799--

--e03
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVTOxbA
MAgS739n03TpRw20dqpbfARQejOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVmpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRu5ErkJggg==

--e03--
```

C.3.10. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 10640 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 6856 bytes
    ↓ (unwraps to)
    └ multipart/mixed 2367 bytes
      └ multipart/alternative 1415 bytes
        ├── text/plain 476 bytes
        ├── text/html 636 bytes
        └ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:10:02 -0500
User-Agent: Sample MUA Version 1.0

MIIerAYJKoZIhvcNAQcDoIIenTCCHpkCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBE1FVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCsQGSIB3DQEBAQUABIIBAClgXf1Y746FTqdLnYlWQE/uY53acAbSNoGw
OY86dFvtfd4kmtKoF6bqyRom13sRj228BwPm4P/SiMKt40967XTuuuYFzWY0I15
```


QV1W+59RRrZnNMD71rG6Cy/t2jcn55iGjpFhVUgD9LMD4Yg02LJfvOoQLFDDvI0w
Q09gy+4+ydc65IKk4qZcn2WfTK1TyVnHAAjc9vLiTl0NPZCrPsfrm7JiKLtyBT/1
CsaVp7atHrCNZmUSb0wrcfdXkRYmMYu8Tws/+Ck/5LBKc6FRRv478oqZLpP88Bkh
370F2AqrfJvdLQZFSfqxeVZbHB06sx7y9IDQUAN5qCy72w6ULxIwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUYBSU0EgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEA0uP/nJwnkTi9bK5viGgKWQ5L
Me5kgUCfpiPFrKfzn98Wo/WeRhNuvvVbK5B+4TT7W2TC9FD+zQ0dKtoU9i2EbBlw
V/nSbVJoUjnFyPYRcAKgw828RfQM1PGZ8pRU0BMlZuk+TkCPdUAIJGsI38trL7c5
pItqwKJEEoZqr2qe3/rt2eWStYDbZH6ZCp5SktozKYK2jLLxYZ15K1qQ9tnnf2pV
DIUf8UTH12NFq9SWC/Vnc1ifoAmzgv/Q3CY5prl3Ucz69LpGI5vAQ25+iZoRyzzT
jsP7xbIHnYS+CHKS8s0IDL2vf3/b/cSOp756tuVd4kGBXYQdA5NV0ghvPXX9BDCC
G34GCSqSgSIb3DQEHATAdBgUgBqBZQMEAAQIEEF90iG3j0vWy0YsEwUhg86mAghtQ
J9wQwdRPPRIjqaFR9ciP9ECMC1tXw3uNHjsj19tgTgzT0WxgwuKrHDGzYyWRPtFD
pEYPXbYKmjH6w8fr2a46v8nQTgErdh00gPQsc/FDPI4s1uR+aCd1H3pVDB2HJ41W
uJhtyalcbFT9As8mNk9izHLd/K4POXKc4W7dhv66BbeBMVBseFDbGoqPalb1RHsI
c7sjqLUsmLEWIKu6e18/KHFuxW/m7p+HPITcN+MzhsIr0AzpAb8tvy8a4z7FCrRt
B1NLjzGSK1qIswiUpkhWgv95ZjiJ2jX9+Bu0GXWdn8c4NNlyQQSS0g7G9H4gS9m1
yx3D1UMHko+nqGuFDECX4yE96LnKFK1hhWkuIRC2L9bVaMB3lh6D/K+k7A51DZx
mr0nb6q1rkAS6xr/ILUCPvogo8x+bEK8fufZM806AaL8cRPxGHx1hsV1KVC0TGka
sGm3koZZrSX4Q0MFYQs16HHAFlnCN6agVFema6sbqC22oNtjsTd79Ee0S6VyMvh5
04jJJqbdrcNMh7LPTbPY7sesrJwMy9VgWh3qHM8q04JLdQ0ssxs2WI4QFahF07L
6Ldu4yKChpXME6dvuybeAjmKdiCBUt79BXhE4frn3Lkm8UWQXUV0nUrGRdoFszf0
5+l+SEre/4oLtBv/IIKF9+rwZzScLvHZNhaZq/6rK2s1C/UlAPBKP9eP1L3TAp3m
na9wJ7kmaTwo9xKFLYP9yUv4sMe8pdMIZqGgh22ijtw0z8qKHi9AaoqXH41y6wmA
r9eZ/HIhXtTBfCpRxBqU47wg4Cn02kk8is43xI0QjC1AfNpWEGA GvpZjyy3v4jE
REQ0xJiu1nmUkyUorx/9N1uYo1XeErF5oZX2J00WR/YUQZhjvLK1uH8iEdXp59Q/
BLo7yKDKt/TwY/3IdjDsx20SgVLekKr0cQC0iAchM0Zg37DGIQHZRknff2aAGhjK
oWXXlfb4M2ym+0BsBkgJHrH63Fk7kxgN9VwUyY5HxyWCQDKauMwUk93I2tNm30i
7PfnkD1S0QM3cw4XvQGgQWfmBEp8P9q04QVzeiZv0y4IoFqh0jiOLlkaup+Wu0h
zk521U/im2A9Mz1W87UNNsFpTz3pP4k0ZA1lkVSH/HGhCivHqp4xwIiIECyt6U56
S72X4sUedoBFRZgZYEfki8XJgaFQHjFLVSTqbBifQbWELa8l6cJrGy7W+Fb1d2oI
6hLQQP5r//j0cPfsTayrV8o7Qx1cbW2bQsPkCttjB9tM9MDwR1ID4iywG80eF/fd
F1H0+6pmvcegreEdmSYJr4QgnqY6thnyBBiFvdSGMUP+3Q8jZqHxiJUjYY2BYnNL1
kjIe+0M4Eey/U4/kUxrlNjzxvXd+7KwVjJaLwPpVqbfBq8cBx03Q1yZPGRx2xVN
4Z8EbSA01oPsdJSrjfgM6oYwz5k/92795rNB8nXAQTqcEGBKbajJbqEb2IjLXCzR
bvZBuWESmwuzqqiCpf7WYyJV0EFQXEdPzXtBe3TAy34J0RLaXKfCdKZ5oF4coh6L
WFlm1QqJfrsAuwb4L5Qe0H0XQLCGnORRGtfl88TFLxd8quUnxHgg0lk07UuT8VAS
6n3N882CFN22C9BNKR5+3bdpdQZOAXuJY/5jYPVSfx9p2y6gmJ+KLux1vYyB6CjQ
sA+bQRqWqegHw5kN+gTXt0UHM0Adqw8D8MPHhU77MwRzaFb6DK4Y0LPBZoVUgXsg0
8Mv52yq5cra82c89712+fHaY43onEGJq2VmKnLkiCbQExVc4c6h+6AnQleZQ0skg
5Q8vzFONHIiHeGbuABnCHmmABs8RyWm1Txlr7MUJcm7gR850sZ0e1KqRKWLGEM4n
5DH2JWl0cYWOQQpnwTWTl8y7hq2rzclQEpfzthH09Ezu3GDBieIDdmckDxtq2FrW
Uo4F+VbqnJLdD/h+QoZGNcCqWeZBeSm4qRKfHbZCTXE7pE6D0aJuw1Shov+Lej85
xc+Fmb81gonG7c3NqajMC0CyjewQULR/qMUURaZbQkQv+GDjkzAdRjZK1cc+JUaS
m6cj1xsZIwyxELtXNBfvvtqPkjrjvzNQoatQhAA305TS9Q1QAKJ1+LenQb+otDmGP
hQUaw5Db/w6lheBxqhW/rQC1Wk1YHcTl7vQr4kUK06TjRQ9RIV6ds2V5WDrhEFbn
O/KGHN7k+WNanxMmhyN3Vpnlz6J90EaFTm548ELQUnEHeQ2z9pJc9TGAAzrSakn/
WgWgonMKkXuQV8jB/CkpYWRXSH6TvoFjMn2wL6SeB5ax6cmW/0318aGJ9otfcXe
0kyNGKbiiT+raZlt7Nno7B9JHLJa5estp3dxb3v1J1lN7diERT++8Gqo11cm15uV
cgdBmP0h1hFRSirl4Z+1DHJ3GRjHoDS5yMI57NpmKC04AsM40RXOMSQdm+RzrUfA
8j9LW3/5MsLORennioIz3/Zz25xpEwLs8VlCP4g8WKncrKluJFc2BECaA8KTC Dai
elIDjix6aC9K2t7gwJKaWdmlUjGcrJNnxs462v4INJak8746dSi8rWYpnFYpc1/c
WPEHXmdVDIME6Sdomiju0tKhP+QrGmORQuRCHfyws8cLLDAyyJxmdQxi4Zbka+de
uBlJkntYvg8mFm5fKyZ2iUAPzFpGNvxA/eDYKPE4opLKd0rNtHakF2fhyq6m2LAJ
pGd4PJ6U5huBF1gazcSMDs0cP4vF6mBgUEB1DTUkFCisSgLHmDouZ2CLdsXcJ9ZU
WbjJbX1/ZTX9VWcd83AJW3HQD0vFHKNVL8GejHQLdLC3iln5D1I73CDT9AYINPth
BsChRv2Au0eYpwuyEoLBHX5QzFEUVh4wG5qDgzBBzx28sl2CGKvFsaAxWan/NdAu

g3mcMBEbtinMPxP2ifqaaxsRoRVjjCbhT7ouZMsPtgJ2oFJ9XGVBJ+c1l3bxDnmu
mEbiKm1z2g+TfjsqL7GIpctQKz6Nu9hr5sY1/Zvz4VrQxU0dp/WL+M4vGJRHCstX
n+kLYSnepevLEPP0j7sU9Mokt5jVNx1iEwJ3U4P9g+LI0oKrUSZczoZ+V/+M0vi3
oBS18iTfFR7840zWLD5DWK1lqIrnEzLSVV/pZ6ZmVxFK3zan/AM4Y82IvzM8vci1
/eNI1Tndd1JAZU5zLak09u5eac18GYkk840oqxH0X6wsMh1qftgg0BABA0U27cJ3D
7xuXm7EWcUXrQMVpNG0/eG9VJ/it8NUrp1k8QP0KPTQs43jJAoHREYb6deyEwgTt
3L+yqE3xoUB0SQsczkcXGg7ACv/sb0clhUon4PngjT8e+gc6SM1YckQT5KN7dTe
W14Slku9qpSMVJI5+XyvtK40X2LLuKjUCQDz2tThVu+AhdfigUqyMiSJr1/fcDDy/
w3lQQioXXXU0dwJhgzmHG+016o4uOHxN4iYijfkQW+Zil4AGMF6xNYbw8iKhM08r
ksvdV0g2gCSwiISXH7bfynWXD1QrDSbr4DPW0U7/EfvH/wGX52wh7EprDPTMa9Xh
aekbkX3QiE2R/LPrCM7U4li+FmEw/d6cSK9Ge2HYufj6z1PpKX1tyLD+Ucosj+yD
dufxtDKIoXA3iYISLc95pWcAu9V+V041Rv+OBH3vY4KsLLi35aF7F8xaj2HjFYi0
Q6UjTSxWSOMEFmRQm1KFj9brBWFeZUx+C/kFDdtRg9ZPhUKxjSQTgMuJoZyFq6B+
vIrmQT007RTaQgZZDD6bY2cmuQAF1EJ/4oszywS+yeiyl2KvNUVUQTZ6ofCZcTZh
7i0KjkH8hqM9xYFvHU/o8ymXKc1JDDgDHfgN46NNNh0Feq56/ippiLLlIzCr5wtG
Yc48C4WhECxWIrX4TVktUHGgKJGLQYI2qii2kuvqKCavkf2z7NJW8781xZLzg0vD
6+19H0VhVreHwFpjg3axrJ0iA4D12Jq7RgdBqTiB+rTqxTTSsvMld0ad18IgFUYp
dk9kPP5heCtT/kNoqeMvTCYtv6SGgoT7oX76gU0zHv1bWq5nm8p7mIl+CumgeBoH
xhFUaLlPqGVendGWAfQmNXDIHjZ46HvzLg2ANVxfNnxvHXVNHWOyOh7GqknmAWob3
GrFF9Td9/UoFD3+Y1r4FRUPHXU0qaJq6tIY25TttzYWcvJozJF/GK/77XVIqQ/lT
gLajNfWSKNOWv+1l4Vks/ioylcXGKMtPWysEhyCdqtSnqf6cvcoEIyyjBlLJCi9S
og1Fom9Kul4HiAtXwPhSLEoipfPIVITOTcOpDp0ZtDK3Famr1IphyBe8tva1S0hH
9MOLtdwoRVbMUvSGy2gOgWVvpegVHTGNJ0nmDspvMEektjWUawtVQnkBWCVeEaJaQ
bx6bH2fWf0vHvt0aLDk+51evRDovLAQof6s54hvdW8wT2RS4B9J8VFmMM2dvK+ku
t/6AhCpr7Gcd+9LodG31XETykfwKjc3s+pKQ/eQt1C4X1ownt9IS7t9R1670pR/J
7qe8Yus3cqXS16PmWJRWMr6+qtNK0TwNRKVrg9CgWFSAYtcTw10mDrRLITDvQz+9
JTgvTaQFA60+QqVyygi/JvU7reNiFJZ4GSfw/fvpfWS2bQuH7HWms04dG74n6ZBF
i3407k8HsNd6PGHDQeiZmKlwnmr79b9pmZfw072QBmF1zxZ21+K2ts9S4ZjdmP6L
VETvWFRmjWz/Z3h/yxQkqol+VZ3U6LbLh6MJ3QdVgTXCq0jicb2hs83an949J9SS
cFfibs77cXmRpGGi6QLhRySwfCNtrbFXgvmJXe3am6t1PAvuW+3hg7JzqDi3zanx
ymQ81qgp7I2/xHY17faGyKvOnBvwUTcJ10YsbnCyLb3zhLPgW3WeWz/7MI6/V0aX
3L6acMB4yyMi0lGyQdCxyccMrqxjw5lq1kMMbJNISDTkCIqU+ROQVtz4f5TZk4Af
U+ATVySGZ23DAWsI7l8vX43wRtMn0Q5zSkDK/u1TGfh89rSbk+4bq9mbCzWNLjG6
fpXTRx0cW8pPrC9JGKDxjss1dAYK25GX512g63g+gWRcEzUEPTjpY48YjEcfonus
TIWEvgrdorecsRmwyB0vPYkEy52JnKjbppPTM2Weow3e46VVsrmgcB9Ev21WbXH7
RqK4EtgDpDKNJtmpw/14w1+Tyr2IuOHXW0mfWkSz4JLZD6f0JS/v6DqYU8spFRwV
qN1lgvvcmw6BfxKoym1JMM0kb15iFxFsFSZLegDYRZmBkp1JRFpWM0qti/R0ngM
f/QfhOps5JLznigPwK5XdIRE2N/53uDJ5FhGsUy7FnZYgmJiSXC0asNngmdQ90Zo
FQ/uijNReo/ozFhlGElBU84o4qaUDYdyDAqQ349npZt5XxbHpcHY4FwZhiQBm0A+
7rInBdHfrFR1ZkEZtnGr1GV2KXZk8aPQsbQMzYELU841jSpumlw/NlTdgzbzGus
T8QH8kRbZLwItMQfofo5+VPJoPvldu8m7ezixf7H53fhPiN0jAnk1MAM+mCPGBNk
W1G7GVAZA8eIqRoPvdVh6GCBauMrrLL0vjGX/wF+Wb1tR5CobfWFPQy58k31f9S8
AnyXUBuxEqHz1UZV/gS84sE0NxrB7bGj5+pFb0As74G2qprKVuiCQ/OANa7r4I1l
r+NehvRu1f4piCbk5gutF12kig4pEpvzdFQSI3Zn8Y/nMj7nuzQjkkooH1wdiw1X
8DjTccNQbEuNUaBc4zFogJHIQve8GuXAZvhslda9YWZtL6JfBw+sju68I6/Ubc0g
gslspiJ3+EDxXV8UyT8+Nuw/000mGidIwenHENutkn125rgLiTSvdBASsP+Qo+8x
rczJqeqah8MM/IL4WRNI5GMDyGFZDWbVBxur6JuVS/zqYT4Fwk5B5ae1CueLzoW2
7FL+9IKLVds9QPGGxz4Mo0b1M6uknK1lCtUMx4vI1V08J0F/vtizCu8LqMm9YI8n
++OXIEPV/isP/faYsFaLAc+Sv0aBniCWKxkIO6X8S6MpcVswKzFTpvQ7Neuinbji
eOSTPnciebKkKAw5nBtb0s6gPuvJg0ABVD08rYei8Rxp84WvUU+P3nzIv5StGDdi
M3SJ+vSVTZXY3CQGEc760i6YfsQFTD80Nz1vdbhgeF9kBQZUAcPJhfhfdkJhnjni
GWRW9Toy07Iufd2Rqe8qZpl/5e8YeCjraE+8FYgRAMNCIPn19dvBT0kRS1d1aV29
iZQWcvt5jCULyeCoQ+Qiu772ZlgToKMS6dP8Rzu0CKkLoRNQzsbTctEL+8wIM+Ym
u5y/nDH7Igvf1INUPuU84CghaRaocFfmTF7iPFb0sq2WBq5hvtGXRqh+k9vpq7yj
wIzbo3LbPalddV21gFhpd7ASg8u8bAgEkarf+C9cejIDtk+/WzilYuX/yzv88aiX
KwdXrwk0GLBHaRsNWPipOUxhleyfA0gzSSm57vGB48qsR11p/ZeWNSLabF9cLKJI
eTi7BEg4LjmlYKuLNsTj5ahbjrerLWiMgX+fUkss3mb/tYc5/FS+GL3t5gpt/z+v
AwauFCK5hr1mKqtzFRr0PNycXRhnBz8JKNJRCnhH/7pze40Zax3Cpn1lK/TmSPjE

```
s3X4vRfC2jn3KDbwd6me3AAkHikYmnLlE7I4WHyc14KtIvw6ZUcHvYNzL0rUJUdw
Gn9/wc1MLJib02ZIm9JYgXIVYeLTd2zqEdTU8kA0ZSU4fib9yFSPzsTqfK1FWQqb
KxG1EkKMeS00ZXQieebr+V5FxISLdC3iShBCxouDlSVKYETC70/Cmq44LDDtDC/w
ymdXt/kRTv/Bj4ymTCKzMpKZCKhtWCaEuQucNcVeV01vj+iHxfZuIXxJE/Xc4+V0
g0/OnaEc+0N73/fNkV/QFrOnOC/u1jeRPSWUWkEK35UYCIx1/wuJXnXDDZMVYy40
GJOIKqOCj0jATNR2m8ParmrywvF+IEQvINz2G5VAYDeolRqaL5azDA7vuS105oeu
E0bZ6Ug9KUgmR12ZEU+28oEjrFLBNdp0s2BQQJx0A1kRYi5ba0rcq0oUWDnbXVW2
MywIzRNt5RgTxQEXh7PaauYMC0qSoxb/9lHzp63tnowQ6wSf1+9s6tkmq0cqHuwC
p6Sv+faNqT6VaS38LeQK61hgt9nB00r20zcc2qYoc5QxJH0/dzpPNRutqaf7Lm30
GLvJiAjn16D5+Wm1M/gqTCmG8FRuf+KaOpVFeoXMNhFVjNPtJP68x15WD0iemszC
qNTjE+Xy/Z0keHNdPuhPA2BcG0lcnawchEPibXFBHP1Wxqo75f4bLZuG7mDkvdP
63Z3N08XTMqWiWyc6EpwIh1XZY8KH7zJApLuCdovDjF3CmuwNFP05vGdu2zKx2Z
VM0e34JUy8/Y1VfXm4L4gKJbjByWuH0xCavNOHRknSPZRhrgrNWZQ423TYIHjRxU
b5Bzg/bEXZntfWJs/j6mCTHrUepBA0s675njsNfdoiJW7Swa9Rm/XtZnKetNSBju
QcDg1GqXmLhe4ELu6wLs7n2gIqHAL0XEm0bBbCGD1ah3SnTpYNkkKKRcbg3D7uW
c50RsFu5EXiLza2xw1E0Xh109Br4YW2aoM7W58Lb1AQ0uDx3wMISdWCCSuUQ75Tj
8XFAHLH4iITsWvMcNP6+ExA2otAcFhuMCsMHLUm4m8wTh7ogdrkZhxFrD9M9/Qu
MbIbqS36eFtjZshXBU6iydu0jCWHZ4r2aXl68XwunN6HSHhEmsU6+WKHbEKNkE9L
NWJsPljtDuM94Axjrf5MLugZge9Y7C0KLvmVUn9p0Y19CXEAGpGFHbSPYQCSkXf0
YZxU45ZwSKIP8P8QaomSD3y2xVFqUph0xm/CLPDwkSZm6Wl3ZYMKNuhR0KxeP4tc
DUNfKRkyvZx0M0atctx0McFN9JrnebOMh+20NEYlefIHI67lRUPOVguMOK/XIT4
we0+LLiFJB9bFLDXd6aib3JY3jVf/1nzGKu7+Qr6XnL+Rh1qsBtt1aBWhPjwf960
1b+PbEBLZN+J8EErhbaNJBQfigS9fBE/zk/I90/fUqQxhX1AofJwH+jXH4XAfWTr
04a6dVJThq5yN8kWrDUP5TDY0dUf8gvML2s9BtVmRARquPBQGJLZfhh+6xJXdi5c
1qaCYxN6IwYc1v7ctxQtahSVdu89QXG/SxwmkLuvIbLfhJMnE0Sz+x0iVa2tLJFz
2GyJb6Nklwwk1YvG2QALEaNL7jLP2YcQUdg8LbxKgmPOFhRRPZrwvzXcrgRHIQ1k
No4ZCWBkHs0HZEBzAeGKP0ZdRTley0lG+RgkHEPgau5dLnlnaKlKUInzbbsvpv/Z
Do6Pp1R+ezTkMoDFmi0UgGrHnhIwbrsciYeqCaCaCTHvCq4Yc3dry+nVFlxMqq95
X9LucfCcSAAvD0QA4ecf6LpdTIPnv4LcdlFqR8ea6uw3tQ1gqxUPVioTsavfV+Nn
xCGcDCoOqQkmYz0WjEklqJUJU4B8VkdgjIz1/+kD0DZKWuo7WGiphhqv5M+VJRr
5hldXDMRhyaNKA56Sa8yN3tWHY0XmHPgU1XL3MT0QT2GR51QbWq16+1sCkeaFL5b
0jvQqWn6p0DbQ0qNzCk+qqiJjD8Uz0FkpN66amptse6KXgc71xp5fBE7m6VUHV+e
6yhJ+9NcCA64prKqBxosV0yb5SBWZGofF1pgmbStt+1hvcPA8TS1Y3L1Vd8GCNP3
BysnpeELKcGGHjdUovPTWk7v/ewl/dJ1dVgEiRsnSU7G4bMhR10Y3lRER902wjLm
6zdOuNbd7LrTimhtu6lWIFtSgrJpPNKpDtGjGn5X8R8MuAFJFibkS4uMbL1Fty32
bESHzoLqSLRgWgLPZQjmrTyv0gvYyauKjZYslBnVqjd+oBq9JUgXh7xKsG+z2KQo
V4QC4M3z0ppx76fYMETf0MjP9Pm8KyuhEHXIBAXoVE1rer2m1ptaJGF7wUJAqEL
uJiKSztN5S5sFe+a87BsIlDWkCLZRuD04a0+ndSd343yK9CMfYKbknZXtC/cAvD
2cwFag+qix+351gdmGd5L8tQC9V4F03uy0JQU90g0Twq0nE45fvLj0J4rnivuQkD
NMypJdswmGcd8TWFdb8kQMtZPNWuupbV5w1lF3ibGEhGqt0+4/gu1ua3jg+cHI3o
oKBZUuvYGLXrbrYnPE1b3HQXvxDVd8m/+KLDNiwyQ7UT676iJn7ARCYZCwP/D3g6
zMc3NXJkUZ8KF0HqokaaJ3jleLoMi6JB23bhiv/RRJuYk+TCwX7uBKF8fnt+E802
YOhbKcnThdDUREGM2QrsjZeHZQ6qgIkLUedro8EsPI8=
```

C.3.10.1. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"

MIITdQYJKoZIhvcNAQcCoIITZjCCE2ICAQExDTALBg1ghkgBZQMEAgEwggmeBgkq
hkiG9w0BBWGggmPBIIJi01JTUUtVmVyc2l1b2JogMS4wDQpTdWJqZWNo0iBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFmZlZwXpbmUtbGVnYWN5NDQpNXNzYwYw
```

LUlEOg0KIDxzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtatHAtYmFzZWxpbmUtbgVn
YWN5QGV4YW1wbGU+DQpGcm9tOIBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4N
ClRvOiBCb2IgPGJvYkZzbWltZS5leGFtcGx1Pg0KRGF0ZTogU2F0LCAyMCBGZWIG
MjAyMSAxMjoxMDowMiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGx1IE1VQSBWZXJz
aW9uIDEuMA0KSFAAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVz
c2FnZS1JRDoNCiA8c21pbWUtc2lnbmVklWVuYy1jb21wbGV4LWhwLWJhc2VsaW5l
LWx1Z2FjeUBleGFtcGx1Pg0KSFAAtT3V0ZXI6IEZyb206IEFsaWNlIDxhbGljZUBz
bWltZS5leGFtcGx1Pg0KSFAAtT3V0ZXI6IFRvOiBCb2IgPGJvYkZzbWltZS5leGFt
cGx1Pg0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTA6MDIga
LTA1MDANCkhQLU91dGVyOiBVc2VyLUFnZW500iBTYW1wbGUgTVVBIFZlcnNpb24g
MS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9taXh1ZDsgYm91bmRhcnc9IjMw
OCi7IGhwPSJjaXB0ZXIiIDQoNCi0tMzA4DQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UeXB10iBtdWx0aXBhcnQvYXw0ZXJyYXRpdU7IGJvdW5kYXJ5PSJmZmYi
DQoNCi0tZmZmDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Z1ci1F
bmNvZGluzZogN2JpdA0KQ29udGVudC1UeXB10iB0ZXh0L3BsYWluOyBjaGFyc2V0
PSJ1cy1hc2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNCiN1YmplY3Q6
IHNtaW1lLXNpZ25lZC1lbmMtY29tcGx1eC1ocC1iYXNlbGluzS1sZWdhY3kNCg0K
VGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtY29tcGx1eC1ocC1iYXNlbGluz
S1sZWdhY3kNCm1lc3NhZ2UuDQoNCiRoXMGaXMGYSBzaWduZWQtYW5kLWVuY3J5
cHR1ZCBTl01JTUUGbWVzc2FnZSB1c2luZyBQS0NTIzcnNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQv
YXw0ZXJyYXRpdUgubWVzc2FnZSB3aXRoIGFuIGlubGluzSBpbWFnZS9wbmcNCmF0
dGFjaG11bnQuIEI0IHVzZXMGdGh1IEh1YWRlciBQcm90ZWNoaW9uIHNjaGVtZSBm
cm9tIHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX2Jhc2VsaW5lIEh1YWRlciBDb25m
aWR1bnRpYWxpdkHkgUG9saWN5IHdpdGggYQ0KIklZ2FjeSB0aXNwbGF5IiBwYXJ0
Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGx1DQotLWZmZg0KTUln
RS1WZXJzaW9uOiAxLjANCkNvbnR1bnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQN
CkNvbnR1bnQtVHlwZTogdGV4dC9odG1s0yBjaGFyc2V0PSJ1cy1hc2NpaSI7DQog
aHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNCjxodG1sPjxoZWFKPjxoXaXRsZT48L3Rp
dGx1PjwvaGVhZD48Ym9keT4NCjxkaXYgY2xhc3M9Imh1YWRlci1wcm90ZWNoaW9u
LWx1Z2FjeS1kaXNwbGF5Ij4NCjxwcmU+DQpTdWJqZWNo0iBzbWltZS1zaWduZWQt
ZW5jLWNvbXBsZXgtatHAtYmFzZWxpbmUtbgVnYWN5DQo8L3ByZT4NCjwvZG12Pjxw
PlRoXMGaXMGdGh1DQo8Yj5zbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtatHAtYmFz
ZWxpbmUtbgVnYWN5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGEgc2ln
bmVklWLFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUeTdUyM3DQp1
bnZ1bG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGh1IHBBheWxvYWQgaXMG
YQ0KbXVsdG1wYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBjDQp1c2VzIHRoZSBIZWFKZXIgaUUhJvdGVj
dG1vbiBzY2hlbWUgZnJvbSB0aGUgZHJhZnQoNCndpdGggdGh1IGhjcF9iYXNlbGluz
SBIZWFKZXIgaUg29uZmlkZW50aWFSaXR5IFBvbGljeSB3aXRoIGENCiJMZWdhY3kg
RGlzcGxheSIgcGFydC48L3A+DQo8cD48dHQ+LS0gPGJyPkFsaWNlPGJyPmFsaWNl
QHNTaW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZkHk+PC9odG1sPg0KLS1mZmYtLQ0K
DQotLTmW0A0KQ29udGVudC1UeXB10iBpbWFnZS9wbmcNCkNvbnR1bnQtVHJhbnNm
ZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdG1vbGogaW5saW5l
DQoNCm1WQk9SdzBLR2dvQUFBQU5TVWhFVWdBUUFBUUFBUUFVQ0FZQUFBQ05pUjB0
QUFBQWNFBzEVrVlI0MnVWVE94YkENCk1BZ1M3MzluTzNUcFJ3MjBkcXBzZkFSUUVq
T3l3aXZkbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3a1oNCnNncnmpY3FW
TXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWbZlRQUmljaWhBZjVZSnJ3N3ZqdjBa
V1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUNVya0pnZ2c9PQ0K
DQotLTmW0C0tDQqgggemMIIDzzCCAregAwIBAgITDy01vRE5l0rOQ1SHoe49NAaK
tDANBgkqhkiG9w0BAQ0FADBVMMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBtIFJTSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTagFw0xOTExMjAwNjU0MTA4YMDUyMDkyNzA2NTQxOFowOzENMA5G
A1UEChMESUVURjERMA8GA1UECXMITEFNUFUMgV0cxZzAvBzBzNVBAMTDkFsaWNlIEExv
dmVsYWNlMIIIBjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEAmpUp+ovBouOP
6AFQJ+Rwp0DxxzY60n1lJ53pTeNSiJlWkwT/cxQq0t4uD2vWYB8gOUH/CVt2Zp
1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6h
AQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXj

```

WShp1cI3lcvvBZMswt41/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2
lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvWdhJLAgFpW/jA/EB/
WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBggp
hkgBZQMCAATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0l
BAwwCgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyA
KRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTAN
BgkqhkiG9w0BAQ0FAA0CAQEAgU14oJyxMpwWpAy10vK6NEbM11gD5H14EC4Muxq1
u0q2XgXOSBHI6dFfX/4LDsfX7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZ
ncxGwy2Mfbh1Ib3U8QzTjqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuivZfg/m5fF
o/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR1E5K9JiQaJY0nUmG
pfB8PPwDR6chMZeeqSQA++0IKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS0
7K459CyqbqG+sN0o2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQIC
EzdBBXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMASGA1UEChME
SUVURjERMA8GA1UECzMITEFNUFMcV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBS
U0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1
MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTBTIFdH
MRcwFQYDQDEw5BbGljZSBMb3Z1bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0w
I2juwdRrjFBSXkk7pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZWIeYXFK1QHJD
73nQwXP968+A/3rBX7Ph00DBbZnfIt0LPgPEwJttdg0VQQ6Wz+CRQ/YbHPKaw7aR
phZ063dKvIKp4cQVtkWQH6syTjGsgkLcLNU5LZDQudsGV+SAo3nBdWCRYV+I65
x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWC0nsG1lyXt1TL
270I6ATKR6JWiQVCCpDtc0NT6vdJ45bCSzsCAwEAa0BrzCBrdAMBgNVHRMBAf8E
AjaAMBcGA1UdIAQMA4wDAYKYZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBz
bWltZS5leGFtcGxlMBMGA1UdJQMMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIG
wDAdBgNVHQ4EFgQUu/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0jBBgwFoAUKTC0
fAcXDKfXCSHlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgasN3
/ggSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNv0Fb81V1iffR
TF/KtmVEDMR/sYeqAH83KM5p3e121Vh40HhyI0qNuz50ShNaACsioQ23WxHGvy9v
sdVfnbhsplRwG9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0I0vg6mrYkK
TM/RCGnumghxwYToj10yD5Gs4D2IJCw+FX50Dxh52MbNRYXTus2ZPRPM8JXNQC4G
Wv4km3M4rKnJDD6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H4Con1B8f7R7s
1LM2cSYxggIAMiIB/AIBATBsMFuXDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExB
TVBTIFdHMTewLwYDQDEyhtYW1wbGUgTEFNUFMcU1NBIENlcnRpZmljYXRpb24g
QXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+Gr0mqnXMAsgCWCgsAF1AwQCAaBpMBGg
CSqGSib3DQeJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDITixMDIyMDE3
MTAwMlowLwYJKoZIhvcNAQkEMSIEIDe7/NLwTkhNon7IR1M1xi0bMU+8qMIZ1No5
ANcjz5C9MA0GCSqGSib3DQEBAQUABIIBABi/HvXTe3Z+La1tuFv57ZaUvY6kegwe
OGiZ5UPa5FBpQxoE/1vp8xG+UVIUnpdV/1THKpjKFR6bZZff1/4u4NFeBYwI9yg+
tK1cYz+B2cscX6FDAGjUr/6QxM0wd+o17bnlZJJDrXvv8B5A0dHFosy0rDSrvn2k
Pzc6ush4JvS3aee5QFEgtd1bQx9fx3t/QhBsn5kGMC+3FzvKtmAYU1z0unqvK4HV
I40Goh/Fm3uzNxtQ3/rzE7ws1Qkrp0VlBxVGgUa4dZ1VXVIizkRz1PRtis66F73
EXJlygf9Btm/TJDUivXGr7fCI2i+njByX9vqUf/0UANsPevCy0HQWCY=

```

C.3.10.2. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-legacy
Message-ID:
<smime-signed-enc-complex-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:10:02 -0500

```

```

User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:10:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="308"; hp="cipher"

--308
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="fff"

--fff
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
  hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-baseline-legacy

This is the
smime-signed-enc-complex-hp-baseline-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.

--
Alice
alice@smime.example
--fff
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
  hp-legacy-display="1"

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-baseline-legacy
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-baseline-legacy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--fff--

```

```
--308
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGGoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCTkDKnbcLk66sq1T+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--308--
```

C.3.11. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#).

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 9925 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 6342 bytes
    ↓ (unwraps to)
    └ multipart/mixed 2003 bytes
      └ multipart/alternative 1104 bytes
        └ text/plain 373 bytes
          └ text/html 468 bytes
            └ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:12:02 +0000
User-Agent: Sample MUA Version 1.0

MIIcnAYJKoZIhvcNAQcDoIIcjTCCHikCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAIT/yEi7Aox0H3WdBU9Ff3ge5PZyEKHiXwCp
exVEZRgKm2m1PHvc8STLe9siVxz90H+MbPfTQ9RYRw+xi0mvK+mwpCPfAf9QDCWw
4du75zCBVQ0Py/m6+SDQRtvHyesEe4taEjnI07DcGj5ENoE8ugCcjr34HmBsIILF
+OLJQ9fTXYjeXQbXjP0InPjQk1GgHnfNXgtIcTM4XEA/EEjPSrphXsifgnBf0Dm
smBfCKe7fSPN6tEeP+DIQkuQVZIrBZd7f+nzM99ixMH7kpI23G1+BCLeSr6M4fjf
```

gMoL4tuj8WgT8kr1W6x3583f0onWNsVDW+9FJp5iefg5ou9g/y4wggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECxmITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAIN4h5gziR7BMQ587FEgEjT0P
M8QJzMfBP1gZL/P0dBeNvMqLMABEZOna24NjftAZw887hhvv5nHuJIBtE03ezN6V
wZn0tzznuqMXBExx0Hq+h47VahUNmg5zr1VYBVg5001vXXPVoIWjW24vwZo9Q1hp
0QqGC0MITLN81RpwG9FTgvtGMx/uDs37IxHQDDH81VqSu50BbuDEYPgD6U3NtzkC
uVlW9aSqA0scGwib7bVLdmIoL3f++HUWD+YDKHnZ3M08E2u/trYTc3ofiU9RImKo
SjMLKQVGQYXg05sXb6IUWSXxKi43BfeI1YcQsHE6TMCcBN5v4esQ7rDyIKLzXTCC
GW4GCSqGSib3DQEHATAdBglgghkgBZQMEAQIEEGjqoAw+Ed51rHpzWgYvdraAghlA
YTD4kiJvM0Lc1TM5w1rdgJ4holTX6BDFIUPye3Mk0g20XYl+XKES4fW60C0vad0j
2A6N6TbJoxrHQFy3tSCnLSuQf004BY0Y8u300s7HMKV0cQKFkFAzv8STtpu2u0UA
2pKrkjK/BCYQ89GzGvhSInN+Lx475Hh811B8Ue3JrxI/x73cNufYsaPUMRQnYxPV
F0TI4k7kxaELKwradV/owdJnu1GKq68tX5/GRoQMhFAZHrYdYDzv1G7FHRVQx8cK
2BZeCEfCvYbYFu31hVmu+RB2MRFsmKt7FedNnc2cqNLTaCJURE6qSMcsBfxoGME
TjZJUvtB2Fsoe02UvVz0QvoJ9odB6oihKRsaEUe14w6aIpgwGS8h8LJiuG5yFlmj
j0kG4sQu14wc9zHG1P3MZ0ivrvUCxag900Y/qI3aJNj/KgyGyx2ncuYps61w49kA
6QSnvPBtcoVGmu+VlmtSS5AscVHnUfcrj6HYI068gVdJF5zW88qf7qN9rQaL62rF
Llt5TXz6TaM6+S0Q14QXA0nGk7Ee1iy9e5Anu2DPm0jRZfujwouvzj+hBteIMX+G
kx7f8HiaSZP7wCAkw219gnaRQbyUvDaYDWlAS+ldBkK0jX+zH33T19F//aKw5grY
qAcC08rXY6755AubfhUk1xmuR2nDeNIKx/q+ur/BUhrXH99788T19GHJVCqVuzk0
R6wAUL126kqU5HWRfXqzt6yjoWC+YU4tZJQRyFZmyU6BvSJhcKck38lwktvXuvb
GBQ9Dmu+0qUk53SXEtbnxgp054JyNRBpX+FP3MWqiMcQdLY+iI1eSNoatXEeLRTE
IzMicYgx67jI3rgAshwBDBfxhXnqlbby9/IJWsmfYlInhiubdlZ/wJMDnPMbE88r
pMw5IccDR2jM5PvQsRjRmPfUDkFXBio2KNUVMJy3AWpCUKu4/JxnR+Og1fs/ffbe
m1b794TlEctK8iXRzDp1CLGFTpsHtA3RYHHPd3DM2RPeYl1FYWILyuHTbZB7soKG
dJR0gpL6V/zpxo7y59v7y17FEvq8+OwVkJGx8pGrAPPd9R/7S0j1qxSZVSzgIEWA
9fawYV7IcaSH6FhBSUgbQRm+javR4RgPHTSHrenFUm0/hPT1PL8GFddZFnNhHZ+w
ktF9x98Lf/RlSwqT+01Hdgd1Hk6EytYuLRhT6h7YxBIb0iKPe21hVV0jFqnAqAlI
YhAACyQ32SJGZAfPQ1+ttP6g9bGxKWb6hxn+eWENR4BTbSujrR6dkFIQW7fFBZwDE
PMTZ8tJ8V2E1DgU0gd2RJabZ+FKa0DAArT4dFs5RsmCJBCBrydtE1Qn1QjoWsdC2
8HFI9h87fxcAs6tSTNtV6dLIgnDCu2kBWKEmaAbu07E00UPV8708WbXGy4889CE
4SuGldMTX/h0r/wzSim+HFndJF+ocLL/7R/ynV6V70wYsGy3Qba1DrG6AH0QzIMY
u0tK2R/y6KDxKTQU0Qpt4TBzDJu96D48b+BxIQpB9KXSbNsNQuHBq19A30FLzhxb
kELYZmenmi89s1mRgdjQ6r5673r2kGAD5601XLhtT67QsrBNMe5FX9EKHIKdamSY
a8web1LDrpPHI8K7tnuJiBPIF0/vAiJRkJ2ARDcuHEAHVu60NX3+0dy1xiwMkR8/o
ae7dI+RQWgl94g6kd1AKT7p0yA4Paah0fZZ0SYwmR0MTXmt74Xl0/AWgL0K/GunI
4eCrBCT1ewUae109F4ue/2vm01wt590GAPZM5N48LvTjLo77KYK1w5RlFawWCnGm
MHw5osNEEcntNcukumQkoNVbY11PVH27L51Psm6g6sZJlaXuFz3o1k7mXUJjddqPZ
TPem/JqObrkuIAX01b6fYasm4eYZ4Jj0GvW0xZSVP3dcEj0+kWiug9/8UVjPqd38
GAaxDn9qoH4sVfFg0Qm9HLnZ4ebSePb5xe/kb1ft5iPv63T/1tWe5IOkqRlKTKbS
WqhiksIPGv2nruMokawT0e+lr+CCE64epfC1N6YzE5zcx9ZzY67iUNljG2cBYXKR
028Ik9ayqjuw0YbFBET2yreVT4GK7Xn3fWAKqzkCjVt0I0w2g0pL46hq4got/D//
xT/xMCEnLSz9hZB0KAw05FAaLzbEpPbS6HsfPAgithbCHSOLAXN/+qQtUrS2vtiB
YBF5sgUTtp0oYd0u5Wqnu/XbHmHvi+uBIMoTbAS05+D59mcIwVGdutjJ0lwWITQk
0liBQwd+0Fe2Ro/yE28nsIg+sMzvYVH5gngAmS9+gmwNNr6j/MMEZTJeIdqpkjJp
98cAJ4iNrve1yTYuHAnBoxw158Rnpl+GBGB0NP25MWVs0pTuSc5MlyoufMB59hj
SMboejGK2bBxRfSTGZ7BdDM7+7KY5mQotONOCpMQW9ubklh0kUUSlUeawRSr6pYk
Fml7mUWMUP23PESDEgNq8j60GsZVT5fLxo2Sn97VhUXnXPCAE27G1N4VYU9U2CKF
G7aNU7GWNm+pz/Bf+VJ8VRIKofWYNShAajmhfizhz4SqipwLhFRMp3jGXA8F4cmM
lPKqqUz6e1eRH4bWUGPm2hynM2A9tFG6W03e+Z8PsCnshABKq/XBzkavRC1K+Ry+
rH/D3L2RluVHbejNWR9qbumAAvWQf6CZX0yZc8FVXKZd9sPSn3h5u6Uub/01kl/A
kPN0aX5ld1+ZG62301u080FFj9EMK905PJ9iinzeCFKHVjfdR23im01WOF3QSRIM
iUyPGqsnlC2yg/CA1mZTmfK6rwU04Zhd7bf9287jE0InJwrhFIZg5aFSn6hR6N
15eNF6CY3m6icjaT+Km800YjxcMNw5MmgPu0qXYC6J2NG8ppSpR6czacZJWgPKlG
XdfFfOQTcyh26KlP3P47Dp/ZK/ciDQ8ZoSxIhT7e8gI813SdwkTSy7e2razbi2vA
ZxDAQlpN1stx+do0IPjWiFrDWlWLwzcS9i0AZMHDnXY5418zNXG70wwivj0t3nI1
4i/EQX6SF7W409wjM3rGdr9lclKpRMR5dWB/Viflyoe+9UdiC4emnXosdRxxK0Umz

nJ/ej+oZGsTQ2QYgWvMFgKRrOP8tD7L6l1LMThXEvjff+HVILH71PZioML2znenC
j4SGhvqQ78/vgAKSIsXCNy67bNY8BE+vUWDSOYpQ3JTuv8af6ou6LVSPmjIQRxP+
VCoyVS0ymqt/kHFGaNI5UMDQCkX7gDD4E0RoM7t4o34MN3HwNVTri5SnqjQxkt
r+3aUWndQchUHAMH3Sre3Kr+U5+VGSuRRVa07FqKXrbaGD7IYNmfBuaV0aA8CJqX
/0vxQv3F3zNmFCh8aomVmQcQdgI0ZRFso7t/sbT+/FpgMV9xXSzp69LwrpDME771
TEP3J4L1S5f1Nuy12MYr3CfGg058erDbs9x6L172nP4WgQUdyJ9RR0wWpNUPyq1M
2YnFt1iwsGSHSszgv32ykbFhQcPujk1ZHm1omk0x+2KUKToYZwTa+OMvC7uXPxGkS
8vuBzJzQ1X3fZYbsaiyJK5uQxMj2Yp2WTLsPFEkg0xSK15i3vmCWq/kyZMwnrVr/
Ty/xHasuS1BaM+uZEVorN0yFdIwZF7aeAp2yi1j11Izh52xY/hw0cDhoo0X5a8z
V2gsdQQJ5FS1KjJzfs0nsKfXkQCLkzJPCdyzWFlmaUuotGvV37qoCqBWALzsw9l3
8zB5gTGDavIZkf04/HL9971ZcsxuPzmrV9u9NoS4lRM40uGBqlhVaXnPPTSKW7DG
zwp0ocCWWhJE5UrhDxWCZHYDmyBqxk77uGn18UzUQQ17t70/EZueLIQZROZG/701
IGaub+M1YXtB1PXPd8whCsd67NVS1qMkLADbu/S+Nr8Q/K0oVVC2kwrqb4dfHf4v
W224JE3WnFjtvkc6vDBIEEx+Qd02yw5nR7Zo+XqVyoFoHgbUyhbeWTbM8hqIFUvfd
C+BY1wU8jvWCM15NNY8R2ZwUgyfeshwpmNUbuguwy6CIUHTb1wJpYBw1ju0ggXp9
qESnDasfuZ5dIzuWMxxRwKn/GtmFejYuf4G5MVqgzH8GLB7bHmUr6yEVhZjhNAWx
khcDD2o2+6vufzxbB0mxfSg0vKMgTWA43MhFJYnw5aX6ikQiDP18HpQaJLZ5A3Ve
g9AeNhHqnB7pTz/4ZXy776K9AmyBxSXDz/9AJfdEq1bQDW1SldX9UaQjNIhCpKI
tWfu1vdx4b9Fdrqo4Fm9V01uIioQ60xyahrS+ekBjPT18oquDj1IgfWWZQH206VV
ch/9mJmqJLKuqMEkhzVm2RQsbCwvALS2bXmBnIu68sAdrKY+G4Ph/QzoGpG20jJ6
XPGID2SHF1fYKhq8bpqgtzncLXtfcPs2v5dr7ZMeKVBGC0zR/0Xr/YFHCW+E0CcE
MI6PJrXbwj3Vo6rGE6Akvi9t7BCVg+G02Lbh/cLTnClmebaXo2K7CV3913tFbeXw
FruMzbmU8aneltETSRH4BDL8pnZghhQQB+6zynFH71zRUhUSZG13ko5GJ/XmjnUW
1MQkaUfWnLUWQNwvRDn0y06q2hkPkNzJhhUwzPJfC3PhXJBZENVPsVzScX13GmAD
RFJL8HqvTdCXVlyz0HacK6Qzy5QR162gF0f+I0A70Qm8KnRKZvpeLAr+q3Ecv/z
WCWKi/c5RoTsF6U5t18oVTYZpJPuXhz1WgRPcEa6FH03nNkLdXCsyPd3/I3HqRSH
0ic92uDPGcEM9+zvV4IEwesAfKkgHpfBNXv13QIk3hMdhjJ8Z0400ENThDGXimiT
KxXfIcuJc5MGGPsSCiKRaQ0p0YIqKB+DIyEdJHvx2YDE0QFWuRm4ukFWN52LgaY4
s6SCHseFczVZ1Uh+dXJi6dadYf7zrEEcZWYqo2mzYqHqs719M30uCOrmT1Ako16E
ewgMFhENK2hzCxCpQvKCN5sZBdq7UXYrAla1xhVzPP148S4yYoFx7R37GZBB8Lmv
dCHESeIEXQ+Mk1gPo6TIgn8/0JGcfFYBLXWDzNSNtphIzN9o3TFsmicL2ofWfidi
L4Q0a3ghvADS/7rV/cu0GnG1NUaLVgF532W6iMEHMyW882iGjp0D3rNm8sDx+jRI
FBbDAIrvF1HZwTfSX1v0umSCE7a4inm9n9xUWPvNGE1zIgGJ1y/1lKD3nQs6V89V
o6J74qxrJZpM+mrSkzPcXuIoa44vCiNcyfCceSSjCNSV2KQs03n0iCbC7HF/1DJp
BJR81nccq3A2i9UJsh0mv2tPtDVFWEJ5DORn1EdtMu1rHg4HYJFA4ZEEZAACPokR
VvwV1GaYSEMYE/C4vMHry65qk3JiHkPL+ceFv1zxyL43F1xuZ0rEfUykpIuChCMA
I6NSfW/ykTdeKu3weFTDCEX0NxtfhqYlJUnmJwrHwdIVRwlKK0ixDTb1NKDef0un
4R9LWn+nXpmbQYp3n+UIBqQn3+b98H4rBTyDPq30hkzK2ZkVsfHkE5WA6x95RQm
zruzY5a48PuGAcRbGUt8Ne/lv4A5JFc1iETkBCX0zSDdWrZpAwDUXnwYjwUc9Hon
aWC2g90gTT2DwFBD0WHJoDr0SfquNsic1LWEE25QoG9yP+AByxppJJDtyXae2PK6
tC8wx058N4LnYIZhC0EoUEX5IqbNoNFWTjNeAScWXdBnN+NgvYkYPR/ATVH996aj
Vp0djJGVCFVaTphqroqer+f9PUk27qXbaK4tp1wnNb2+zK6IVQsK81+7Bi8VBYKv
3j0go23Cp+276nQbZthzf01T8DKYs1E41M46DFegPoTqFTn9Y9/CyFxQ0K/+uT3Y
yDqlmgJGCRj7Lky0gcZGW70TkgyZar5VM+uW9M6ASqenJ61HrZZ7e1NMuHqNe0w3
cIERFOT6q/njz01e5VaWWqrcPud00CPcTXzFfG9M6gEgUjzLkEg7E40XPiNFfrGZ
3RRLFP6qYJ/LFccRsD2gFQFGm0FmbK/rVGPn9c5mjf074Tqb19VvzGPYyHb94LH
6hboBD4gH/DVKJmPn157LZhj1ytsmG5tGYBzBaG5QR+C2V1YwNBFRs9A8m0hsIQu
srundztS8LickI6eR6hVp09bclXmxfA/YYPQs8pUIi2evAemdXPa6kZdQcU3bijA
nlsml4AmYNF1w192wDTZ9oVeAZH8AJSGRghRAa2r/G77oyge4EmmhqwWBxdshuii
N/2bpdiuY0GknJEo0SxTu9d6EncSxwVhAudZ2mynG+AYgJx+LM4ZriVZ7DjuPo+
gU7XLwsEZY8towvuDZsh2/6UJTtaUtr/2RGUYH2zuy4fCeREJKu4wissg9vA60e
ucAGOJg3vnnZKy5hxgNJjJhJCuy3QZrEqbsWavqCuc/Iee/rBEdQ5gNZ4AZIEcvM
idqXhp2gLSsg20+nUEVxsiQRCQZqQHwCRXjaienkctMxet2rnGjvCz/ZDnEivLfd
a6vRTZD40GzxgmK5brcltFvUJs9AY9dfEE+M1Mefeb78pDbjwBb0CN6A+P59h+Z8
6Tz8US9RLWK0rr78voT8P0v60FVHiQhAKVjAHh1HRfGe/ic3utAY4YT0Yx9B8QIL
oSFZpCSyk8st00JtmcXdl0WJVTYwPzoFtr1Ebi2MvRqKKUHKPAuuVsk0s6ZUyzLk
z23Dqu73fvt41DV/lvHXoFuT0dcWV+v3zo/fq63efD3ZKqtW4eEoBv6Vrt6xpPdy
14YG0mI9NuGsUhUTsdNV3BiyjK8KBS43Vp8AemViMfaV0h8gJgmAs3kt6UPLNluy

```

x f d f c A J l Q + j 6 N S 7 V s Q 6 a 3 V e D q 6 0 m 3 q n / v + C A R G F h 9 S G / s h + f r k b t L d 6 w A d D 0 3 3 E 8
4 + Y / L J W E l k s 0 Y f Z Z k J 8 P n 9 4 y E / k v R L R I u i 4 g P o s J k M m u h c / h C U 0 e x F l k i q 0 d R J F 8
q s 9 H 4 q m t E H C I M C K 4 t l / 3 / U A 1 d w 4 + 4 H 0 G x 5 F / 8 m H 6 W T A S S F Q l P G z b B f N H B X Y h E 4 J m
J Y d h p a z 8 r Y 5 d j E G r w d 9 g x 0 J / x 0 f u Z Q S T M Q A 4 D A y b / k e F Z Y Y / o b X o C p z T b 3 u A S m m 8
S G A i u r g R P r z 0 l X U B z 6 e R 6 L G m 5 + T Y J s f 4 t X F 7 y l U R x M 2 9 A r S 8 F a o 9 K + R T Z D R h W s 3 1
u Y a x G b y / Q F m K o v p u d a T / N P g V t p v 3 0 i h U g r E n M v h 7 n v A S 2 r k / 2 + t A s L A I p x m / l + H C
4 z e m v + j o i S m z C K E E G y 6 B j 7 a m Y p W l U + 0 h r 5 t h U 4 N 2 M y L 4 G R y 4 X E a f y f a q S h R A c r A F
a Y c h X v f i Q 4 V 2 l d 5 7 / P 6 X U a K n 4 z n 9 F x z R b / b 1 y 2 Z 0 q C E m B I 1 n 0 s S t a P i a Y X f b I b t 9
N t w W B 7 p F v d w w z 8 4 Q x D e z E K f M 3 B R F 4 P 0 0 v E y Y q r a F t D U c h L i 4 j j 1 C y k / T p l 6 L 1 t e Y
q 9 5 n w 4 K k / b Y 6 R c e / c R z w J K B l f / 3 3 h w 0 A 7 a B x o n n t x l 1 q s I u 5 M K a o i 7 x h g Q P 7 3 C 9 /
x Q j l U s K I I Q x w 9 u 8 G 8 I 0 B h W 0 A G F F R h f o Y I j w X Y D 8 V K c d z s t 0 s C R P M Z i N U s K + E l S 3 8
N q C o 9 + 0 9 N Z v y P F 6 u B E r Z M P / 5 C c X 3 r 6 o w S f c S k 0 Z X F v b Q A U Z M y B n y G o r Q 8 M S 4 A Q / S
9 R w N D 4 a A s n s M e N I W X T a v N D C H I a e z 5 H s i G w h p p q Y 9 h 2 e C W e g f r e R e 0 d i P 8 5 + x o 5 r o
+ 7 K L U I 0 m W 8 B 6 z P 5 T 2 V S d F Y Q b g 8 0 j I 4 s R K a 0 E H W g 1 e F l r K 3 X X 0 y 8 + v 5 u 5 R U V 8 P c l c
C / 6 o 5 C o 4 V E o g a Y 5 m h i m i z v F 7 u 0 w V 7 l K N K G Q U v B q s b X e 4 M j B j 8 7 p e c P N K p 7 J 9 M k e W
r b G 8 T q k 8 Z x F G e u 3 W p 5 W A z I Y V 6 8 8 t w 4 r Z 0 B / j Q M s v j W / u u e V X N A 4 t y L M f Y u E F r D j m
4 + 1 N T W / y n v i 0 9 Z t o c 5 r A T j 2 9 m f q S X 6 p I m P / C e L 3 o S n M V S S + S f Y O W T / p 4 t K Y c / E D
y d K y U h r 3 f H 7 Y s n C + m 0 x p x i H 0 7 V 8 V 0 p 5 M P 2 + f q 2 4 m M c o 3 0 1 a Z q H b o H m + c C 4 i 3 0 q N J
t 0 y v x C D F t 7 U T g E J 4 F E f q 1 A I p N t A 1 X t X T 5 v L S n B k X 2 U 0 q j L 5 F k h w E P H e 6 W q w 1 l 6 7 B
x 8 u z V R u 0 s C S g L p o 9 L j g p 5 6 l y 2 v E r 7 g D S W g q I i t 0 c V i W x Z l U c 0 z z a V r D W t D D f m X Y F
s t p j I H k 4 B s J G w o q J N 8 G f 9 I G V 6 P i 6 D l p U t i f B c D E p C o B t 7 w k M U C H p / B j q 5 l E s T t Z A
8 6 y R q N O Z K L u y W 7 t q D f O P Y Q U s U p b A M 4 E 8 h r N 8 4 E D g L Y M C g 6 A C / Q s 3 H / w D 0 7 c J 4 L C k
M 5 H p h 0 6 h i y e h a n u M c t U V y v y f S b 1 h W Y 5 L E L y r 9 U K L Y H X M d C R m 6 S I 4 l h k c D / y d 7 Y R c
8 x X J w F V S B S X c u R F Q D 8 V i G o 8 4 H N N w 4 5 0 a / k c T 0 t f J L N D k 2 p s D g M I C j W k i Z D c 0 J 0 f F
E x X 0 6 5 S C D a V S K 2 a 2 h S c u h L b 4 o 8 7 n k H P T t m C w s e 9 2 g Y Q l g E J q h A U C e 4 t u p S 3 T l c e d
r Y x 5 p 0 T R q 0 a 4 s a x y Q w 3 K 0 k v C Y b 0 0 v r 3 e 5 y w j + I 7 F J m d T / 3 F R e p X H A d J g e y m S m e l h
M U n Q V v R e t U v + t b s H k 9 6 D X j M H U f v C A r W c j f 4 N f u w e E u d 6 J A t m I x Z h m B F T l g / j + o B 7
L 3 + n u n A 6 / d D r I l B N C C Q / W W W 3 S T p A h F C 7 j B C z I Z M J M w y P 7 t R k 6 K L + P p t f M M W D 2 r J y
Q p F x w N D V C K 0 c a + J C u h J 3 l h l f j r e x P J K D 5 / h h q G d K q c 8 =

```

C.3.11.1. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="signed-data"

```

```

M I I R / g Y J K o Z I h v c N A Q c C o I I R 7 z C C E e s C A Q E x D T A L B g l g h k g B Z Q M E A g E w g g g n B g k q
h k i G 9 w 0 B B w G g g g g Y B I I I F E 1 J T U U t V m V y c 2 l v b j o g M S 4 w D Q p T d W J q Z W N 0 0 i B z b W l t
Z S 1 z a W d u Z W Q t Z W 5 j L W N v b X B s Z X g t a H A t c 2 h 5 D Q p N Z X N z Y W d l L U l E 0 i A 8 c 2 1 p b W U t
c 2 l n b m V k L W V u Y y 1 j b 2 1 w b G V 4 L W h w L X N o e U B l e G F t c G x l P g 0 K R n J v b T o g Q W x p Y 2 U g
P G F s a W N l Q H N t a W 1 l M v 4 Y W 1 w b G U + D Q p U b z o g Q m 9 i I D x i b 2 J A c 2 1 p b W U u Z X h h b X B s
Z T 4 N C k R h d G U 6 I F N h d C w g M j A g R m V i I D I w M j E g M T I 6 M T I 6 M D I g L T A 1 M D A N C l V z Z X I t
Q W d l b n Q 6 I F N h b X B s Z S B N V U E g V m V y c 2 l v b i A x L j A N C k h Q L U 9 1 d G V y 0 i B T d W J q Z W N 0
0 i B b L i 4 u X Q 0 K S F a t T 3 V 0 Z X I 6 I E 1 l c 3 N h Z 2 U t S U Q 6 I D x z b W l t Z S 1 z a W d u Z W Q t Z W 5 j
L W N v b X B s Z X g t a H A t c 2 h 5 Q G V 4 Y W 1 w b G U + D Q p I U C 1 P d X R l c j o g R n J v b T o g Y W x p Y 2 V A
c 2 1 p b W U u Z X h h b X B s Z Q 0 K S F a t T 3 V 0 Z X I 6 I F R v 0 i B i b 2 J A c 2 1 p b W U u Z X h h b X B s Z Q 0 K
S F a t T 3 V 0 Z X I 6 I E R h d G U 6 I F N h d C w g M j A g R m V i I D I w M j E g M T c 6 M T I 6 M D I g K z A w M D A N
C k h Q L U 9 1 d G V y 0 i B V c 2 V y L U F n Z W 5 0 0 i B T Y W 1 w b G U g T V V B I F Z l c n N p b 2 4 g M S 4 w D Q p D
b 2 5 0 Z W 5 0 L V R 5 c G U 6 I G 1 1 b H R p c G F y d C 9 t a X h l Z D s g Y m 9 1 b m R h c n k 9 I j F m Y S I 7 I G h w
P S J j a X B o Z X I i D Q o N C i 0 t M W Z h D Q p N S U 1 F L V Z l c n N p b 2 4 6 I D E u M A 0 K Q 2 9 u d G V u d C 1 U
e X B l 0 i B t d W x 0 a X B h c n Q v Y W x 0 Z X J u Y X R p d m U 7 I G J v d W 5 k Y X J 5 P S I 2 M D E i D Q o N C i 0 t
N j A x D Q p D b 2 5 0 Z W 5 0 L V R 5 c G U 6 I H R l e H Q v c G x h a W 4 7 I G N o Y X J z Z X Q 9 I n V z L W F z Y 2 l p
I g 0 K T U l N R S 1 W Z X J z a W 9 u 0 i A x L j A N C k N v b n R l b n Q t V H J h b n N m Z X I t R W 5 j b 2 R p b m c 6

```

IDdiaXQNCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbnMtY29tcGxleC1o
cC1zaHkNCm1lc3NhZ2UuDQoNC1RoaxMgaXMGySBzaWduZWQtYW5kLWVuY3J5cHRl
ZCBTL01JTUuBvWVzc2FnZSB1c2luZyBQs0NTIzcnNCmVudmVsb3B1ZERhdGEgYXJv
dW5kIHNPZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQvYWx0
ZXJuYXRpdmgWVzc2FnZSB3aXR0IGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFj
aG1lbnQuIE10IHVzZXMGdGh1IEh1YWRLciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9t
IHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX3NoeSBIZWFkZXIgcQ29uZmlkZW50aWFs
aXR5IFBvbG1jeS4NCg0KLS0gdQpBbG1jZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0K
LS02MDENCKNbnRlbnQtVHlwZTogdGV4dC9odG1s0yBjaGFyc2V0PSJ1cy1hc2Np
aSINCK1JTUUtVmVyc2lvbjoMS4wDQpDb250ZW50LVRYYW5zMmVYLUVuY29kaW5n
Oia3Ym10DQoNCjxodG1sPjxoZWFKPjxoaxRrSZT48L3RpdGx1PjwvaGVhZD48Ym9k
eT4NCjxwPlRoaxMgaXMGdGh1DQo8Yj5zbWltZS1zaWduZWQtZW5jLWNvbXBsZXgt
aHAtc2h5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGlEgc2lbnmVklWFu
ZC1lbnNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUETDUyM3DQp1bnZlbg9w
ZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGh1IHBheWxvYWQgaXMGYQ0KbXVs
dG1wYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxbpbmUgaW1hZ2Uv
cG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBIZWFkZXIgcUUhJvdGVjdGlvbiBz
Y2hlbWUgZnJvbSB0aGUgZHIhZnQNCndpdGggdGh1IGhjcF9zaHkgSGVhZGVyIENv
bmZpZGVudG1hbG10eSBQb2xpY3kuPC9wPg0KPHA+PHR0Pi0tIDxicie8+QWxpY2U8
YnIvPmFsaWNlQHNtaW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZHK+PC9odG1sPg0K
LS02MDEtLQ0KDQotLTFmYQ0KQ29udGVudC1UeXB10iBpbWFnZS9wbmcNCkNbnRl
bnQtVHJhbnNmZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdGlv
bjogaW5saW5lDQoNCm1WQk9SdzBLR2dvQUBQU5TVWVhFVWdBQUBQUFBUFBQUFBQ0FZ
QUBQ05pUjB0QUBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3MzluTzNucFJ3MjBk
cXB1ZkFSUUVqT3l3aXZzbkN0a0RLbmJjTGS2NnXbFQrenQ5Y2lka0UrNkt3a1oN
CnNncnmpY3FwTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWbZ1RQUm1jaWhBZjVZ
SnJ3N3ZqdjBaV1JXTS91bGkNCnZkUGYxUVoya0RE0XhwcGQ4d0FBQUFCslJVNuvy
a0pnZ2c9PQ0KDQotLTFmYS0tDQggggemMIIDzzCCAregAwIBAgITDy0lvRE5l0r0
QlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEWRJRVRGMREwDwYD
VQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTvBTIFJTQSDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eTAqFw0xOTExMjU0MThaGA8yMDUyMDkyNzA2NTQx
OFowOzENMAsGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxZzAVBgNVBAMT
DkFsaWNlIEExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mpUp+ovBou0P6AFQJ+Rpw0DxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB
8g0UH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5
R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJan
Z/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmswqS6oQcAx3Weag0yCNj1V9V9
yu/3DjcybwW2lJf5NbMHbM1LY4X5chwFNEbkN6hQury/zxnlsukgn+fHbqvwDhJL
AgFpW/jA/EB/WI+whUpqtQIDAQAB04GvMIGSMawGA1UdEwEB/wQMAAwFwYDVR0g
BBAwDjAMBgpghkgBZQMCAATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1w
bGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUGMB0GA1UdDgQW
BBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2
GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAU14oJyxMpwWpAy10vK6NEbM1lgD
5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfxf7fSIus8gWVY3WqMeuOA7IizkBD+GD
Eu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8
uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR1E5K
9JiQaJYOnUmGpFb8PPwDR6chMZeegSQAW++0IKqHrg/WEh4yiuPfqaAvX2hZkPpi
vNJYdTPUXTS07K459CyqbqG+sN0o2kc1nTX185RHNrVKQK+L0YWY1Q+hWDCCA88w
ggK3oAMCAQICEZdBBXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTEN
MAsGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBs
ZSBMQU1QUyBSU0EGQ2VydG1maWNhdGlvbiBBdXRob3JpdHkwIBcNMtkxMTIwMDY1
NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAst
CExBTVBTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFjZTCCASiWdQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6
WWyTgBK9LC0wI2juwdRrjFBSXkk7pWpjXwsA3A5G0tz0PfpgyC70xsVcF7q4WHWZ
WleYXFKlQHJD73nQwXP968+A/3rBX7Ph00DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CR
Q/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH16syTjGsgkLcLNaU5LZDQUdsGV+SAo3
nBdWCRVY+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0

```

nsG1llyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAa0BrzCBrdAM
BgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAEgNVHREEFzAV
gRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGWAdBgNVHQ4EFgQUu/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0j
BBgwFoAUKTC0fAcXDKfxCSHlNhpNHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0J
oJanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnN
v0Fb8lV1iffRtF/KtmVEDMR/sYeqAH83KM5p3e12lVh40HhyI0qNuz5oShNaACSi
oQ23WxHGvy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXmT9cG6jbMvcdH4
z0IOvg6mrYkKTM/RCGnumghxwYToj10yD5Gs4D2IJCw+fX50Dxh52MbNRYXTus2Z
PRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H
4ConlB8f7R7s1LM2cSYxggIAMiIB/AIBATBsmFUxDtALBgNVBAoTBE1FVEYxETAP
BgNVBAstCExBTVBTIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFNUFMgU1NBIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+Gr0mqnXMAsgCWCGSAFl
AwQCAABpMBGqGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8X
DTIxMDIyMDE3MTIwMl0wLWYJKoZIhvcNAQkEMSIEI0k6rjm9vW4yAFhPqraTwTSM
poDXdAk+kSVCc47Smx1DMA0GCSqGSIb3DQEBAQUABIIBAAURi5ooUyIh9YruNpF
Se6sDsPTGmIcZsDjQ/MZV55S4pmhVBQu4SoVZDVM9KHKxqfBbj+aTs1Cyas8R88h
cWqd8xhiU9ufoC7p6qEMVIyMvyppeupRyjQWUCH+2XtQ5sAVmr+F+1/Valuj7JZw
JU8XS84oinCF6uApu7eucGblt8t7ek7j3JXoFVE7g8a/01JKg4ezNV2RduQeNXLt
m/lBVIfeii0smgmJa5RTgbgAakJtdo3odHj0cI31eANSbQ1E3XENz2E9L8JWxYNP
bBceEhIvu2A0tV2PYCBfrVp0WTVVWHorm8GG/DyvsAsa6eGJI55hA8VeBg170gt5
nzc=

```

C.3.11.2. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy
Message-ID: <smime-signed-enc-complex-hp-shy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:12:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:12:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="1fa"; hp="cipher"

--1fa
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="601"

--601
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-shy
message.

```

```

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

--
Alice
alice@smime.example
--601
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-shy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--601--

--1fa
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGGoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAAcELEQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--1fa--

```

C.3.12. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 10920 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 7072 bytes
    ↓ (unwraps to)
    └─ multipart/mixed 2519 bytes
      └─ multipart/alternative 1597 bytes
        └─ text/plain 564 bytes
          └─ text/html 736 bytes
            └─ image/png inline 236 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:13:02 +0000
User-Agent: Sample MUA Version 1.0

MIIffAYJKoZIhvcNAQcDoIIIfbTCCH2kCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBTFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFGU1NBIEENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCsGSIb3DQEBAQUABIIBACgBnn7CPutWy0itfe5dCraPLDXBE+WvvHIX
EhTzjfwj80y666bZWDo8VCR86IK1U13/OR6f1a/FyLJ04yLW+1Zn7WVxxS8PKGrO
oaE56/oJxgqRRL3qnY01rMIhqqFrG2DNh6rjRnd03witWba76ifzdWdCz3JRCsrC
3hlh5SMSLYH500TDFEJ9tGDGmxFZ5+x4FJ6D+1J70LRo64rtPHthyu05N1NXPBXU
NIxSVFQ4f8j5AS7Z8oo/79IoX1wU1v7IEkq0mfrx8sXrcqZbkmw9bPRGZrWRZLDf
7EYCC0IF+sn6USXf6nd6G1vRAgWaUd1kiZChjVRwgo5SRsAk9nUwggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECXMITEFNUFGV0cxMTAvBgNVBAMTKFNh
bXBzZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAF0KeyT8lWzqPQF4leLhR0RAI
pTb21ahiLRjfx4mWuotY32k8fCLESEmH5bHrjdt5FNI/jLC3t9bAtFMEkz7VPZ+
Fgj1BT4Bteuw4g8miNcIU+xu7g13n8H1kTx00kAmGPZg/m0BYJZYUFXSQB10Gja
slGNtLS0Km11f/u13p0CLRV0+nasldZxm7Rt7Zd0Uis0PDZfMeVWTS8s8l9ifpJA
YGRJpKwzty4BUMvxbgUBzySofIH0pc/DlcFIB+s/S0Dgc7xAU8CxU7xvo36dicgK
qm6TqyYQDvBBXfnc8MWfVmE64sWISQ+nWJIPvTzXh4pZ0FgjKhNUd0YEV1Zz8jCC
HE4GCSqGSIb3DQEHAQAdBgglghkgBZQMEAAQIEEMVrSF0MP06N601pRZNHTXmAgHWg
JGppsM+z42CDVWr/cZdmJAF0qTh58Yba5feUkkVha+SVHfhjgaW4v27XT3kKnraH
7tkFwxRvPa/qSYKSgCS8LZeHEj0mh6HX7mJjbWIEogBw9CH7kUUsq+YDmZ4ReE
+teYWio5HaP6aXoiy8qSyu2kbzz/EmIUxEIHwDGtbZ4f8Hqpo9/j2cXR59xGspg8
0u588sbXipWzBv1gxN24aRgpBov4818XHqW9JzLozz0G0bZwdGMwZeKrtSPjtE5K
Qt2Gonk30Ri3LmLPVHQ8TKv7ZeEUw3mY/95noB2rDvIfm3sX/bBIWTttWj2pnzQv
dWl8byZ0otx1QjJcaLbmL1Vxd2U6Lo5RNsYHL+Bsf0E6roSBwk7UacD0tR/tiMKQ
aDe0sQARmHC8+0GV7uKV0p6puZT1RGEkVLW9Pz3MvHYfVQCn7UU4HWz3vjUoCCFn
KRj6CG7xKUHAdQDTmtfKf1F6t3ba7Q3sGi2Lw7FH2RG9u8S00RUQvYTxWo0okb1Q
H163f7DLzIgyii0aZmtrS0E1rHKhs3utQuYqvBtR7fvUWFC4GtqXTETThwYF84YL
iVvYhVQp5TWF7uxxJUyW8cgYqAjNnqi4Iif+LXDtrbf97fP7cAmcE3rNxvDn771Y
Z2e+Khh/FgaMEFRzNN8P9itpd87YGY+mwde3bBw3fdzVInel1gFaxplGebabqpup
rko9Epu+i891NSkwnKYMDqb3azOUW70zGbW0w2Fvn5VcD0FK/eTVLwpn6WHhg7z1
x2yZHQ7QMUCtKiAv78kjLuumezciX3Df4KUjYidPFF11LI91tmZAn6ex09vtq55n
W9A5fzn0bqeN/xhBv47IwaHTYozgbCY1SoqNqSmpqax+WG1Eiv09b7w4jn+yxFkb
smZ+WJJoMzJpvUCfZ5QeE6bVZhoFMPsDWa4UzzWhiwxFr21j5guaWqJduQgv3qHE

```

qF82ovG4Q4gR35gGHebJ6dxV5FOWD/3Z53ZrYMZUZxdwW+bWr504UgFH0A7ngvau
vHgOyTnnxvRzvKSkhr3uRItr8jM4+y0a18HLU0mi0+/L45xJJwf8A8GKL0BCNabG
giTHu+/5KYG3j6foE8mf4x1UAVG1dXP6QfEXZG1mFV02/w4vGJTz0tOrYSPJ3bXF
+HahaZ0S7KXpN69rRqyFchtTC1Vbm7b75q37+lzLHisVebzvco92TyClaoKoolfZ
sifJRf8KudETwNkNGFIj3oDmmSURJ+0YiB3h7zJWGiVGiNd9UBX0m63/7SpTiaYZ
e0UbCM+nQ5/SFTg4gqjQ2PPH7QSo0zioilMyos0AwWQ3E9ThEhKLzoaGzPx/dLri
HL1ZBjjdtGC1lSCFcjdYLC7sP3W2nbnyBMG6dqvwakWGlaAuXPZ1y115jn7yJqPL
Pnp/eVU+9S1UfuqBfZQBvWPhIUyG1KL23HzV0b1IsKqbi1sjxo7DL4RrC1axRFu
E5gKB1VaUCiDkZhiKj6vPQetaCD3bTi6Zr/xj8rH6G0Rr8aWI3HIVgFtwrtuAxx
D0YN114Zm2K26c5FcrTVXh1XCpbRCjj0RqqsVUX3onamxH0nEdxSK0begqfBQwjA
rn8jWS07jm40wmpieJg2Szi43g9C31jwMps0Eu1zAg67/00n/ft/+75/y6j11Sb2
thJp6L2z0VTMJDNbI75P0hY1NPoqHWIZOV9P10L0nH6hcUg5zt8JvXBeoxQdMcjG
uY9ly1w+gLMuFA7KdM0/sEH7GM20wpIEU5gqzoDresGUCE9gAC8kz/M5Q0w4d0mW
t85JlsTwmUbbYgCwjZiDT2Gb6MrNUa14X10bsP02hccuuvEvLt9bBgYywVJcR0
uE7snAIXXHEXodMkwAxwhSlQLcBjDSVUQm2C8+lvhw1W662ogb4yFJNJC0H7c+9k
qTP2jJTSyMxG5ibmzF+apc7u3eL5/OU/prUmnZJA1r8DkfB1opYx/sCBQqJMjYIJ
/ixMshyqcNUGCD0D4+qibWS1vbUQ3XZ0mdN3qIUdvwzgp7YpX1MEUYnb39k4pe18
fH8fwkSpK3j2qJQ6mLPMFRRIL0zi0nk0EtFa80UQgG0LpZKH2+Hqiyr7Zmpar100
Wc3D/M0Kksp44y5hYt3Hexnz6t+fuUedb4N6V43KjFK+DAuU3SZZ170B8vPRQNft
s4x/AYMAcsqGieTau1uVenqwUBoHgm8IRfgGcAwn02Xfk9S1UXS/iFmKC17dEfsH
OrIvM1d4R/+a220epCUGecmr5653LtM0oQM3Tupdit58Rxx43pg3K0vzTKygJ4JW
02qBuNtc+B+1lkKoilnQ1YJIqk6Fh7m0E31qo2isdLBd0niDp3vfQDBiFlTBHI/C
e/5rUmwND2ub3pd006cy79GrEUSdSedhcin6ulsrX0NhBr7FtK8o05IyNVFVHI27
QSi05TNK11lvY7hWqCVIIu0VYwEvuaEI/T0Mok7Pf7yUnJN0Q04t8co2BT7TiH/8
NcyZtmGJaf35R8s8YMLnbg7LUB9wqo1V6EPnLfCkt8M8fcnp0lnQ8+Ynpavvz81h
wd4v49C0f5512ptCgdg5YZR/Q9v+T0c+fdeaF3jhr7/vV/D4NNN8Lsth0DqQ6Ac5
kzz4RbsLLXbK9ZELjgjjyIB0Uome5ytjDSuApeqWgEo28DsTJ0vIECRZg25ZhKeW
cN8uuKI6WezjxeIRM7ZmDN3wvd3amj0SDvK5ASsla03CyGWPZ3RJ0SknCRCo90xm
aSn9zuHGD1ZtYL8P5kfTNmhCq14ktAdH23Lhjqr5FNbhEGi9rxT8CsXUweaqRuK
KeX3UdW0iLBTpcncaaN/3knX8EYdy0vNhQsqBtqu6gZhQTIzB8QiydFvf8ztCDgb
5IfeDoZUru8HzhMXm2+C0xqMC+FKoFjVc+2s81MIrhpMnFXL5M9iPnUKL6f21q9m
c4KjLQdP20Btgeq0WKpD0s9ZWTHyb4wWNZhbKq8AQ12MkThrHymiA2n9EaV076sh
ceQwORLinfQVbkqja+tN0u2jDfKvrbI21h93kvK9ZLP/c1IEt3f7u3J4KgCr95kQ
SBN1SCpZALiazPSWB4Cbr0PKFU+mozln8IvBoYJWryoc4pbX162AFd7dUzXYOW0m
41nXvsg2jKtor6j/CUIeIog+GrPlkfuesFKihydC6oCEjpGI68qU+JG8AhM4ZCvx
4VfB75yJHJ7ch2hytw/UE7K6Vjz81EaxS2LZ1DqiHoBo58QwgPbmmYUU/Mf5P1PH
ybr1KTSeNyFT1Mky+GmpcN5tX5aY+qeLQ7mu6rfYLVk8wA0aoc3N0sRG0+8eigan
01Jq4QeBmRbo5SDbe8PuRqGuGtCi1sU4vXbKBvBJt0DUZ+u7cTKHdZ20s08/JLVv
Ys+SYp60SwngI+E0c85X0kREcp011Qymx0iJT7u1UJHISB9P/NFoA6ovCYBZyRQ
SfdYEkvW+0KpVsBLVdYEouJteWd1Utc6Hi96Ej60S+WtFyV4YUE8MtDzLk1buy6E
YIOFJiowAWYFVwNVw6JPMF0yoHdk4FIj/LEChCLKNUgLOiABgkYOBpSnxov+Ur9N
0V7FQtTJ6/d4szAWZbApUeFqX1iOb/py9E1/DOTGy6oLUnL/iGVfTf+Ajj5+emCh
44Ahob2UH70VQ0HrMT2GDMizGvgzSPnMk22PAYcePvREiu4wJk2tue48CXUkVhKQ
147MUmbKnC6gDnyjsQLB7WZ7PkizbmGC3d6vS4N3CcopEyDK7zBaWppewVagIKd4
q0Mn6Y9iKm0y97Doc/y8VADYTN/EDQvj14j8Sg8I95cx1VInn46YDvH6HZH2zJGh
4xUC31Af0rBVe/v50QEHDcCjFZKa72vc4ieANqQPX4G2j0TegJG8JzxLnHifud79
d+OPxcxM8U1w28ybRNWkP+TiDZZQ6L6lCib82fyMcXxeUiGRYRAHSNOQYzblDBfH
Z1H7gmFaWfJAa5XJtJSpJHEstbiWVOrEOY/kNEBkmdEP54uT/bcxkiQs/f89Cff
K9ShqAb7GEmdQMlnv6rf3dTiG8GGBsztaZAx4/LK5IeoYQUTSrKGFgah0qsQ09I
TaESQK44gRjCe5F9PXjpPK5zpZA0Ti0yBJDPA1h+v2zNj5Pk1N3V4V02oWCwG8vx
XwaF5YE3dKcS6BVMnx31ARxKtp4MIZRXpgma6qeIL5DrAXDOLMoTqZA3fiNuuM
Vn/LIEQxpbxhGpzVi3jcdCthvzdVWpp1+vfg58ydingch1PuWNfkkA0oEt55ub78I
AGQRhm/QMGYkeXOWrZelfpIKGUft/WkmhMPP104sRaJLjRIo+1KXV39TYrlegf/s
2Js4HRz4IIdWufUQHdt0mQkNKnssMIVI30LloLi/0R+hPv1sAc7XshfPzqbIXXd5
ThQXoiSsPBVTy4yHi5d+0LLsx3zfSA+Xq4XRF7bxq4xoaDKBY0CoZe2qVi35Hz5i
sPb2AHT9qHZE63YZ55+pCmH5kiVsgrlj0pQo8QUzYjCbGq6X0w60SbBUHmf0//0
aHB++zb7IsnYHNeEJFCiRCJxYAcHTVWC2RLyfxJz6tx6GidcnhgDMqw/h5Du4X+q
3WTRxMfFJVNjHkHiD9JsNUNQ1liu+I6LREW27IHaxJ3urfJggpEv7nNZKoQ2Fwnk

HinnC1Wc1ZXZBoXpos6zQkmBbx009ciJKPvfU5vhkjg02Ja7eMnvaGem3xw6ubLa
dMCW8zT+Y7l0AY3L5jfw6B4wKt55c0nJELUDrnLqR6ITI+b4Nq8+MuPPGkvXIosV
umZ6sg0MWPQfoGgR0i0F80QHkHylMA9L8cTXiC4B6lei5GvTHfoad+70IzD6ygzP
4ITgaeSC57pB+3ZNrjNn1T2iEL1XZZb4sqwxwDf7mw5FdcI3R2VNGH2Hu4krCWqd
4yx5laRk45ChF9Ygd7VexK7ELSRAd/Q3AvkFAyJ6oL8Isy3AqruaGzvLPoQQGrTv
uT8DajA0tfV8r6EHf/im61DwtK2ccGuBoP3qYXJ3uLqGQRyXW5KrPEeq2UxlbSra
nDGYPQ7+0BB2dg4exQ6ewCBAs6HaX3fHsAKJc0FCf49LC1N7yu7ARvXZ/yUaGaHq
irEWffl4IC0FvYzMv5MYPczJA+c8G+vJZa3qeBm3ZAZWFMZ0zdkjz9joE40x8syE
7ME2a9uBwneLHTx0GG0RZsrL4NFxt5wCG09nj43civVgBLwbjsya0i0/RH+671fV
jmsvZ1M6i9LzhPuvDKe7Htvv6/wJGqBSAsY3PFoEMKQ7n7+Jb9Vk+2906Ivi5+Zp
SVwmHH7KL7Z7/73U5PSjmuGtyPlvQT7RRr9kqk7BbvEbdpyIGHLrMPTf02hIDc26
BsuVz0pDrY0AsUHViaEZWugmWfF5Dub5osg7S+lZEaZG1nr9jn7ZkFyBynC9eci
qQeh17PBaSPLEBAFgvsfoH5ynBiJMLnuWw9Mmw/G+mw2RMEeV4wMJqylB5mP2hr0
0D32KWcDtxx8NPHULbFtiAZ067raGGWkWYI3iIeBYpqCSJo0bFxcch1CfK8VR/WH
YDFwItvBvQ5k/ntvniCeh1JaP2Uwe1VV6mafH7qrmXmvqtq2QEFVbVB+aBnRK2K0
uFKbXka+PbZ1b7311HxAz+xsEAe1UXlnKi+aASl+Qn+pS3YKyuH0zg19p0AmCf1t
50hS7j+0DBgHYFAjNfLb71Jy30MceP7gkj6gW1vHMKHRSHVOC0KlbMyQ8JAgMJUj
8yf09qgbXWZMxyFxFjvHX5CyJ0KHA1JfQNF1y13M158jUHUqP9Ys2gDMPJv6xTsq
T1tvxFLT0Ii007WsU0yV4LCGi+wnrUK5dbhfV6FhdZKNpfFnpwdeLak/2ccMMm
0SZ7WBFFKHBmmWMfozq53590gGE3sf7/C45x/9SDiIsfWQZusA25XiJ0nrJxwoho
5mN97+DUx5nhbKzD/ajTg43kSlDRJFvtbDHC2nYaIl6SLXg6HwhCk6qnAnb4FxaU
3M9M5XZuDwXQ0Z21yjh4Yckfi69GU06qK3Dgc9wugvmz2WI61T5oE20d/4HdTf9e
LNEWzR67qvyUy6tILZi9R3LdAN3HukfmJJXCbaIOUftQQUGRgCEdM5NbSp3UhTZ0
3trXdXa0lifRJ5VfsJmGUiaZqD+yi/p+sYuWRDMu/sSPaSCBf700txsLRrScJ4+B
yqg+AOUxxWYCH/A7kaQ5BxyyJ/HxRRH7K1JRTxTxZChuad721D84Y700FjaRAx5G
yug48Ls6jJugo48ce0zVZKDQYW6cAoufc+zx4BLZobqoIjGn2vu+9pIvED6+Bud1
p4wsgVS0fM2ZktBIM39RDeDb+90NxvKw+V09Gdo2XmcMQtig2oTMLkUbNbiPC50r
diokCwEwSAM/+uXU280GhFo8zHwIMpcfzs88kKHCInrTqS0mNFnxM1bGydDdtMqX
Mz0c57+8uCrQvFAa9yXcY+dCIxMNj5951ldBMXCVzUaJF3ITCJ0Juk0ZJE784+A
e+MSqOBm1GPHya7f7wnAnEz3d1qZ5yFgBV0B4kcXpAaW51gt9xWk8TZ0K+o/+R5S
4VR+wb7cQnYHQNVbMrPCF93Btqw0d9fFDkmvjxAfG8IyPMYUezfSRqhH0qU/K4Y4
fbggbxq1520vax+foW/nQNKFL7Bj4GqLKLdS0ChQxT1YnwEuQ0cI2oQ8zzo9fFC
AiDYruczd8dA7mPuC4FQRcQjNXp7fzi2GKE8rN1aC6/EsZGFZujmVq48+yMQ6Ufv
byymZlAhAbFXNJlQjQ98rkyjooQr1QIjHpFn6wH60fSt+1ncOVL1DMRM+8KpPp9+
U+khHu2wKDtFo0hw1+1seImM0cuIXGLfBQ3fTlPl9p9PcN/Db+eMuPjXv1i/jPyf
z3m8EIOg1YqsSX9IulrvH60hslS5FLSvxG+t+9U1pytiijH8M1UHUCYRd5++yZ+
VwS3SlyGFryw4u1vH1CT3rUbYpxbVkk0aW0e1HFbJST6WvSkB40dxYmha2HK4mKb
a0c7QFDwDveew0f0aEXiLVysKhSZusmsIvS5l/oAZDdeC+qmeEH9yctRIJS3910E
Dki0HpM1QEuc/abzIjx3/KmKMhMVKfbVvpzuwByvXkIv0Y/enWILBWxQWLzpid
h1AzKiewpDZesdXXCw2pRgafPZRrjuAwInpakuU6AuU9TmhHeWgRD90tpleyI5Xs
VimKL81rcuCBve5dXtziFZ0Yj1TfG5VzWaiSX7taj15tvlhSiCmQN9Yz8Cus0fP9
r2kDAroyIts20mukqRYoavOC3vZVp30vUaxnPcRw7o+0s0pbCWRQen7PVtT75vz0
7YZLrXN2fBhzx5kxnbPD8Ucv5t9ixepy0/pSyztdeljHfyTCT9twNeoDKfqqzJ/Mx
HWy3Az1NpSuT4Brqjsja7D1QJenDuCqcMsz6xVL1DM4w+JS5TMi0ejWuIu5Ck9ey
2QIQMqEdYmIRyC0zevw260WsbCdwPMmYInUwoTFifcvTC+JLZvfFp7LgzKa6XCik
dM16z6k0VZKKTjUfJewBdG6ezIecOQZdKlYcjSPy8R1uEPvqc94MTJ5uTdbh5sum
EYIkT6h6DHWjfbJoCTYpbFavprnqXmOPVvoTcifkUemh3s0u9H1l00a8wtIAZp13
gVqQXS1ErzfF6Sy4UKSqAu8liM2WUSZH4bmW36sEBEOykXh//19wqHW17nqGHrgG
AVMmRB42waFaTLysx/yNwyrnpNFIrQoRKi9DgffvDCu94Q/4YfWojNgcooYC5SAR
lSLt6sjIWSp6neP603RDOXq910mbrM6dF9JAL3BAUK0Pn5/+zaaVva5IWyaL9KsH
2mJBvC+Wik40v9k+n91H0c1eIkJZDCHveqfM/FEafdhD7teusBcvxDPhZVQ810mH
phcUd3u0GEZC4L0fEYar1A9B0KEYslCodnDC2cKT3quqtWvhweJ9VttZQgGN0n6w
GLE0sBP4x1pQ5apaSKJa3kVl+Gq+zZs7A+tsl3Z2B1kJ3quYpBkW7/39KTWPniA/
Sx++STetToLGYA7UuVndESoTbHMgjGbS0n94taPNmqejT5aSL/v4SKw3nUGnIeb4
kbuS7CHdTP7cNpo3DC8X2xprJJ3ffZIPH1HvIqjTA27lgs62676XJSG7BIgIrBiy
g6jWth5X+zG2dRcjTafyPSzW+jf1U+cVF1vW2/cZKz//ku7W/1NOumjvJGbuBjif
1m5R2PkjvwAYiDjvV8QmD46Xyh9lium01YYpUKZahTC+K7w3qs9gWweP+aUYOL8Q
0x7RFcCmWKvm6+u2S0fctuYwD9e57R+q555PanLTReyS6FaHddqpvuoxrkPUBT+

Y3Rpb24gc2NoZW1lIGZyb20gdGh1IGRyYWZ0DQp3aXR0IHRoZSB0Y3Bfc2h5IEh1
YWR1ciBDb25maWR1bnRpYXpdHkgUG9saWN5IHdpdGggYSAiTGvNvYWN5DQpEaXNw
bGF5IiBwYXJ0Lg0KDQotLSANckFsaWNlDQphbGljZUBzbWltZS5leGFtcGx1DQot
LTU4Mg0KTU1NRS1WZXJzaW9uOiaXljANCKNvbnRlbnQtVHJhbnNmZXItRW5jb2Rp
bmc6IDdiaXQNCkNvbnRlbnQtVHlwZTogdGV4dC9odG1s0yBjaGFyc2V0PSJ1cy1h
c2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNCjxodG1sPjxoZWFKPjx0
aXRSTZ48L3RpdGx1PjwvaGVhZD48Ym9keT4NCjxkaXYgY2xhc3M9ImhlYWRLci1w
cm90ZWNoaW9uLWx1Z2FjeS1kaXNwbGF5Ij4NCjxwcmU+DQpTdWJqZWNo0iBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtc2h5LWx1Z2FjeQ0KRnJvbTogQWxpY2Ug
Jmx0Q2FsaWNlQHNTaW11LmV4YW1wbGUmZ3Q7DQpUbzogQm9iICZsdDtib2JAc21p
bWUuZXhhbXBsZSZndDsNCKRhGU6IFNhdCwgMjAgRmViIDIwMjE6MTI6MTI6MDI6I
LTA1MDANCjwvcHJlPg0KPC9kaXY+PHA+VGhpcyBpcyB0aGUNCjxiPnNtaW11LXNp
Z251ZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5PC9iPg0KbWVzc2FnZS48L3A+
DQo8cD5UaGlzIGlzIGEgc2lnbmVklWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3Nh
Z2UgdXNpbmcgUETDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRh
LiAgVGhlIHhheWxvYWQgaXMgYQ0KbXVsdG1wYXJ0L2FsdGVybmF0aXZlIG1lc3Nh
Z2Ugd2l0aCBhbiBpbmxbpUgaW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2Vz
IHRoZSBIZWFKZXIgaHJvdGVjdGlvbiBzY2h1bWUgZnJvbSB0aGUgZlJhZnQNCndp
dGggdGh1IGhjcF9zaHkgSGVhZGVyIENvbmZpZGVudG1hbG10eSB0b2xpY3kgd2l0
aCBhICJMZWdhY3kNCKRpc3BsYXkiIHhcnQuPC9wPg0KPHA+PHR0Pi0tIDxicj5B
bGljZTxicj5hbGljZUBzbWltZS5leGFtcGx1PC90dD48L3A+PC9ib2R5PjwvaHRt
bD4NCi0tNTgyLS0NCg0KLS1jZDUNCKNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpD
b250ZW50LVRYYW5zMmVzLUUuY29kaW5nOiaXNlNjQNCkNvbnRlbnQtRG1zcG9z
aXRpb246IGlubGluZQ0KDQppVkJPuncwS0dnb0FBQUF0U1VoRVVnQUFBQlFBQUFB
VUNBUFBQU0aViIwTkFBQUFjRWxUFVZSNDJ1VlRPeGJBDQpNQWdTNz5bk8zVHBS
dzIwZHFwYmZBUlFFak95d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZL
d2taDQpzZ3J6ZmNvVk1wTDJqbzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2l0
QWY1WUppdz2anYwWldSV00vdWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpS
VTVFcmTKZ2dnPT0NCg0KLS1jZDUtLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0R
OZdKzkJU6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjER
MA8GA1UECxmITEFNUFmgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dG1maWNhdGlvbiBBdXR0b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5Mjcw
NjU0MThaMDsxDTALBgNVBAoTBELFVEYxETAPBgNVBA5TCExBTVBTIFdHMRcwFQYD
VQQDEw5BbGljZSBMb3Z1bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJqVKfLwLjJj+gBUCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg
9r1mAfID1B/wlbdmadXPMrszyidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07
k0sV+UdSNRFxrfKeoQEFXg0aGdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74
zFCWp2f1ZkuE4A6141koaZXC5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY
9VfVfcrv9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r
8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQQMA4wDAYKIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5l
eGFtcGx1MBMGA1UdJQMMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNV
HQ4EFgQUo1NB1UQ8gCkVfAEj80e0r83zdw8wHwYDVR0jBBgwFoAUKTCOfAcXDKfx
CShlNhpHGH29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCsTKcFqQMPTryujRG
zJdYA+R9eBAuDLsatbtKtL4FzkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5
AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTgt1qvaKcLQP5U
zpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7F0D7PfB5v94M5274XYxW2W4uKgd7QGn
UZROsVSYkGiWDp1JhqXwfDz8A0enITGXnoEkaFvviCqh64P1hIeMorj36pgL19o
WZD6YrzSWHUz1F00juyu0fQsqm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgw
ggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUA
MFUxDTALBgNVBAoTBELFVEYxETAPBgNVBA5TCExBTVBTIFdHMTewLwYDVQDEyhT
YW1wbGUgTEFNUFmgU1NB1EN1cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEWRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMQQWxpY2UgTG92ZWxhY2UwggeiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1
078oullsk4ASvSwjsCNo7sHUa4xQU15J06VqY18LANwORjrc9BaX4MguzsBFXBe6
uFh1mVpXmFSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0
ls/gkUP2Gxzyms02kaYWTut3SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbB1

```
fkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4Ku
ElnAtJ7BtZcs17dUy9u9C0gEyKRiVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8w
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0R
BBcwFYETWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0
BgNVHQ8BAf8EBAMCBsAwHQYDVR00BBYEFV2zLItHQYSHJeukWqQENMgZmZzMB8G
A1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCsQGSib3DQEBDQUAA4IB
AQBziaI2p86poGkjD/4Kkk0HG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAo
cCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoT
WgAkoqENT1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2z
L3HR+M9CDr40pq2JckzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF
07rNmT0TzPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSr
JNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQLEwHMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTQSB0
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phqzppq1zALBglg
hkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCsQGSib3DQEJ
BTEPFw0yMTAyMjAxNzEzMDJhMC8GCsQGSib3DQEJBDEiBCB1lHSf7b+HyaqXmEwT
DQLFcyd845Y683f1n5KaB6NjMjANBgkqhkiG9w0BAQEFAASCAQRRSDM+MtNb5av
W1U6o2LxrdXrrIy71b8Vw1D3gHSgEaeZ3ZvZ60efQPh40kHNY/oescj+rKZzcLHB
s3RZ9Tnybr7p3kawIEFv1DW3aiyXQ49gQyPHn2Nwi6hK7Gn5d7rjSFuzprWYACg7
hAVWBd4/prAE1mNMR4D00XoPYZn+ggJb/oaagcbdEy3Wrzn02n6TW6Eb7bBoUT4t
IrZRwxPrdP30T7N1eHMMCDNGSxt/fC9rgcRLz+cj+1czfU1Gf+qIxc05HyrVMrKL
+XiCEoOck2+pbpz5WFPcmnRXLgH2FM1SNWU5RwbRu5YZejoKBiUZNIUm1A08d5JV
U3Zqn1/G
```

C.3.12.2. S/MIME Signed and Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-legacy
Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:13:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:13:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="cd5"; hp="cipher"

--cd5
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="582"

--582
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
  hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-shy-legacy
```

```

From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:13:02 -0500

This is the
smime-signed-enc-complex-hp-shy-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--
Alice
alice@smime.example
--582
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
    hp-legacy-display="1"

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-shy-legacy
From: Alice &lt;alice@smime.example&gt;
To: Bob &lt;bob@smime.example&gt;
Date: Sat, 20 Feb 2021 12:13:02 -0500
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-shy-legacy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--582--

--cd5
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQejOywiwYnCTkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--cd5--

```

C.3.13. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with `hcp_baseline`

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the `hcp_baseline` [Header Confidentiality Policy](#).

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 10575 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 6820 bytes
    ↓ (unwraps to)
    └ multipart/mixed 2345 bytes
      └ multipart/alternative 1136 bytes
        └ text/plain 389 bytes
          └ text/html 484 bytes
            └ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
References: <smime-signed-enc-complex-hp-baseline@example>
```

```
MIIEfAYJKoZIhvcNAQcDoIIebTCCHmKCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAB4+rUyYwd5++VSpboCoB0ZnRSxJI2onFBv
klMu5xi3XKXyXOMBoxnRCzqXrG5U56fnqNGN61fyTQNY0uPTYzb8PE4x22E1DGTG1
+PreSLEb/poN0c9k40f72wBi31tN9e6cNJI45aulpg7lsyfqr2Hh1sNUk0+/qeBv
C4+6xvR1zudZARFPFBVbSg5Y78mHBC6Eyou9Dprv3sMIej/t2WLkfzsyZQB3ip6d
y7r4Hr14nTn3NWf1T5PiLU7Md0iAXmXk4+5ZMVHguq/YAQ1X24NqloiH4RJB4+tB
JKvZuWldG48r7Xh3N4sDuefzNjYzRuC6T6bL6oKIyd0xbftbBKAwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAoDxdIdVE0aRiQQ80G0/7+zdr
XaL2a/LqIQ0geDC7+NarHKxIPGromx5GGs/0A7Hc1WmUUAEl26/3yULmY1RIQ7FR
QbfUzddUU1t7nSm3k4J9dVENgfhpqIjZYp4xqsmJNYYbBH0+GL85BMw8MpB3ndvE
d7pzGCHWYtN/7mPYmf1vJmfC25u3kkmkcuFWafKBCfai6fSe85UQg2G5Y/Q44tNb
B5Q9N3QbFysX+u5etKwnPd08rEL76Bf1CBhTu6g0a03HodL/A5jGu8kg9CXqkSwW
vJ+tVggRQTU/Z7hxav2kDa0weKsCd0hSCPbK14e9E+l6bc2QLg6GnIu2Eu+bYjCC
G04GCSqGSIb3DQEHATAdBgIghkgBZQMEAAIEEMIDwGtKy+IO9HP6uP4Udg6Aghsg
```

v/eTch+9+5zUIxYIGGJHR0R2nyggJcHXvA8SU2XqzstdG3b7AzrDoIRcKjqicVSF
4iojFAqAw0A0rFecSokWgHtqL3DAw4BT1Ic/alh7n4IuENIEpdX8wIE3X4xd9np1
Vic3K4eq3Er3WoHNssA8gazrU2Xinfqt15S6sCy5pSK7PN1kxWUUBp14lWRMFRG
iWr6IfyVm9By2whh80v7p/bRqC+4rwmIqQU3SuWzMj8oyrrmAlt+A3zEPRwwj5p
hRAUVeAZwFZN7BVNtqGN34LFdlsS0YXWXWkrhFF48nL97yxufY6eJt5j/I+L46k
2gufwjKVM8JNQ2LeIdJgBfJDny/zXG0Uim400m1G4VrwfoLRDgbidVGWYShiyYd1
azu5pTjhnK+o0tn/SQ0y6wmSwUtHry5zAAI7oiMoAfQ0vYRHZ0iE0fMUw45dW7jH
COFSIO6nh9ieAUPodc+Br1o+ICvD2I1VGXIEtUk3/nC2iXcaMxvAUNVN7f6YqM4H
0+ABTX3JUyvw0GvPWegMRZUax478CqIW6I29A8hbJE2/nA3YEv+TiRggBfKfJKS9
9CgLD09e0mD88+NZRW8Xh1UfGHg538KK6mZT6NooBdT+Q6TghMDsxWHfZGTMpacZ
HVQ0IPvC143e0DBQ/dhI5ijA0teab/EPV1uevc8ezHKJymBMX+VJnBf7D/IPygd
c42YtLuW7Gon/rWkhJiDnWJ/YUKUUSnRI3JKGqfuxQ5Q5nIfRQFziRKTHEvL3Xir
74jr+Oj5HuLVrHYv+uA3+DD8dwe8EGu+HPDfmzGkAWGwaLtrojPlyrzcsEs12jPMq
Q4dpFTFEJSKV2vj0MkoK6pSmPYAcJsaRkyVykZwILOZ5046E/wYZ+JV+bb7vgn91
7u+6ocEJbenZloIkpKd56vDPEzNTDs9zG0ZdA4q2FM31ITK/fdgtznQuu1/0FY0f
507fhnUIIFGkEro0Fm1Cq4FjljsJIQF8zeIn623dFfW5E5wicuLXBWbx+1VlcI+
854RcFUrAjK8C0xULJH3tK/DK3Pee0QVi20wbcdYWBQ9mGA2kOaJO0c4Cd9fg9V
i1VoqxwW2R03SBAilyBmZ0QEaoy0TLjvr2TCK1LQQFv/rCi+Mv41ggF/9KAG0aFA
8b2hoYDWP2MIZBbZMLp+SVENRVmjdv5ok+NW/nFLC/eD75BH5AZyzkatfE4S1oXj
Qlyle+fGzD3ia0xuz0i++PsdU/7SRXefnJog1hpKormrLE4WACamfLVCFPiEepPM
OYCiy+2Yie+jRTEiGw5gSP6GLH3Q8QDPX7Ycd7bDTt7Kv1rJ9/u6nM3N72qfU0s0
KwdQf/b85KgbM5D11UWBG/oWmTSicq5rfKRknyJIUulfk13QxmYW1yk3ZSPS16x
opMhoGLOk+BjSmWWVPYUzB7X+UbpmaqPAX9jhezZpGo56Z/4o6lK+ydGs2IBMR4b
BXGozhRp+ttw+fv5NeZn7BbjgupRrMkybLP3ihAiMPpKBj1+ZWV79SnwQmsRrmV
iGelD9rh4A/Wp4Le8M88ZbCursTbGMZ7AcTZved4GdNFi5tAzieyUfu0geQePKSR
GiJ8cObCYK23tDzBM4czpxtoT1hayHIgeRrKzE8Ve6K6fd56Ycaw/AdnB+orIpc8
ZC7yDKC9omlIYhs+v4iYpzSeAl1Z1EMY/PUcAKMGpj32fvdZD1mfO+5GuXSis4q
mpr8giCDhPCs5INWBFyFVAy4dXJSszOnfptph0BM+DXgU0opZzi46nRyDK4rH1XX
eAj5Xn4vA8rMoiRZkzTBanMuDCMH7eBftzV6tE1LwJvGps0tTsluYmY9CK/g6bG
AXN13DZF6r4PYsSvhA4Dv0DVhu4ZyYuavo7KBwp+79oz9/or+aWoQ4yyPH66tOQ6
v+Pd1Z6j/KmLFdDZkGND0+4xJqrf6L2Mie3K+GFfuCW+QB9zu+prW627gFnL8EeA
M8EDJI7IYoCqcc5pjTeje0EYVT0jhxaTtbqKkYtvidDxQUYv1xVBzGCLv/Bu0hGi
8HntDWHPTHFdVKeWJ44vAMATWzWtLEoAyMtpAWboN9CYv19V5GfwSdQdYEQTc8v
VAXvf2ucI7RFQI28Uv8g1IHdh+oHNq9QsY+d2ItswzJKRhbUU1GX9oXrR5snKTHJ
ZG/loE0tOzgmXX8AEmu7onPtAhF0jrnJ68EACVQpc4vWcJ8x2FyFwUQTmcbqFPc
YUIDyZLJ1oV3eXPCSTYBc0LCFLkaaz8XXSLOEWBcmvu3X5enPi3ac8LdPH7vjEr
ZvbbQHNgzvX/QubBGpA3gYb0sKMv7tZtoQ84ZLvPisqoNwzETQRRwLjoomekk3Cp
gSLSy8xqc4Ip5Auf15Bu3VMp1J2XtFphfSiao2FYXkliaATRVCfV8LsKWWyfOYZy
owJrYBTJ+S0kRK8X1Lc9EYpBTJ+evNXjH02t0S6B4j2y6VFePVplzEXWn377tZzu
su3AhlQ98rkaZYHxCTS2klFlePjwJLUfMl4qly6jBBdGjMMxZWsgn/MMACJBYWH
qhbCvcxf13D6AhED40/DnN57yh1nJDj6nVg8tq2K0Iocom75nXo0EOmM7kSZuwIS
dr4HhRk2ZlzyPX3rrcX85VMGUjPaiI4/E3l0fWi0mk4ZRAih0fM3IfMFe0Wdw20+
9umTwAvIYggG6ZqEiJz8uKpZk+0pqxXkaZlY0h203KHg3s1BKcJbfZOPPZ6tfex1
0Bs7B4K3z9swIct1uqoVF7rHjZ0V0INKLT38ixkrkk7/JGPwXyuwVBZP1JWJRtUu
0hDZUMXK+B3tD8W1M0Lq8tx0MSBPf3BIP8ttWSYUlc7IQYGRs52PoMNApWw80Vty
mjDwKZ/rS86T2wujRG3AB0hRIQcyMXi42dWsDSHIdzjex0ILddgDbSMJiW2Vneg/
OEZ90WUxSi99ewLiB8Wjlh59942xIootNhKujfbFYgtUAbli43mXXqOzpsc5VbVw
7c5HK50g6C5TQDGOaNYBqutP3d7df8abe1rtsZBcG2mfh+Pxx0LtsZrTziourUte
b3xnh2Ek0pudGTu0CjAkyGHIbMPHkXpJWoHojj66F8iToH8jL1eTheBnW1/NWQ30
U/1jquVs6a0GbMimg5/vxIIW/qnozyDfrwsmFSfIhs0cNyJ6pUSeNMYRVUEtoK6n
63DX9EQ0Bm/rKZhaznxHrH4u0b7amC8uXKHEK39JZaKg0gUNpjWXbVkJxB1n0Rg
LoBZzt4u0JNoN13zdDM+2/+JNP0Gq90S03SkAY31InkSjSB980BJY6V+f+02nPdS
QoB+DFXtAk5EV9DYcJRFI1wCLCIhGMcy5n0lPrjucaUPwfbFd3JDkk7AzNtBpQQ0
W/BXtyvT6GFvWnc2P8cnKrXvGcb6YvN+i7mh9JbIC9rI18x+iM6oXE9c7Xxz11/8
R2VatyR3S7v2gj5X2hbqz1xgZHuX+ZaXm6muozmspyM2tNMolYpvpX/kmHN/RPzN
vza7XzHXcZdqNwWKKub8T1/ZIJeA12MMKDRpERDndaR4j0iyqZTMU8qCrtPhmmI6
A51LjLkN6Vy09AWmAE135H+0tDOKwqE3E6DHgS8zn14oBfY+2+NtFdQmCKYF/EKr
s8NGezoAtPxq0Swh/crfgmfk3o0hv9FGM119qUU0LAMy9nUKv0Nsci+70cBR2Sus

WPPZJDJW12F8z+oATPT5+XjEsGzm1AcWSVf4PG1t1SmBPn7RWmSAE74T1Eu0EvfX
4Vv84/BLcTo31H/caIT+SInxeDAON2aF+gNRteIo+MMQeHNU1C+iHZNzs6ye1Vy
ySJ7X2HijnisxBmK015zJN75KdDpQrZt0c9/ko++AGIpYcSLzsyxL5PuQTAXWGA
1ioCI7A3icYsSly7SLUZQXAFMcV6xVXL4zx4ACohEFgydA9s7MNnuYg/DC71qtHJ
iWtODQK2cnP7rptU4R9u8524AwRZbTpvaJeaXzZ5gB57ziN9JFTNicUWf88UkJcc
Zjk1HxtdmtpP4kqiT8MEJQEY8Y4Q0Trn45GazsZnfZZxXxK2EC0w/Mj7/RJ7mCPu
SE0YdFAu2PtDh1jW1JjJv6AeqosoSpPuuvRZt8gBE38oKiHlRgkKRHdjEyVsg0yj
eD7qVkJ7DzYz+sZhrQyigZY+p1A/hItQknAFbLiSB6X0ZCIm1/+n0/1B7hkDSaT7X
wYTKdpA1bCgB1/9z8WAUwojaqu2wCDBG5wvKZsfeViSloXVgxezysvJCVFiHdgn8
8AuYmkph9MrjRvM6eq1bDZWQ0Pxb0kV15obEKTlk7tFbudaoEmYI0sGbQ0LWGRCD
DEu6sftmbXKQCTvy3HjXuZbgSt89VZIFJVu112qU4XxYPWC/vasCJ+atAgQk5Cn+
CD7i9psfPE9EN0mMdxCDu6GHkIYkYpY54dpKeRMKizr8vKrMr04DM+VON5/BgePv
AtgIXxQuQj1chz9z2/AEJsgLnd/61jv5BTJt1FB/mMfmZqRxi4ezRnK9tSiMLLDV
Y6Zj4qmSZxyosNvkUiQ3X6ic0rCqlc4z17cQN5lVKJ9k+mb6MDpDUXsub11FnJb
V1waMVWvpPBZyDmrTB/Rtiinzg1p6kNuoS92Di7yGNpZUQ0jxf75wdXlm9cWvTDM
9x1sBIPiTTIzyW+x+iYIBuFQLth0g1evYXmUZ4BV90hM3ysKH467v7VcdIhpJgrF
KepFhg+942rWXAgAe1aFEhq5bBgUgydqyJ+N5IIZUunphdodrNgSWI7RHQJfWktX
yi+BbcsWYWyXvouW3UIAr240FpW7/cMPoRw8w6tPvQ8PCvVfkeG8Xxg/WxiVtpuS
CIetAgBBW4MI7C0icv91TizUM81hCrcU0dcqtPdNU0XQziGqa/CICFHX/4sOMP0K
UMbP5Q1Y840283qajxk7sVEas4PiDaA1feIn3BhMwkaPXfleRS1vc0779SRhc2Pm
yBuc5UbfGsaZQ0gL/WsZUYLk6VAt4bb062rntIn9dZTacrJl3uPQtuNQ4brG6IM6
08sFERdIwRFVxSyT+chE23cMgdCszZ2EwpkDbld0ntdKtKd52FGEgkft3gYdDV
XyZc/17Iu9r6kD2M4/dn/W2I9vmBszc+NhXhA/FE2+X6pZgCyTFmbkH25Q3nDDjz
UcbjAmvMEGVI90Kv1kp6+qIdkUCkAAjigA1p4X44JSYDRjSovIreP8CawufuA+9G
vJ+5AyFnexRk4yCGa+IE5Rt5uTctcHXb6ZQKe161k6WLZ1L fJ1wrzU0bjpcEgNS3
PJ07n6QkxiBpqwnc89mAJ00rSAYxGe13vHpT48kX6CHdqV+LDr+21MN1BM1XBGXI
qRt6X5dG7zfhNCoGQICAd3yj8kGW99VhBBc2QZvK7EUUVJF7LAqbfzS2EnZ5G4a19
Zq15tnQkCJzuN0vwaUkQAuGFri5e2LRJILklwskqJP/aMUaXU9XLff+n/ld4Gzp6
m+fgDU6mmkhWasYJtjR2UTdtu2VB1EoI0irhohnUyfyaFbq0kEka+p16+5kr7ds9
fAbTJNdVjyC0cML77YWqBndfs4k/vs8DteMnwgE8VTZFc4FHBfRLD6rUzxLKKLr6
6tFOWbph1Xnmo6oLswNBucyLUcZXD22PKjS1Hbnp3o6FXSdUPTy0qt+g/a7N8q/
QC15Fs77G9kc+dLpETXCUX80/H087v/74ACcFenSeGAwTWK3gszmbeyvyzqo8MZ6
8xZxoPbf2kg1MS8Bbn50DDgU91G/5Vst70U5RvzoBiHShB0QLNTuYn5dZCaJtW3p
U5StAaV1CoBbdvkCH6U91GuSoEV+fpp1ZN/U5vY2PntEhEiUcTwTIHTeeJmpXAHY
KrwT/daJNS3hA1EXu4ZQIX+981EehhkEqZuXhm+F6AZWce/NilIAf9YdYrI7pXx0
Ec8jn9roF0Sa2X7kDWJ3UrBjzUM7fmU4ypPi6vH1HF4RD6t+IOmAPmkNiMdd0xCG
DpEVW9cJmCcZi0W4s+bpjIjwWM9j/TSyNrMp6Eur3QChghCdVvN3P5WVjtDGZHu
KNWz+s0pB7zMEj8Mveu5Rz0/E0J9JxyELJkMviqCRfAmqJ40ekZatX4ZJNYIdav6
C3qVaiBcumVHOQNMaaQy2LkdV6yDzPchMc6umzCeeyufkGs4RmWfaVietjuE76nX
fGfsVjcg0Cm+5BzYvCKmN/xEEYtMjyElByLzwcDvX/nedsZV2pyuggYZjqc/qYC
1sHSBNjgVWQinYDEbtebj6I4i/0/0eRv4vfcdE7r8mFm5Ukx4JP9MJfKaNPWDZ2
cyXZsH8/i4+/u+P99onw1y31qdpC07Xtzo2UKpdNla4Gj1f0ij7i+Tuf057/13WA
XQBcvABU0H910zDNiCioY+A0+qHOWgS95Qgzqf1+wwEZFTC5r1V2yq07eePrW0/M
Zy0HdPVUNmEavV9CZ2Cv8KQ+atL1uLkw24jNHYf2Fn1Mndb2+iSX9lqP2FfaHXbh
XSzsMcVxj55iA1m1BAFWoHR2yhJUJS+UtB38Vx1byWlrmUtZup61i9wFo89trRx2
S/xfer8pdtg23ZutvETVfjFmNNG7w8Yx1yKT3gZo/eG0slrY7hR/WA2nARc55fAB
ELxGuZJp2H87J1noU/4L64IGHSNS5kzyStSvoihAg8a2bmV2j9FDBW2yUMdqUiX0
opb2fcM0J0F0SECNmz4n/EDzKLZjJmw8daMbELRVZ2Fz6EoUzmmYQG0BLEeFz371
Ei0bjukJA1aUpBfosaw/f+Ft/PUYlpJ5hXPfv8qJ+bpmHF2ACNPymYDJ01TzvMs
Q0zDJUZsMSENb24FCR6eMLMBGa+Uh2ix7FafPTqx1p7B80F/f3royH0NgIHZkm38
SYvwLs6MYKlioM7+wMU8qDOYweh1Igr6oBDqaeC8lrfHai7c6h67QgV2qDlaJy0
ejoTbnWuRDmTrRdINTRpne3SQoKa1SzUfARcbuWoVC5cmxdL+wLYT3PM1mWZ94cW
XNhGfb6qcwBtK5PWxxwIj6RxxwEK2Z/+EfWHHiqtHT8Ft73gILqMYMce0ve+8Adx
g4JBn/pKvTaEt+n0/cUJlN1zk9Cpf19ug8y798vMD4vQJ8Iv9xk+zaNZ4SRrvZC
jbiEXAVuwkGzIRobUDC4gE/PnnPB6hbhJM3dsBhfh+LaZfr21h3f4anQbunn/sDh
ohLXkzDz9K+9RN2P0uS+0M1IHnBqX7vH1SUXpw3s018JVEF8gigXF5GV7F/EXW1M
2LEvrVjXI301VHSbhPogCD+98smaAnIUuBQ7Tr+0nSIMKZ4Bct8jyx3C1d1Zk31x
X4VrEMLatemExIVkIqk7VC9a+U8zV5vpyJ01SDJo9Bm/mbxi0M7DwSbaxJrOURPI

```

gFJveIetLrwTNeq0auBcuGXjyQVdNQtLIXydBGtZg6Rj9W0/yeHQYzh8IUlQB4It
TBTniPTYpfUiVe6acfDDKeESd+S6SH9ZNaXnZBTqxpJHeVUBtFnp1Zagj1ZiKP9M
0CRAycswHBfIT9BGir4odnv0k9aWifBHDqjGJ4XGaiKSQZ0xuZRZdEPyoRg9FsAA
mlyMF+JdANY9hGdbStDS3ok2tKiRPzArphUass9P30Mrp+hphehljDw58vQxyIj2
rTbdv9G4A8gE37hn1A9wo1mW0E0K2nL1/CVPNZDlavLTWcx/RCLUGTgtvQsERVa
CktsA9Fd6jUK2bqZicvS41RXRHytLRQD/WbNR6iGFq3ou6iKSWi0AuwmMgfcnsT
yREWaTY3gs1eIHCrmU1qfxz6WecCM2DpgEQVL0cZBDJNB6d2MsDjkcGCrsi9hPda
vPDNKMxsAAfkeUT4nQ1FbkGFN19wfMvHzZdj3t2nv280RyarOMR7JdZy8uH9ZC2x
MBUUPa8dcLqfCsIwfMqHSmHwoE7avo4B+j9gaFb0NyUrpS9XivPaR4C/VdpvmEx4
uPCQcON3hnxts4H0Bbnxr567VRLH9M2lh95uURXg2QroDNXBKibYNLExrGnsuR6e
G1+GPxXV5k5LB3QavktPU9UUnCTU/yh70JUJJC7LAic0kuQfG8W/cVWa92dXoGFic
sePH1GM5AmG3EkaeXiTr5gT2gG6S2J6WfarVJSkvK2DL962V5btA9qFvu85hxjC+
/XcucU1bcePirxv0ZfXeKeyk0k1NKKiJ3bVnGZpQIql/dT1LxPFF9pEDQM0tucec
cuDbVmh691nt5Wx8Emk09BXRW0sxqgS9Rp0ZnYl9/0CYwJWH178sfRfuZvCG4Lv6
bd1a+A80hEsh0hqzXEZlRSGNSVw7jIN5CIXX0cs62UKsx/+PQQIV8RQZafy2vzbz
N7PN501YdbE7nRjIMGMRCs5tibuuKn9/HRY4+NsaLik+olW74q1EHp1N0gtRbiYM
wvFTWnTqguogKEwb1RAysycPUuTV8RvnGN95y58c4pnpTwZRFw8rhGnE0VHSTVq8
6796GuKYcExa3RoX2PUU4FDpufq0kfCRlWxvuUM5m2lr73TA2hb6icXhsNJ80EGa
AfufQi+RH93+6UFTrmWlsxMhRxR2NpWxXNEB/7tkyjpK5jh+oN0f279PapJ3FfLO
AV7phEbm4W0BSBdNjmnzLQipGKzsyTd4XlgaXB2HqxFlWbKWJdAdHkFK8faN4SK
zttxOBngAlBMDptxEi4tev7S93SFKoqMwY18vHlLOHi/oFpaWMjJsE4uxdqvtz/x
aeZMmgsd1ZYRykbGzjm8cMeoQawJ9HF6AkNFPo9+AsgXCuPNhutGzuCv3vAWTg
yXAiMHDuzahSggfr7r2ixkDUxD12/5RSeSDvCkeCWsjBKVpyzoWn2QksAMBoETyN
F2gcjouX2Cp+0k0QV0e8Y6zIOWE/SGUKFKUDRJUSA8gkpfXWDPV8MN6rAMULWUGP
jYcRtabSgnlXKn6VivRiBlGXvp7iOXpsoGtMwof9hUcoo/HYMAvdsd5anaIZU8tA
g+c+80Hky20J5mzUWmk1CcBIW09yyAHsy7ivSVzJtxDuTrQAuuH92MzgYvGnoioM
uaK0wNzrmhAAhBruv0XpMd/RBIu5+e8EM+fIuYwwwYDWIpn9vMbKkiBv4h5PQ8+T
cunAwgNdg0qVFeZ96Gu1sIHttbexEvSADg9fplx7TG+DZgSrDkxhnJ80a0hZhZ2F
CYJJrvEcQn+/ItTftmmV5tpG2r/LCufYFL26h0RXdD8=

```

C.3.13.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
smime-type="signed-data"

MIITWQYJKoZIhvcNAQcCoIITSjCCE0YCAQExDTALBglghkgBZQMEAgEwggmCBgkq
hkiG9w0BBwGggglzBIIJb01JTUUtVmVyc2l1bWVjogMS4wDQpTdWJqZWNo0iBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmUtcmlVbWbHkNCK1lc3NhZ2Ut
SUQ6IDxzZbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmUtcmlVbWbH1A
ZXhnbXBsZT4NCkZyb206IEFsaWNlIDxhbG1jZUBzbWltZS5leGFtcGx1Pg0KVG86
IEJvYiA8Ym9iQHNTaW11LmV4YW1wbGU+DQpEYXRlOiBTYXQsIDwvIEZlYiAyMDIx
IDEyOjE1AyIC0wNTAwDQpVc2VYLUFnZW50OiBTYXQsIDwvIEZlYiAyMDIx
MS4wDQpJbi1SZXBseS1UbzogPHNTaW11LXNpZ25lZC11bmMtY29tcGxleC1ocC1i
YXNlbg1uZUBleGFtcGx1Pg0KUmVmZXJlbnNlcogPHNTaW11LXNpZ25lZC11bmMt
Y29tcGxleC1ocC1iYXNlbg1uZUBleGFtcGx1Pg0KSFAAtT3V0ZXI6IFN1YmplY3Q6
IFSul15dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDoNCiA8c21pbWUtc2l1bmVklWVu
Yy1jb21wbGV4LWwhLWJhc2VsaW5lLXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRlcjog
RnJvbTogQWxpY2UgPGFsaWNlQHNTaW11LmV4YW1wbGU+DQpIUC1PdXRlcjogVG86
IEJvYiA8Ym9iQHNTaW11LmV4YW1wbGU+DQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCMGZWIgMjAyMSAxMjoxNTowMiAtMDUwMA0KSFAAtT3V0ZXI6IFVzZXItdQWdlbnQ6
IFNhbXBsZSBNUVEgVmVyc2l1bWVjogANCKhQLU91dGVyOg0KIE1uLWJlcGx5LVRv
OiA8c21pbWUtc2l1bmVklWVuYy1jb21wbGV4LWwhLWJhc2VsaW5lQGV4YW1wbGU+

```


DQpIUC1PdXRlcjoNCiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVklWVuYy1jb21w
bGV4LWWhwLWJhc2VsaW5lQGV4YW1wbGU+DQpDb250ZW50LVR5cGU6IG11bHRpcGFy
dC9taXhlZDsgYm91bmRhcnc9ImIyZiI7IGhwPSJjaXBoZXIiIDQoNCi0tYjJmDQpN
SU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UeXB10iBtdWx0aXBhcnQvYWx0ZXJ
YXRpdU7IGJvdW5kYXJ5PSI2ZTgiDQoNCi0tNmU4DQpDb250ZW50LVR5cGU6IHRl
eHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlnRS1WZXJzaW9uOiAxLjAN
CkNvb3RlbnQvVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCg0KVghpcyBpcyB0aGUN
CnNtaW1lLXNpZ25lZC1lbnMtY29tcGxleC1ocC1iYXNlbGluZS1yZXBseQ0KbWVz
c2FnZS4NCg0KVghpcyBpcyBhIHNPZ25lZC1hbmQtZW5jcnldwGVkIFMvTUlnRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcn91bmQgc2lnbmV
kRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5hdG12ZSBt
ZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0
DQp3aXRoIHRoZSB0Y3BfYmFzZWxpbmUgSGVhZGVyIENvbmZpZGVudG1hbG10eSBQ
b2xpyY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNTaW1lLmV4YW1wbGUNCi0tNmU4
DQpDb250ZW50LVR5cGU6IHRleHQvaHRtdDsgY2hhcnNldD0idXMtYXNjaWkiDQpN
SU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2Jp
dA0KDQ0aHRtdD48aGVhZD48dG10bGU+PC90aXR5ZT48L2hlYWQ+PGJvZHK+DQo8
cD5UaGlzIGlzIHRoZQ0KPGI+c21pbWUtc2lnbmVklWVuYy1jb21wbGV4LWWhwLWJh
c2VsaW5lLXJlcGx5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGEGc2ln
bmVklWVuZC1lbnNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUETDUyM3DQp1
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBeWxvYWQgaXMG
YQ0KbXVsdG1wYXJ0L2FsdGVybW0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmtpbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBjDcB1c2VzIHRoZSBIZWFKZXIgaUUhJvdGVj
dG1vbiBzY2hlbWUgZnJvbSB0aGUgZlJhZnQNCndpdGggdGhlIGhjcF9iYXNlbGlu
ZSBIZWFKZXIgaUg29uZmlkZW50aW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4g
PGJyLz5BbG1jZTxicic8+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9k
eT48L2h0bWw+DQotLTZlOC0tDQoNCi0tYjJmDQpDb250ZW50LVR5cGU6IGltYWdl
L3BuZw0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50
LURpc3Bvc2l0aW9uOiBpbmtpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNvaEVVZ0FB
QUJRQUFBQVVDQVlBQUFDtMlSME5BQUFBY0VsRVFVUjYyY2VZUT3hiQQ0KTUfNz0c
QW5PM1RwUncyMGRxcGJmQVJRRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDlj
aWRrRSs2S3drWg0Kc2dyemZjcVZncEwyam8wNDQ3Z1lEcGVBCmsrT25KSGtJaEFm
VFBSaWNpaEFmNVlKcnc3dmp2MFpXUldNL3VsaW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4g
QUFBQUJkU1U1RXJrSmdnZz09DQoNCi0tYjJmL0NCcCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXs5CVIEh7j00Boq0MA0GCSqGSIb3DQEBAQUAMFUDTALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExEh7j00Boq0MA0GCSqGSIb3DQEBAQUAMFUDTALBgNVBAoT
U1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEWhMQU1QUyBX
RzEXMBGA1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQAclSn6i8Gi44/oAVAn5GnCK4PHHNjrSfWUnne1N41KImVaTC3D
9zfCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2Gmt4jse2Dqs
165ernT905NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
TtMc1zy++MxQlqdn9WZLh0A0peNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqLlqhBwDH
dZ5qDTI2PVX1X3K7/c0NxbvBbaU1/k1swdszUtjhflYFZ80RuQ3qFC6vL/PGewy
6SCf58duq/A0EksCAW1b+MD8QH9Yj7CFsmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMC
BSAwHQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsoX/Ht9Ii6zyBZVjdao
x644DsiLQEP4YMS7y4q94RFFdmdzEbDLyX9sfUhdvTxDN00oHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVt1
uLiHne0Bp1GUTkr0mJBo1g6dSYa18Hw8/ANHPyEx156BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80l1h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vR
hZjVD6FYMIIDzzCCAREgAwIBAgITN0EFee11f0Kpolw69Phqzpq1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEWhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxleIEXBTVBTIFJTQSBkZlZ0aWZpY2F0aW9uIEF1dGhvcml0eTAg

```

Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFow0zENMAsGA1UEChMESUVU
RjERMA8GA1UECzMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pd0/KLpZbJOAER0sI7Aja07B1GuMUFJeSTulamNfCwDcDKY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMftmd+K04s+A8TC
N012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtwslq7
ktnNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSebwXLJe3VMvbvQjoBmpEYlaJBUIKk01zQ1Pq90njlsJL0wID
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAWQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAwGBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
J0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahixRn/C9
cy31wbqNsy9xfjPQg6+DqatiQpMz9EIAe6aCHHBh0iPU7IPkazgPYgkLD59fk4P
GHnYxs1Fhd06zZk9E8zwlc1ALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQUU1Q
UyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzdBBXntdX9CqaJc0vT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHATAcBgkq
hkiG9w0BCQUxDxcNMjEwMTcxNTAyWjAvBgkqhkiG9w0BCQQXIgQgzz6zrLzs
Pn86IlgRgm7Fheev5QucTU+VJZWxIirBFk8wDQYJKoZIhvcNAQEBBQAEggEASITl
JnQGy7Cb5U6BdSMX3mnksCOX8mvaxy3o0QqNUbUGhNNPKI0LIW0djHUL2Eq8+99Y
2+WvVn3ZKAJ7KF/89ja3u4NTiwu30wWsd7DL7t1z8DJBK6JuyaY4xtoHUPVa2gL2
1atPowCt0X5RF7lmiHQZnDGGUAzjLpVsFnyIVAL3QG4/vW609d+ae0+ccdwzzUh
lE03h3qpHK9wX5pWBNZCfdmjdXUFacU+fMe1mG9I8A1HMY09zj+rNz3onoIHJWJ2
FBWS2tqK2eW8yCf/LSq9M5k86VbTjPjvPz8FqupzugC5sUAx2JMUfU0q4A9hW+j
g8PE0cwaEeY0MdSeKw==

```

C.3.13.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-reply
Message-ID: <smime-signed-enc-complex-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
References: <smime-signed-enc-complex-hp-baseline@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
    <smime-signed-enc-complex-hp-baseline-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:15:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
    In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
HP-Outer:
    References: <smime-signed-enc-complex-hp-baseline@example>
Content-Type: multipart/mixed; boundary="b2f"; hp="cipher"

```

```
--b2f
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="6e8"

--6e8
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-baseline-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
--6e8
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-baseline-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--6e8--

--b2f
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcELEQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQej0ywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--b2f--
```

C.3.14. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```
└ application/pkcs7-mime [smime.p7m] 11205 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 7278 bytes
    ↓ (unwraps to)
    └ multipart/mixed 2666 bytes
      └ multipart/alternative 1419 bytes
        └ text/plain 478 bytes
          └ text/html 638 bytes
            └ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID:
  <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
References:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
```

```
MIIgTAYJKoZIhvcNAQcDoIIgPTCCIDkCAQAxggMQMIIBhAIBADBsmFUxDALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVBIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIB3DQEBQUABIIIBAGfiAnt52E4d0n3GCoKxpwxZ5jrJBpfmPh0+
ue/FmZE5klqdljABWt0bNZZ4JUCbzv6ML0I1Xmn+00SQ8JXpX4WiQhIE0uejfcI
ksFg9SyHfxsqmW5bh9b2VvTC3mXRF90+4bEkep7dcp60i2X33jw3E2rocP11cdY1
CKYc0CuiIp9guS0JPCenBq+OGJHJL7o3HC01fNJPC4XtaPao1xJNAN3Uw0TrHNL
RGwkgtY6Gxw1B0U1+Kn/T/rkkUgqqWrw+K7nX5WtPUW1rQgFoUHHJUZx/fXMfe0e
wWrybho46jWISNF+xDiuR1+A4188E/Q7+4RJVIHoJCa3box7MEkwggGEAgEAMGww
VTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EGQ2VydGlmaWNhdGlvb3B0b3RpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAcq7+FdWfup7R9o64oTMQaqu2
Zj3DOLonCZ92tFaySyaZY+bCvA6/vLs5Et63c3ETWzFP7HUYNfjBDOTsgrnZAzEz
bDsg3XVZGWf2vCYhEDe1RKchq5H1PPEjygp5Pj/HE2p8P0BGid0msj1nSy23FWM9C
Y+Y3fhXtcV4qB7g7FQMmB4bghxgouiPVE3kt7wCuPw6eku0We+GnrmI8qoh7aFdZ
```

ehgq2K1IA09UXvNGV0r7XIN+w08iVxM6DAELNqZ9dVNZ5fpz0SsIPvGNCZZSr0jU
Lk4+6eyHo/5qLXDFhESGRe0XUe6VSAz3hN4Pg0dsyoA02/emgR977VDsavjeVjCC
HR4GCSqGSiB3DQEHATAdBg1ghkgBZQMEAQIEELNpzmwBEJh+gxLdI2Gm1ymAghzw
mLnjPD9k41KZLVG+i7LyAI11h/fYPRxpnRjSm1Z2xWhHKQMcNvFHF/kyqZDc5fI
Ud3SenoCrX07gLELALwfH3v065D2ETNIshz/KoujlxswSettcE5LRBDsTeNwRgl7
1xSL1EjagWzAWN3i98C0M2xL679Z1RLVB+a2NjzVhDE/NktouFBQSQ5qtlzvCByc
dtBpo9IW0w/COBfm8tuzR+Cs2uanYx751Ku/KDyJfnEl+mDaP65pI5ooKrMcazTX
YLzjwwDi+idhdZxucwuWj977fBe9bQ1R5tnT0jKuch9hTB6KZWAUNANINEA3SISJ
hFiF+bYE48cBaFhSMU+2cc16qdWFzJeut+F8MESc7xpsZfoeHC3nXXcGEQ+j3UWo
Qtd48yP3m1x7m6Uvd4k2JPaoAu+N3uZhSJLwgePW/J9tMix+VXsiADBZSrV03nnH
Gd8QCyHZKAC8QBefhVaRHcx fVmtT2Ru20tKZQN7kev1KSPkpFV1u/iJfKFUFyNy
KoPGRWS5HbyD8ap0UGmVHpXjwcmA6anerktkde0SsqohokfQgU9v0GP0Djtn0v+zC
tu96SSm3aEA11wefb1I/9NiAwgfyFdf1bTJEUvfMXERJOCWsfGhyYEQy5LAXq0QM
p5R75Uob2D5CaNof7Uyr0o1zY8aadZ10qQ+NXmFCQx/yG5nrMgv63By+gkgb4bbG
AumBjdpJ3EGpJ/SMd19X4vVZOIkqrJ/D0UeFk1MMcbsrfr1CaB/OWc515wiHxFI
HTXRM8fcq27KCiE//L30auQkBI3NaP2t2EuBvusEGtCSSBUtb8t2qZxW/PS30S+b
0Ko/wnrQmoVx4Cq06ZBozVs/PKZUE/TcWSX9PhRUcaK3236Co1mZVraj1Fdcv+D
ktr/Sau12du4SVYez0MKTc0A63BUWuKNHdvI8IJueStL5BBSEWnnjnP7DRj1vvvF
mEIKebXZeAcqwhHNbrurjazzQA9GXXQELXm9gWvMg+IM0BH+MEpmUzQis81mb3w
ghPeVB9U4RkGt10YKcxuR61QkvXzhfU5ePsVeTzZbWVopx5wNrbb28yyUdG3uob0
MuK1LCEut1RSYJcB41aeQGKenMhBnXTAlKV2J9aUionW0KcjkPmAL2JfjNcBnUDJ
aUg0Ub1Nss8X7zHhTpinKyKEYPinab00YV8g1m31kt+uam1Msn84u9TSK/a1V35C
qs2jbbqjaVenV1BMKBk8JZgaQF8YAUPevrPsyFpzY9+Sf9kvJxx7zByV8YRCRBH3
2PSYrChF0og6hNa7dmNpLDix+rZgPiIqAeec4FUzwBJqcn0ueHZBYi2k3ExqCX5S
FDwwy01ilHh2DgSL3u5q0ouXZJ3nahivC9JTpJKYpTipEt0D0K9VXExYG2oQ38fH
2J6R8neBfeDWcN2aiBHnDnnTgVMY66QKNYkJM6T9m1pWmjF40Re+cjK08Y8a91q4
tj55/rPNWPhYrQZqERvda2V0Ia7ywljPtrQuEbKLVLX1ts0KDJV6KACps0rTZXmer
Fb3LjKxTZYCDjgG0FIC8TpeGDEC2VTU1gLLN+TsJx2ZGuCRqrIwzgdymMwtPL7mQ
ORAK+Ff/HaOuDLGr0oyTpbBGgmKsZx/SEoS3ZL/c4IO29Ywh1EyPS1DDMXqVsNE9
8mqbP6um2ZH614EzNm8sqPs4Wmxlp4AZNFy3yZPihZe7VVO2hrhPBj0LVLN82gcu
Kbn0hhfLTbSvvSdR2/sUbQ9pUJUq8VR85py60yGUa0EAiEie7BGy4AjHBGinW3f
8z5qEewOT/Hn9B0HIPY8nNi3k27/RD8bvYXktWoR0Z7n4UrkkBmC7ZwELunkp4N3
wzGA/Waff+rCdC18SwoZQCocwyM9cmu6tcK1bn1Vyp4WQVDqqlxakGkXdkCkU2tGr
X7d3R/638v5R7ZcTtIsc0YvjT/YD/9x9DoR1kqDGH0TP5v9nIyKuRVfvSpsPazBI
2IcZj4d/042JYIAPKokr09/7DVjn2h0Ds5RGNWJxcn2gB8ff7MYuMQkn2WpzVcGC
4IQu4k3PpLMPFu4DAbq8qH/XeviqP8nTjURCbtJY2oS0vY02Wy9kAKGjq+JyTt31
R3KPfydNjc+TckbDx1Ryxr1ZDgIOarfZaZmpWky33LyHf0fS2B3lsix8qQit5/Wj
8EvLPzSxto31qDN07AEHqVWD3aVLxfwHcEgrEqXwJBtNx004TfCDCrLR+X2b+iX
U7Va69ojWSmL6xSnXTLTzaJR0QtTJ3AmR2gNLsCVH8gqkPuK83N4VyR88pVTutXV
a27zk0tCB0BB3w76cNXNeG2fmM2T7eJHjJLLg9voAgbRM8tva9uT5r6YExK4h0dx
fsNnZuHrWxa0bb4AyUGiA/zMHuiLhASTu3Ueru3X/sMGNYxg3nCT1v9epe529TM4
eX66wEY/aPL/Ms4CpSXXfwy2PjU0oOu7JTDgmKc08cQqjC/mxEI25u51QKTAcYhU
dAzow0A8CpEwF1uKtRPaU5BPMoCe/+xdPlxXNSYcHr0yHHZJxrOKC03WJJBG1aEd
MZva54oMQx1LlXZeta21rF66qMrPfp3uHf2d4I7H2pgDEoLygJBuWqy73jzmMiib
fxozGcbKHdE0VfykiyRgLRZXh7zEsveyyiss7/mhQIKrZkapNiYwzS8KKmcw70Xd
gKxW3d1QG4oa5eK3vYMGaZtpXxeMrx5jrbcYiT3bBatfa/GutvLSJjUog1kk7/MX
E19anA9JKBEFI4cB1jVSapS6oyxWzQ12cSjaVturSNNq1ClSdu/nqYx2j2SCkokR
q7LX0Mi0JRYhc7fihBpjkv0QjW08kfz/H/EqV5SWabPUwLbMB2ccUQaH1hcofR5
xx5+BSBE/TMywN/ymHFybr+zfcWEaweXE3MxX0bxN2GK4nxSfW7N1jEdEq/Piww5
GnMIdA30YK0TxXZPYgCSGE+X93aIimDhGySHR7sHtwdt6CfYyvCnU6dc1KsFjx7d
nRRjwetZlzkRj0hGWYEnia5EzHZ3fesqJ2u9JXFBAUJWNe2nZk5Sj62kzLfsEab
WC5slugY20gghb3qkMJW9LJR8H7aU3me+rGR3UeDMqQyTbzUPnd8+pfBupRUNyUg
m9KP5JPBnDX8s0DWhiIQpQiD09I1UpaRkVqtRQxernB0a5qHTo71q2BmbYoIn8jw
F5b40UAhbC0kv9AM/5KDLzTSS7/DCFFDRrXUWW4E4k070qFbahrFmGZmbBcMg7i
x+h7+HlHNRyEQwgEpsYDiCMna7uigdVo0d1Ik9BXPrEEqiVx3218d0U3tKrQ285
u0EHQTfpG/LD+jeFw0E5pUPF0CfvC6ehmH1JcNoB7xWvf4YEJN8i9jhYx1wECWYR
Clzk9P1hkJvpMv85Du1jQUqHbHg0/w3uZnkP7sj46/z20YWGVKh53uXWqzs+77ea
x7JfKviVo89fALh3rxrxrvQu7LV0dqS0nZ8eZtXqabIt2+k1501DYCyXU32dbjUZL

gfwFdSn/QsNd3v8X+Sg/+95JUU2DihxNPsKZ0Ge10EznOaxMm8u8Ry7WU38JUKNG
1XrHcgUZ9fqPvJcFzLKT6+H/BPYL5XUn4yxtmx56ejicSdQqmH8qYgc2nn6bN+4
EzsA8Mj0bAfziRD4sNmTd/pWSjWfX39Mhj+dtmNXS6ksXpl30ERv3ivlSfmpk3+z
egRpGurwB0RH/easzdKvSHYgAtmVeD3yvGxVpDVwLg9bz2pb597KK12HErQmJaCK
pqz/Yvac1qE6ZSm0FgNGVMspY9ttLqYUNEPJ+Hu2aCt0xiY9oNsoWFj/kFCZk4jg
I2khWehw0wq9qw5Cw0DXPhFnPWbsrheTNng60zeNfPkKG5IKIOmHpsg5/CFijV+h
lCYCkiUU9L9Z/ENd3XA31VQWDeRbFqLPiOcqY/8U4mbrH+zmpjPgYKIQ43Lt9UhT
NiwNs3kBCQ9NGy4AtIKjmxqncw1UXpFzLLHuPE44yWZ7d30/nv06Lud81tYDnSh
WNAG6z4PGmbwJKV4NePEngi+HDHxpE8mg4YLpmN+Jo7dsRZ9zBtLcWayy7crQEj1
uGwVLKtp2K4ssFSPImmIQjeTPCVWLZYwuHQxWmt2fhcgG+G4WQmHjjBeqXqftegu
bFX1HioRnjgWhC9f9JG39E4QvzxogsomX+X61UneCu8V0hohq0y8eIyFKI9piFJX
qBk02Yij5ilf0w9EmgAvM04KgX50ofTC05G3g1r+/NXo5ojmcXR9vbHv3ZZQ1AaV
9kntSirAyE3Ug6pBc3F1WRDH8WJ/Ysdd3s8j9BQpTn31hkqwhTadsOzCfKJuoG1i
UyMCdcPoxMf7DwpX2LaqDcElgqLUz1zJLNtry56eLmbanGKoTgW5IDz2JTBIdodE
hvZS74pHATmajkAxyjUIGWpZDj81R8B8q09hp0kTUQ1sQpbtvZaAAno1QcaMaGg
oc6l0/i8g9H++kSdZ0SpJD++015/qSk1QXVVyD0S1hNCrww5MCXD/iAIE2XkMZSv
63TyFubFwN8gK9rARSbWEiuzckuyxviAcP7cm6tsPvfQLnyqzC5is3Vv8GNrFPkX
zXigDLGL8sgQV8haNSY4HjeKBn9JwnqZg/nh5Zq2FRJUth7kZXu57KLE+8QmV1V9
tniJ1081VjuqoYYsF0+JpjjVvex9gG7t4L+UAzAGiu+LHUHCLp/aU63w8ve1A6h5
kwt440g/Z5guB8660yhNQKb6ye0d0Mtb8mycDA33daQvs6017rDosjKj4U3SJirq
nSs1227PCg26jTeNxBxHMI6SK9KLPitZKEBgV0g6XYa2pldIC3FAQQ76++AP1kl
ruxPv+gdd9lgZh/uFsr2+Wswr1RBYyMztQbPEXlg7SWQ+xkRZxwK7+2PBLP/z8yM
SffFBZhV81hNG0xuBT3r44kMnFxY8GnzR7fHX55Mr3TCV42q9nX2X0dmeHA+Nkci
vSuD002wH5f9hHNM1otmghimhbWTS/DP92Jq0jwZHQ9K1wH6AJrZ8YXS5xPrf0u
GBMQSpOF3g6nrvvxLM4T/VXVEarXAp2SsVE1L3EKmmxCujqKdEJ+wxv/AdkdIJ1l
kpab9Mks5fZLkpWWW2GfTC6j8FnnRWKc/fn+GsJfWAG2307HYzMT40nxw0JIn3/j
i3xhoYoyoPAZZy6Sio46klwjWfn0XjReW0elgRHRirVwp0uoq2vS5xoFzWTD1a3V
scCei1QcMTvgJkXIDCYG+MZC7TrzNFZf15e0BoX0DnT3FQjQcgxNMPiLCuyQ4rj4
hg1lV2PjIdkz+MV0rrw3fTX31VLULU0gb1obMog6fUGKabTPgB10rBhjJp2luLyyK
K+siCj10dEnEgyGoDvYdlaVuDbNhcTU13kME83+0VoUPFaznTOumnRuVBUXY3scY
lsPe0rHgPu8uhJTbF6/mBHHzwX8EsnrRKCNNWwWdfJ055oyv3NgLSAJMT3ZLOR/l
eUN8f6VEN92ACF9d43j5r6XoeMJJEvgi6LNg+fKdvgebePo0YpN3kdbFQTAqIdeKp
pGMr51BzW/MGg47EAbwQ0d1cMYWCTEjVwhyF8nnfKNCvgVEHcbZ7FNZh2u3vGeqb
zUzDzH7nYtQhI8bJ1Txs3g0jWnEq0K/HE1NtY2uz65q9kbrwOL05hFrtTmsJBBV
L8IUsPy9m4CARnsJ+uZW4rKyw/zZGRmcy87UiCkmsKLumjzhJSPI6ySxezra1WqW
eXP5mVK1KgLCr4yRppfw2+DSeMz4wUi80wFR/mf+q+F3Pm0ZxTU6WcLYo0Q0bHdL
GD/qNfU21GQRnDo3oob0t2obPVKYVCKNp33/A5KwwAD93bu1A1/vQ6H/zdMwxzwv
aqJog/voP8aVQUHx9demRipYqj1v8M023AYzDwVbcidIT2tupNt3HIUjVuUCriuK
ZI6i02rSYN2n+YCTjuaSP6+9GzAktEZAeJoS7L2A4TKlCpXUawo1Lyu6WXiC0ipi
124DZg+ibs6BL8nHv1qy12D4yb8NV5qg/xY/gP/YDymLYGJMiUGUGjt33GwZd6Jd
G0CQfDGJekYYWkFyWDzBUuKdh0zHd8ZVd/swhx82bZz7RDrxYBt1IzU3oQwgvxjf
eEHVWX+NcuameZuhLKahNapl1mQ+ReY3wfaQey3zg1pYrQEHEGtoYiwD0ageAD8
0CcUf6ZqoY3Mpn+qNwX95P09L+GfGK+WLYyoUp0Mv7I1EDYpdQ28rowkRldB+ba
lt2dPacRH0xTglUXz1JzjvqLOYtPqfF0JQtYFHziTesBJf3tlhQrErV0Qb15fNAH
tsp1xQz5pFHTmCv25HBLef04I2Yy1aLmhjREVTs+1xBYFLjb4vV2z1J2ZypXASg
Ydi9XTH49kXvMSP3Z4CpYzGR06xhEgUC26Rjn87fvFrTCchhRbcQkwXtxu56xQaV
qlBMTCIqKtNCIQwCz8CQey2aPkbLSY8DCwi2Idgy11NUPk1UWjgAYbC1oSDvnXaE
GarLMjmnJm26+ckeTbBMZH34Hw47+6YTirY3/c/cNivichCMKpamJcKPWWFXpmps
FW27hjKNJ8Wb1Vvay+Rph0CzL54dntxi0iPcAxeLA6Lz1123g7aUygiZfFrB7VNR
Noh9yUrhzsSG308HvMyrF+iT0srVd/oSQHz2CasCgN5xz6X6defNayLrKwwIRxam
QNJ6xMFD+5ZHV+E9xaobz1BXY0D/NPYzeTF01UrPpd+o/qB8WZ+q1mR6YiV5KxM8
5CcjbWhtSxq0mJXpyzhy9Pau8wVe6vGgGFxFeKPDGxQAoSCOW+5xXlg7r6BljZb
Tq2IIwILTcmJ7p7Y0JmJC+LVGC1YETX+gt841A7wUMtZB5pgg2NVwS5oj1z0HLc4
GF5RvxsCdM1lG/7c/d8WTPSSiUXjmMo1uaoSPT2licvPYYab7p310GIxgokIpAjx
LDAknzbCgaWRVprPvbXMPGSDrxIW6ekj7/ZAl/GdK9wci0E1ICwAoDF2Ku8Y4N21
6QdVQ9/z5pXVAzb1HBURHDZ+fv/4TlRDEbmNKK8bjcUj9EB4dUF7H7H1MHRUAGmj
MNKumY8GdyTq1Q2CLneUpq4YHdkeMU0H/1C20fRqLzGiuQ6+JUz81S6dd4fK4zM/
0844Eeq0p1CtB3ptpK9+Al4jmX9deiVhs9S5rxkRkQXU7ghUC+Ovg3t8bkq+Xdg/

```

LCQAtc98/1GTgYoJUHb1WZmACYowoQZeMHYofLgogXPJAg5rEsdxRuW110Un9GHG
9Q6yG6Qx07+17jBQHbJk8MVxnKa8Vh1IDHyMS4KAuAJc3kG8xwZsPQHcJX1H+S8o
Me2cTdBNFFNkyKXcY514nOK9Leu+tGGsRj0JsI5bek+PKfz0C+U+nUJ238wnNcxe
sIk1j4G0UE3AmFEoaqAQM9/UZtBtAIDmcqgZf1bAHtf1bIwMGO/etFmQzB1EgKmd
5EQXHRsWsD97k2QJ5SqzQs1JTy6HTGWTMW85RKJPwE8d+Re4uZ+uMYOjm4pHV6hE
lmkzyiqw849RIWj+okEH7amdDS0vHI0U8n+hEJ44vUPp0SV9Zjsg6h95YwHb49rg
fg5FeKQC1KDj3NfWy3Kyjcnvb1FAY+4U2tikqVTF6gHuKL14uRqLe6sRIoHcYPjN
D+2ylKgwRyGtvMSJQ2NzFXb+eIz5F7PrqtUj+KKZ4hyT5qI8GL00/YBuFzQtR3ts
HU7A/aICew0fa0hvgTxok00WWNPnYQYLcxBo251otY6eqHWacLqb+0rQyCE1irwc
KqEm5uTWwM70EuUnCc9Rc8P3+78U/zNo42kz8Xmr9QQNA9u09zWKyYCGisSlou0K
eeaaViMiq0iBoq0vCYVxcAPUFLqFa9G1QDKweGeDXcobSI1LaA6F81VUe16EU+I3
0dcgdsn05ge1tikSoBm6350M2bsXUahKXslzZxlwuZC5gDRyHW9mt8SiRcDBw1/k
+0I2G7Te8u8DDYbrRQay/g00dWEoqZJ8HRXSgK4heGd9xtYemfvZcSvLDfSGr4Zm
x81Qix6s9LsWhHXx6EEem6xiXEFg/UoUiqToBTg+o0vx/3IR09Gtm5Nr7Kspt/AJ
RCuhq5nMp3tFWtoCpXem6CC4GyTew4wI9U8sv82Hzu9J7IeZuHwqgHvHqUm5if8+
Z86qkKjfuaatH1EHcahU6KvCY2fKtkw4k6ZZ1gb+A+qExuRVXoJ6l0iuzlhkpJhX
4JwV3ri9SjFND3aVDQnBKNdYP0LnVmJdOea+rh1Gj0kIL4IYa3TQoJzK4IEeQt/P
01/wDTLyzmX7BMTP9KLo1/i08ZberXefIva6CHVnSNXaJrk3rQ2LVfTJA3qE1Aud
BpJIX9DLym5cyCD1AJIF4h44TXo1aek5WUFQoJmNM9QdKB1qwrB+oIAhAwT7Zwvr
Hdt99I98G/kyehjuJoJ0RNVJM9LPDgquYCW1jo1sRxv84cYM5/fGdFoDJZ0T35e
E+0WoNjrwQwJv1hdFATH/TVyqFOh2aJ2AXpkpf76h3b1gY9MhzNFVX2uhdMv5nU5
mjYVX6/HLdS5FsJuaDZa9DoYRqBJUv+2W7sPnf3mCvrzyqMP2IAbcSWOnHKovU4S
5JwF698f/nF2zpuAtaAo8CScF040LNA1WMi0CzhGpaBneeytIUvREtz2zyYMTCSu
h1sP1UFReIei+mAiY12DRVrcVgrgCohoxueJjYtYCBsBv9Vgq1DNohPekjLbC+wd
VsQW0le4xL70hJTREoW4jhoAmip1dZIp7VLNb5R0yXyKdUK+uRsiccZ885vrUSer
ux2LT6mcutD64Y9drHfh1zRh2w0/NW+JqUupsOpUi9uNzMicZMWJm+F6ydwLuIS
1FCR121ku91Yh1bFhI9j84JdJAB1XG1l8gi755w/Rh27dxmj3r24iq4wB90zlu32
lix5u2oy+nSU/EHwbayAtiLeSm6FVNxr1A099xgTDkm80WxCpSjzqznzWffI+uPq
SoqL/FjUUV65GxqmvnN66kGPI9QeX+pmHA9D1sabqWgy2zQKmk5QQfRg01oU+kIG
Aq5U6m0FKBJILTa8gC8h4Hbuachiw9w9wiBFd7Nur6/ZhzZz+CFlyjlo1u+SWfbj
M7mpNDtOfifB14SVjHwbupb9mwaToLe441lHrX860x7MTvR7AJZ4e9ATb5Zk0iVA
uzJilcJbun0sEq4moIHD1Pw4xs4U0+6N7qlupHeV11x9mz392+9RW8/r8nZRk08g
NBr1VhambZliGNjAF7gS+AoyZdSFHvjyUZ8dx0Tw4qEGvUparsp2MKHqmF0+29Ty
Gk0getOL6bcoW29PkhnodKSscod7sk4C70hJBj7RrJN1A5YuwrWzokeD3rjEzqlj
dmRN2m9DQnXNEHkSxSxSckgIeLZVsrCxMVONTCrdfQnKnzZDgtoI4EYFfEE1N6qQ7
v8LtiJyqtmYSPU3c3xb+zsWtElso+HfHElRwsY8ge485xBwtGTGKZtCcxsKtj97X
gb/4pfvziajCLU/MWnE4fzQXPjXk8NEQRdk+EsgoC0xnTPShAnW+MDN143ndDN+J
+BuTpFVF/du0+Vobv3N+3dH+Qd1qhui+q7R+ojXyp516X0IZCKr6211hAGGI7i+y
Z2RGCHIF3AA3ncH/An0X0RHgQi7ZIoSGDoHR2v0b10XDBN1zRXXiVEUGu1XuBp/o
BDnnXqCLT2Nng2tgdU0XvbIfgdr15/zrwKEAbG3yJa2iGsotgdiu1DgU7lftlPq
ftTzg2nvDkTGT86AsTQNM2CLARtAmQnu15v/0o926jCr+471rEXfN6Gm6zkww0AG
ZyE19pnIaF/p7tczePNgug==

```

C.3.14.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
    smime-type="signed-data"

MIIUpgYJKoZIhvcNAQcCoIIU1zCCFJMCAQExDTALBglghkgBZQMEAgEwggrPBgkq
hkiG9w0BBwGgggrABIIKvE1JTUUtVmYyc2lvbjogMS4wDQpTdWJqZWNoOibZbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtatYmFzZWxpbmUtGdjlXJwBA0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVklWVuYy1jb21wbGV4LWhwLWJhc2Vsaw5lLWxn

```

Page 181


```

OTI3MDY1NDE4WjA7MQ0wCwYDVQKKEwRJRVRGMREwDwYDVQKLEwhMQU1QUyBXRzEX
MBUGA1UEAxMQ0WxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIB3DQEBQUAA4IBDwAw
ggEKAoIBAQCAlSn6i8Gi44/oAVAn5GnChk4PHHNjrSfWUnne1N41KImVaTC3D9zFC
rS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2Gmt4jse2Dqs165e
rnt905NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc
1zy++MxQlqdn9WZLh0A0peNZKGMVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhBwDHdZ5q
DTII2PVX1X3K7/c0NxbvBbaU1/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf
58duq/AOEksCAW1b+MD8QH9Yj7CFsmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETWxpY2VAc21p
bWUuZXBhXbXBSZTATBgNVHSEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBSAw
HQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIB3DQEBDQUAA4IBAQCBSXignLEynBakDKU6
8ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsox/Ht9Ii6zyBVZjdaox644
DsiLQEP4YMS7y4q94RFFdmdzEbDLyx9sfUhdvTxDN00oHz53PYDBh4zE4Nar2in
C0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MvtluLih
ne0Bp1GUTkr0mJBol6dSYa18Hw8/ANHpyEx156BJABb744gqoeu9YSHjKK49+q
YC9faFmq+mK80l1h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vRhZjV
D6FYMIIDzzCCAREgAwIBAgITN0EFee11f0Kpolw69Phqzpq1zANBgkqhkiG9w0B
AQ0FADBMQ0wCwYDVQKKEwRJRVRGMREwDwYDVQKLEwhMQU1QUyBXRzEXMC8GA1UE
AxMoU2FtcGx1IEExBTBVTIFJTQSB0ZDZlZj0aWZpY2F0aW9uIEF1dGhvcml0eTA9Fw0x
OTExMjA7NjU0MTA7GA8yMDUyMDk5NzA2NTQxOw0ZEMMAwGA1UEChMESHVURjER
MA8GA1UECXMITEFNUFMgV0cxZjZAVBgNVBAMTDkFsaWN1IEExvdmVsYWN1MIIBIjAN
BgkqhkiG9w0BAQEFAA0CAQ8AMIIBCGKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4
TfA/pd0/KLpZbJOAER0sI7Aja07B1GuMUFJeStulamNfCwDcdKy63PQWl+DILs7G
xVwXurhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCN012
DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtwS1q7ktkN
BR2wZX5TCjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPpdtTMSiPR
+peCrhJZWLSewbWXLJe3VMvbwQjoBMpEYlaJBUIKk01zQ1Pq90nj1sJL0wIDAQAB
o4GvMIGsMAwGA1UdEwEB/wQCAAwFwYDVR0gBBawDjAMBggphkgBZQMCAATABMB4G
A1UdEQQXMBWBE2FsaWN1QHNTaW11LmV4Yw1wbGUwEwYDVR0lBAwwCgYIKwYBBQUH
AwQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZm
czAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0F
AAOCAQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d6
4roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27
PmhKE1oAJKKHDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahixRn/C9cy31
wbqNsy9x0fjPQg6+DqatiQpMz9Eiae6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnY
xs1Fhd06zZk9E8zw1c1ALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+uCDgN
G/D0qyTbY4fgKieUHx/tHuzUssZxJjGCAgAwggH8AgEBMGwwVTENMASGA1UEChME
SUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBSZSBMQU1QUyBS
U0EgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6aqdcw
CwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHAQAcBgkqhkiG
9w0BCQUxDxcNMjEwMTcxNjAyWjAvBgkqhkiG9w0BCQQxIgQg4f753q+skjOT
bEs15q6WUySCAbgxtWkn7Ci2/Q7J9cwDQYJKoZIhvcNAQEBBQAEggEaiUGuCHAE
JkzXXnkH3k8yFGtEkkMscuC0JOPwqnxHzILBDYt9udpeParT/dr00VgRKxCQ0mxT
sz0D65erzo+ZXfuXC5+Q4hzqdNkQhC8Vi7H2NL8KLSBrXNLZtG82xco08fTKTWVq
c2HwuAPL0+Yh+fTfqr50RnJvPVkTx197KxTA1YNQh/s+Uuacumnmr/3iuHwjubd
+iesA8wZ9RWSmeg4FGUzaVrTRIhJ8p6YQQYJc0omV9GuRbjUzMTL/fOB0G6Jho1
aq6nGVcsoVTMIrH8nJv54eHQtWtYFBJI855oDbkIS4DxH0WR5121BayRN7MgC6q+
H+cJTAZUD2IF7Q==

```

C.3.14.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```

MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl
Message-ID:
  <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
References:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
  <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:16:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: References:
  <smime-signed-enc-complex-hp-baseline-legacy@example>
Content-Type: multipart/mixed; boundary="63c"; hp="cipher"

```

--63c

```

MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="802"

```

--802

```

MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
  hp-legacy-display="1"

```

Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl

This is the
smime-signed-enc-complex-hp-baseline-lgc-rpl
message.

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy with a "Legacy Display" part.

--

```

Alice
alice@smime.example
--802

```

```

MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
  hp-legacy-display="1"

```

```

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-baseline-lgc-rpl</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--802--

--63c
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGGoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAcElEQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--63c--

```

C.3.15. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#).

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 10445 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6716 bytes
    ↓ (unwraps to)
    └─ multipart/mixed 2273 bytes
      └─ multipart/alternative 1116 bytes
        └─ text/plain 379 bytes
          └─ text/html 474 bytes
            └─ image/png inline 236 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";

```

```
smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:18:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
References: <smime-signed-enc-complex-hp-shy@example>
```

```
MIIeHAYJKoZIhvcNAQcDoIIeDTCCHGkCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIEIcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
BoQ0MA0GCsQGSIB3DQEBAQUABIIBAH1YUDAZJtrARL+kRtiQU4vNChzIMY4Kq+ga
tvbsejCyWpP0J6bCjx7IuyFyTQzpi/rkcBdyphDz/sEzyF68mAtFvGBHhV3wi0Bw
V4+TCpXHio01a1fDbWQTMIRhNoT0CwkEq2AWzMerj1Pk1YGzRWQ2F8v5conRtN3l
guvKXr3vyaD2wbq6UYIw/x16vTfEmqFvNRMSsdWdqjVrrPHTTVtUI5uBhKq7f1C
dWt7nV0qTglW8WKB0qgABKT6E7PqafUzXMBu1EmjFhJyNP4rrQYnY97iVbPnUyyz
SUUb5pLZ0aa/opENPk5rhCQnb4eEnbGS9lu/dE+6y/I9/17eGFowggGEAgEAMGww
VTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAh+lzMZeSWj2T8idRFSZ0oV1
VYyCijzcJJEp4Mfq3Ta/ln6Z8wAvgJAuFaph1mMGKX1iZIN48te6SmQ82IyBqvkp
m76opxs260nNZ1sVvwhTIWzQjNUY4sxTF5UDTqKuLAcr0BPTtVvgsJtMi4rWDbW2
MbZSy+mxyEWldkDZ0/2BXgEVXNmBgJ5qUUMF+31WixM9Y+iN9kF6194V4TbBQ9U4
fksuKQliK+e0XqaZibATxgn8B4arubpnHFw0bjna2bMkHmQs/eT3VEI1RSF4Qg3p
FvDzXC/jHqrhbtnQkR/zY8bpNDFEiBv3e+myGaL4CsnU0Mubx5tkhP4IzWXwRzCC
Gu4GCSqGSIB3DQEHAAdBgllghkgBZQMEAAQIEEBjNxqRyzAx39GzHbZ04Cw0AghrA
KwtFLWZ1Im0uhZJ/SZ9TDEQXGF8Bt5WnyCp3PC8m2ygyxoui8y0XLvH/X353IQzhv
ituNjd5CN8m6RWSHym7NGYwifFciv/usZk1/pvp+jVzvFW/GAaea3oyksAYJz4o+
y5IG/TfykybUNyDEtJ3kMS5D07rbDgGJn7qoK/7rEbTsUf1NSIEDVkfM8SEHK0i
WdwV8u0J59d4mx11u0BU7+V0VFbo+YVPBHuJYJz4U6Gp48Tu3IdAJQS+PPmY6IEX
+3rE1+jcf0KXxs7PRjZ684uwteMkekMEehxNSQg2HJw5W9hTtPI/qSdCfx1egfR1
+Lcj+sLi4fPXK8cdo2Kc9qGiRci4PRSLxsNCRX+Pk+YrhE1/L1x1Q+06GmVR7XYc
fU/SOPL2L04jFToHu27NF11T7s4diVsWXl0Mn5umgo+c0BNGdAM6Thh50Guyg0lQ
xI0VvwTbhNE6Cm4g2okhIY0j/Ko6SludZXlHCCAXsnG+80b8If9CjwVkb1dv8DqJ
81NPoiSaJj5RCbfNy1RE20jLjkAKzancfCXIzuBuReQaUnVKAH0h6Aj4ixx1awrX
F8hJm+iWDrnGhkb0zsgR5n9z1IagCfiS6JWZ+N/lyeoeTuoS3dNPEw6wUXmC5h0
oXpJHD9URu0ScbrQLF5Kx34B1Ppk/WVRJLxbSy72sm+7wEHOC+Ft200KofzJvZ2N
Vu5f18qGj1Y5mJl7/jNVR6t1G4bN5wNIXZbdVeKWDvvp+iCFXbB1hsu1M3x9Dqj
zfzfTa02JlPHZhtxNyw0a00LFDQsblYVYWLAKG7mq34m4jKSKWINnbkaeMo0xEN
l5QxwLXbgrE8oeYifgeEsdV6ep7jyGaLF0qU5qXh5PowHiXAIWQ06FI2VVJwmjST
xmcm8iX6sGUffC+8C50li2T9whpk0j2RUx4udm2e29TAwHgCioUwwwKGiws3Wusu3
fqhYuzHCPXqpsfuJvt6l2KUqhAdrdPOYQNMbef3Pyh95qvHctln/pNIwDjJHRC
w+BjdZcDlv1X0rAYid60xFxJL5vjS9/NLG+TD+G3Th7a+T0ItNk7RHjff+CSMfi9
68ismududaCBb1okq1yWJiQLxSJ9ozQnwC2Ic933DjXnFkw6PIgade8pNM6TM96X
NmN77vF0uKCMoC5MRGk7FY2h1iQ/w85AZyUL17BRcUL8JH8zyaTMAZAP6Q5ejK/
XM01usJFBjiD6xVtMeqz5Efl8st6J2bcC8FEg220EQELere/FkTw69i5XZGBZNEa
nXy0zF3wQUuqjz/XXH/x33AEvjUfbkdJRYqPQMn0poM5NplvS7GVaii+TqdCgd0u
T3R0u8Tia6tsoWHMk7txFQnAVVOMij/F97vJQZa2ts3WK72I6S8zMpkx1kXwzwhq
0v7ksP7t7lfrNHHFLSc3GqzcNwejgstoY4sS0JEUInkqCqAX+tC0wVmLGA8IfhjL
mYhFxsUazeWwG/Q9na0ynI5X3z/ccLaUYuI590SmGjYaws5QjDj23s680lSEba/
aNF6/7Y9JidaDBXqFABRXlrrCqZ5l00wvWnuuPX8daVas0P3b+5Y7YHZkG+6tEo
x9BhJ1ZpZbMpk7SxMTIZxEhSq3jjsHAuISce0P7FNWvnrrQKuLD3eV3ywqrXeI5W
8rEukobjQgZrk0PPpHw2diFf1bk7YSfWFNk2iD1x0o+5Bsy5XrEUyrACIKzKn8cT
4jUMw/G7hBQJdrUlcsMtb65lEGP5RSjnzNF0ksBYM0+Uh96xPf5FuF6B8I0hPrtv
HoDsypNnLNPLxc2I/RjjiJr2rc2vkJRwcnG/x2F8JztPwRrSQhgKkopaGkTLY89h
Dd9u98WAepIr9Wj8DumN3a1fcrsDcDOL//TuSepd9juMwKkTthvXa6fRcjJ2oxNC
```

EZLtwLh5wkfF7IdtNVGig2W02ykfDcCBq0TBdcTXTEJNjeGDUhAXFRwYB9rmm4nk
HkxXKyH2sK3JiUcEGREIfARSJfxAGU4oP328378006QvIoHGHgIP3DnsBMKs0JkU
2KbBAMT8T4X61x2Me76idmwJPSP+hnE4rPw9bKdn5u9eYlU0F25VoZgln18qJq1b
C6brgQTszKSHlgvy81ug/wV3PCpz6L80xW5c5J7ig+OWwb2tzfLM04F3Tvssqp7I
MA8JfSHSF3pgSuEGenTZxBpR6eTo/VSEIE2rPrYKik1D4MxNzuU10uKl9FCYkwb/
Lcorm60hJOPtcvYp1iJJx3MRtnda1HNw1lMdVXEbJErpKxhSW/pgaRrCdX/I2pr0
pZMthLK0w173HAWYeVvGU3scA8mI002KGGFCGJvp4IbbQ4nf0f3M6hcHqsum6cRe
LgB5e02U1nA5pKR5iWAIkmXWUTfzCZuYA0aBznTvA7zHNNf0BkQWKgieZjyckVb
8YaObWSsr98oha6hU0PCfdBtajXL2JrphGXtBc1DVLl4VTgy+c1VYZAXDdiD90v
KGrXft03xo7cU2TIcFFq/ZbjWJud8Aj+s6jacBjjYoLuNBiNyWMVINjDviHA34rZ
XSEV5J50nuQtFUP8257z4UCqwk+ABJRW97tMx01Lo3sC0i+Pyh+c2CdxvUF0t29i
okI9N5cc2aatwNHg3mHgkEhViDuHxF1v+WFFwjQb1tIY+amUDZsSnTAjXuJ88tAk
iuptLA07DzBa1Z1CunbQwddIgrYiKrzw1T7b5Cbaqpugg6V49pNNkXEtV0MIxR03
QVaxfFns/ft4dXxKEBmWdj5AMekWDCG699IIAtuM7AYh59g/qRnpkZSSBlUUG2zS
wvQi1iUhK6U0Rf904+cWfCivZuL/FUAToUq892VsVrzZ0beyLtqxGAM3yf05jPpZ
yStYhYt1HWtX7v7jd6Ni98dNq+3gmfpq9z779aTxIckL9myqTNURGjrNyXf9lmc
qauyW8MagYn7U/Bwtax0h5qpjLqcmOPUGo/TmPmL6MN+znzxRLBsakvDNED4tARq
2QYkoR8HLKvbp8q8XBtf/I/23S1qEnqqprnotd0oRgaJUw8Z/QyVmwC3oxV1VQYV
c4391fZLwnVbky6v54ynmtjIf9HLNCL3fIA3p8DF1mzGsZidD4WS9WCiU0x/lRqT
hu1M9VMtKo01sCJ2u2cmF3aYxTFbFH4j92zXv9ugW1EpY75AgyklIjExyITYUQdq
PVLPSG8HXnuoupDb21hx8WjIjCLz5hprxKvZ5UimjsAHb2A0cpIyhx8pfiPohDu
QL11dDHLRckYPBBm8cAsIP3NAKb0cIk66q+4xMPqxEOd6qXI0yUW22dju42PTT8+
MgpMRf7I0j1J+cLoE9/QUcXCTxHOAbtQv708dLdfRY7H+Ssci6BS40G+SYpcGDTa
OTJluDN69HueqqfA4iCCJm0Et5AQ5wyCx492pwxNyeUdRxs0PMfiDAyuaAxQuLww
25u6R8adQG1x1+d0sotRg96VBNNGw0T6Tx4CFtu58CIW0Etd9m+rRoyKM7VodxSs
E0Wdga6CW13J00lcm72S5BRJeBkhDQ446suFtiqjMJhPhS8nctY8esx4wEd7VhF9
MPmwax1m54LjkSJQ590XtQxiw+yQbep6uR4AaE2SMktz0TzuPtmIL1Hb8njC8GCM
7bDvosP+ja8fjF+hAw3Cnw47itF+ZmVGxsWmmt+RkiQo54+4uZ3Xi3IZm2/AM0FY
5TDELYiMK3KWai28NanThHb17mrKrJ3Y4LzImYW7sVK6Lim/lQq2Q0wTFYs9LYBn
fRoFT0NuVtteN3eMa+ERIKCVBdunP6c6uff40ZL/lTKGP0gko29f1EI13R9VH0jY
Rvq5pa79y5WkIhPUngA2rmZz3IpREvN6wE4c0rix54QBklaz1yW2LMVYXnI2Q0x3
ZZgC0hz0xjYqY/YeloXR5pPz24CJAbrMSCqAhtohYDmkTJUv/ov5YKvE8IbDvUVu
fI29aQ7vh504eAKG9HVK8nNV2GvuM/+32LP6alvX+yIUKRr6BLyt7H6lw76E1BDk
pgxMmU1EpPaSo3BTI8eALDTBNLYGOK98kZqXemnrYbVAJgMS2hUfeyZim8tFf5Ws
BMKOP14SoK0Emn4PJXV8A/2XMsYpTzZ9nWGx25HKaXhaAIZGaB8D0Askil37VhmK
LGe7dEqg/CHIS0ydVC0CqF0dsIYVqpCzp02XpbToS+kNoY9T430bUwIq7rdDRIWx
PUkgE8AIP0k8uqI6wCeF4giwU0jhJl4K+ein293xEwKasXD+o7HNcyvluFt3g8F
s0eezk958peq4R2Jm4KySsu0sPfeq8YXpbdwpZjXRkK2sNQLiKLmBsrTr50tJoQX
Paaut5ZMi63Pln8eWMfIFJ1/7lMDPYeTG0zrbyQXg+l111HKgsuBkr1N5iZcuCvk
sNgGhW6zDpWf2IXx0nAdby/+6ZvCh2PzT094n9y5yo0W0UfoUK3RxHfleEcsdHq
3X2/utJZhmM1W3HPxyW8C1pDxkXKnTHArjRVmu3zCcUbeEJEGc/c9pmyzx0Nen10
2yfUuM7UYk0sLCCmQy+8UNt0eY373e9RYx/JtRSnYzRQT0I5UdSGdug8fBMc1wkX
dsKLO/SP/xXo3J3ArIPesF+j8hSJitarYc1RTpcSHuqTZ+QbfXB0fqXIV9KJietb
3ufjGwvYIRv6fQ81rICQW6TeCRvLM8cX5PtPiEt1rQ71c9BKgpqgxt57nsd5b4w
T/nZ7mM/ks2m6N09KxZ2H9QYSSCo77MbQCbxDvXhRS4aDUec1gkTQHLsdJDnpRSf
n06JxmqSBp90tJ+LDHS50G0Rtlv23GQ1yrL3nWnL9S6s8ohFGlokN13tgWYQe8Ek
YwZiyGw9Dz61JQY06QWKWYkqfb1JZqlmoZPxDJY42PqXz5gczGTyvorOXkapWfVz
150JeNPnQ7dZVqECSUh3dqJ6LxEPYTy703my4BPIJLl+ImT6bhFDieig7cf9oxqR
ZXeSphW61KYyz3yFpQ+51E6/ebZtejvIdxn3YC65IogPRgdNmrX8AWuzQR/SR5/6
oi02YjKc7BwCaZVTcGXHI0YbZplraACMCrrgz94XvbaPZ3WX7AbJZmxekAqMdQR0
i/OxyiojevnNhr1hfBTCagGJr3UiTKnQzYFBp1NphHq9Je45v78N8A5ZjZQIEthg
pAPu9ZujQIEGQxWKWfsWIAKEmVUFiQ+7WDBf8G0FCRZLqUmitSNP72q5r6Ao5QoI
OKjIpF+QB1lhqQK69Q+Td/Q/Qsx13W40E5p+1qZNhJDgrYneZBxwNy3BU6GXQoCI
gxiAonb/XB33G463hDEui/MbuVvsM0thgFgvzko6wIIicqrXYbjKsubVKeCWMS2/
09XDeJeZjc2psmuUi0LR40U+7mLE9YhRmITxkzt1L8jJigSL1kmyTMz9EXHndIXd
7KZZzML0gdy7z3KaPQyP02huJXjhLM5+Dd/+FI29S9uMLAQRXphJEsKHpnEtK6D3
H/5rYHV+2qWYEjI0cPnf8RzYkK0H/UI53zISf/sFC3zbbMNBC3+SPH2K73Ejpwaz
zqkYDSWy4pfEn1+maXEaUbbgZsCEE7Jktj2TS44HvtL61UiRnbcPbwEZbn6PMKre

9vBpBrLJDpmIsbc6dHMnSG16+b/Z72orc1933yBuq98dZl1m7V4R0AqWHrcH5Rx
oXn5UpvZqLWU0ounqRQ/DPnsPTPV/6fsQFu++RfrzkossP8Ukiy5VhIQK3LUf3J
PX+htDhQZg810yoPqj2Sr3tTeYqFeIefaJ3cJhp7YPICxJetCXGssGn0Tt1/b+KK
ZHpaLdtDehkX2p/2+fhXV1a3QQ7vGXyK5oHJ3+FmGatoLqpVL0eRjRJT1TZA3Tq+
33y6gb8svU7v+CkDQXU3qg6u80LULvTilXhfJNStVwCsyTnY+K9meirGTmdvd1t8
08oCjTN4F0JpaXrfvHwDR+4anTnvEsCUsF0ECQ3a/SrJbHP4zCozgNba8utPIf8n
P4DDlFKeaSVHr4KHS4hsuC3o4HSbFv0usr+aWZjsgKb0yhPKn0EwiurwbIS+CNiJ
Pw5ae7VSytlPmC+WfDyRqiflGFJHBTigwEdDTnuKsrYn/MsZGrpUgx0fHFMVBv/k
Avh3IBP3ky1D+leP/RxkXwv0iyxkFsAF4ewm7zq/Qkp5CYG38+vPuf+iF7fH0aOL
kk7GonZ69KvKBL5YJXr1oWqs/SQ2SJ8Yc/Vvj0aDb/JxkvRXlID0ymvflWL19K4js
syVaVsJn43hAP0rHW9atEYnvjU/3qyWSoq50Jxkrm/pgLwzTWo17t2V16uwnY97b
XVu2/2L/R/VXaLZwT0AqedQ2Xow0pn4qwpFCkvmT0Kci+Zxv5M3A9csSXjciW34Z
Uk7b16JYAT7Bug6zPtFFco4u2n6AWOr4cBY4uNYb/PKNG5C/4gg+LkuqffrfHb6
OdThNppZ+F2KgeyYHFaKbt7woVfAnQQvEETgDPLPiqcRp2mmhAzN8r2Ia2Cr0iSf
5fhLHnZVA3QSKMIyedXfHdFM025ibApSM89IIEcwpNo71F+APthXCU/9C4fBCYim
C6N6ORb8T6m16C2rdHGfndZl9pkPfTQtNkTsWE8fP6LwV0V2w/I5h5hWre6Qpqr
jjDuIMamfTniV8RKvtXmXTzHa9cdUnqOWczpnzz+8nLB5v0qh6McrUquSSqxMhMY
ZeVK5hMssM/OkwcqMFCxCjZtA0idAVYkuPdQLR8Qw7Vw99BHFSV9fI/NCB0LXIPA
NC3nJELTq21ZI+/EHpIKrz3zDU+oV5ipm1wrFWEGcjSzbxA9+1vvU5Ra9P4tV0xQ
FfwQ6mojU02Sy4p1vQoaRhDLAN8DPHHFC5AU6TNMxka260UC9s0uPIRIVFcdpqbX
QvnEiHLNT+uGt8DKhi3sb/T4GKUlcxCM+QLi8I+9a0sdHyiWGDm4xb3LPrwPh0U/
yHzOQSM0xwkCRai/WEROFSEP9weogqu7uIrQBmwFkBQUneQV4KeskD5H+vzZWb
opx56gTQRaACZpLCTn0jdIK/Iieeo8xy4h0AAs/nV3s5Qb2f9e15f6EnYfSiWd9X
dHfN+0txgDbqpUjRumoyM0YjuNFwdTxnz8C+YCqkT90f9nzX7+bIz+Bq4CynvAE7
W5Mk6JRIIRcCwwwX2WSMX7RDVYRg5F+gxFFkxknOZS8UFbAvR/jkwVjjPEUS1FIm
71EhZW7vLo30aGku7kNiitTeW2qRHD1wZq+aoPG835iQLWgdH62tF/0tRUv/qtNG
Jox77mnuq1iW+I1FKvEibrNH1CDipCDE0D1+EXe4iA0Ux/00jKV4ONKy5eDk/t55
dzB+JpeHlAs2AUBbQeDwKo65R6s008JC1PbiTXVskuvjmFS/8uzkDGc/JehezRN/
ZHg4TI47xzVwKABMS3F7nPYWZTKy+jwzdPmueCuDZsktDz1RbgIdDR3dNg87iNTf
03XfznIaTKplEqoxRMM9Q0LjnzNoDZtPOnWg4awzg/7aNB7BjN1IfX1KV7H50d3n
RNx7rnVEFAx57JMTFAJcK+Uo4ibci2dMNqM5cpAX9LPBmsynfSxaTzhPWEWpPQwY
SCGCmiVvJFG/TbSCumjkIGBXPsJpPCJhx4d4hC1trjq96VjYkV09N20P05JK1Ro0
az4SI8kqj7Axa5UffxCpSSfbn8ehp78IxsxMG7tBZ0AEFVJV3679zzj2NVdhFNb8
CkmHo3ya6bdZ/NjdSy77Cd9Vt0jy912g4X3/s0ausdD0ZorBTFTU1VKupLDo9pQb
C69iMim2eRGg7g7wsh9YQbe809hwryUEtDeeeIPhbE5gEk8xjP2t101kmpk4ViRW
FKaTu/IKsh87trtQE89KCTppUDCEy6N5HEirPnW9vEJo4qRQZ2ApsUpnVYD4kR9t
sME+PuecHiRhqh+dEo9EHHdrhyu53d9fCcGhbBfNWy4Sf3nCnh05hzzUw3fcpW9p
7GkKl0+yWcpxc1f0rvuq00AnQihtlCQ7NydQ54x3varOZSLZ6dopsXnJGS1fawI
GUKl06Cv9Gd8G6ZsMr4bhjyD2prNnJpOcadX1r+LEkfX44Xv3EHge3J9enOR+fMZ
tVQriToOEMB5mfEt0P07rwfDCiGXkAZPCukMC22y7Yksqib8o512oWcbx5l+FVF0
tfmy+c375n2x+wth+SPY/LarQUDs01V/v+NC6u71TjyMhqkWEGDbxtDq0+hrUkqG
B95VNgIGFmdvV3+ILD13Hx/rAf/eMfadJ5F7Hlw0jdXbnEQsYXkwtX6U0turVohH
lUFqqjdsECXP1o4QFii0+a+WGfNEY1KafnBYBbVpIouu8g3SGtHKrFAPxH7i4uFb
nCGXYM106HBdQkF5IHeVH/Sh3iDPnK8ilfSUXIbo2QiFnuuvb280VD1hDWys4q1Y
82bQdIQOz/YQkDNmUoM09ZQEtrZGxGqqyDrKtoeGnuItavI/oQFs+n5f/p+B7ebP
+Dq4AptNdZliJTVrkKKw0buQJmrcUvWKKxkUC9/N5DeNVV7yVuyVBUOk1Q9Zub8X
SNfkFDZ4I+CfQDrN9YedY+lAMjcmiYIDn9s2RmYnGgAVlYweN7y8hE36sNAxDUKq
AEgC8bJrTay7axaqj2m8c/F1nXzmKBn1+Q4zSW8oeNjvfSpfS5ZeljHnyHrZrUN5
fVyet/3gok33Qqh58j2kXSVGWJrtbsIk1x5Zu2Q+QeUmMykA21tAe//NbcRm5NzW
fdAyOP3IiVpwp6w0rtDxyBeDDmPS6Jkthp/3A9CmD7jewnt2D3f90G1jLZI1nvvi
VxqKkC+yHGxYKc1kdvZnkoVPS5sGA3STRxzWgffzZ0rnvyNjKneokJY2CMA89A8wm
cdAbA8WTxolo70bjelyYipGb5BWUqWvRbrVUYS6lrgLToUIfVSS/beNyjwwmjHgR
C3a2iQQ74kYyMr1iBj9K0cUeyVSBHOMvWg5Xv0Phovz6waVZdSWOcxjDslz+Ghg/
c74x37hFQSAiIUt9ZzrE569QNP6wcGe/S0MxL5MG6bqu5BH8MGrBeQ0IPRCwXFWI
+Hvwh/mIF5Uc0hssRDYNn9YxYA0jCLsjpxjMcDJCMUA=

bzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00v
dWxpDQp2ZFbMVFfAMmtERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0KLS00
NmYtLQ0KoIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIHvcNAQENBQAwVTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGhmaWNhdGlvbiBBdXR0b3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAOT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDVQDEw5BbG1jZSBMb3ZlbGFj
ZTCCASIdQYJKoZIHvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLoAJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAaA0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQMA4wDAYKYZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGx1MBMGA1UdJQMMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUv2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTgt1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKGD7QGnUZROsvSYkGiWdp1JhqXwFdz8
A0enITGXnoEkaFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHuz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBAQUAMFUXDTALBgNVBAOTBE1FVEYx
ETAPBgNVBAsTCExBTvBTIFdHMTewLWYDVQDEYhTYW1wbGUgTEFNUFMgU1NBIEEN
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOfoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEK
AoIBAQC09InoWDGWPk2af0+StijsNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwOrjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUBYQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbB1fkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDA0MAwGCMCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEFv2zLItHQYSHJeuKWqQENMgZmZmB8GA1UdIwQYMBaAFJEWjnwHFWyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjD/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENT1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJntjh+AjJ5QfH+0e7NSzNnEm
MYICADCCafwCAQEWBDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTBTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpq1zALBglghkgBZQMEAgGgATAYBgkqhkiG
9w0BCQMxCwYJKoZIHvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjA5MjcwNjU0
MC8GCSqGSIb3DQEJBDEiBCD0vcxZnCxjXaOpfz5cIo9Maa0SVODPCXLJlV2Wbq4Z6
7zANBgkqhkiG9w0BAQEFAASCAQB3m6q708hB5tmuz6jzSJ+nCR7C0BRbfKypEnSP
k2tdLa0AJWRhQljSd4klEJWy3x2SvLL9q+rSbmIWpK34PWVL1E7gbbJIBjfp0IUo
+YMSIkhKFakFugulEi0zQG/HgnMENl6CDXa5ZrbW53SEpNpYgchUcpg6Z0y0B07
oH7Y0qF2111RRSzsJNMMDAm/1LvOFBR+nUERAHhvq1dpGpNuvbtAh4itWLLbDL1R
gIvrihHbqaUhf4VDQNg4MWjdHGATgPHNAb4hpfaxHxGEv+NYB/65VQWKGKMUzjqk
aLH9nVThiA1E0yirAA7VlmlvLUQgBem0pjh6ixnwK9HfPb7pG

C.3.15.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-reply
Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:18:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
References: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: Subject: [...]
HP-Outer:
  Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:18:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: References: <smime-signed-enc-complex-hp-shy@example>
Content-Type: multipart/mixed; boundary="46f"; hp="cipher"

--46f
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="fa5"

--fa5
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-shy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

--
Alice
alice@smime.example
--fa5
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-shy-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
```

```

envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--fa5--

--46f
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGGoAAAANSUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRu5ErkJggg==

--46f--

```

C.3.16. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy [Header Confidentiality Policy](#) with a "Legacy Display" part.

It has the following structure:

```

└ application/pkcs7-mime [smime.p7m] 11505 bytes
  ↓ (decrypts to)
  └ application/pkcs7-mime [smime.p7m] 7508 bytes
    ↓ (unwraps to)
    └ multipart/mixed 2832 bytes
      └ multipart/alternative 1621 bytes
        └ text/plain 576 bytes
          └ text/html 748 bytes
            └ image/png inline 236 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID:
  <smime-signed-enc-complex-hp-shy-legacy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:19:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy-reply@example>
References: <smime-signed-enc-complex-hp-shy-legacy-reply@example>

```

MIIhLAYJKoZIhvcNAQcDoIIhHTCCIRKCAQAxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTBTFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGlAuaN5i488nW0BLsFYGGzv05Z7LYU/2JcF
bCWNgmWkZXJg15jwdzYH+xrTDHmk3Lm3+zgK9UoV+SCIBH2canLBrEgBk7KeqP6C
XSZ5q9yXGyZ+CqJ80msjvhezu/F/WR0o1CP/ALvzwu3TM1C7WGX2VId+dkYbJlqh
84usiISTo1i4K5GBGP5TwCt40qFNq0oiCh3PMUyZQ02RxQcvW031j8J7ASKxA4gl
ilSjC4Qs5kf+TEUc+iy1X8DQJu5t2CMmvtaBSHCB0kxngQLQC78JQxojZ+xEP182
HHqi3Mqd45z2mR12GuJaMn1W/OhaUo1Y7AgDOTGDIY+8QeyiFJEwggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvb1BbdXR0b3JpdHkCEZB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEADR9K8p6a0/i4HviQ9Tt9Pb7R
NtG9AajTJ6rALd1mRmDlpwQjKLduufYKBCxxB60LkiTUXGPddtruirSbEsj0a3cs
ueHgTUPxC8z7Jpmjk0ab3pgilymcCB3ajskxKFCN+kssejHIc/fE8KoJ089fYMjv
J8BPk6giYB+FCfz9FEDGXxWjU40QdmYRQlhRBHmaF7CIpCyjo2VnJJlp7STKfAe
nKbbEbB0sFfw3U2F2AfEmobmNixtNCaNFbdMQLV/k1+oGuAkkgZC0+N+sSfAZ5DV
ZQvdd5ex51NjMhSVh1qp152LcGbtQhP3q0hWaqDYjmd1P6nWP5/PrFgQj0cZBjCC
Hf4GCSqGSIb3DQEHATAdBg1ghkgBZQMEAAIEEFzxfgxbma1kU7vL68qwqfyAgh3Q
LvLr/03CJmjsYS/t5iURfgrocyJrvZk3RW3i14gxNLDFElcTKR1fCuUGnaV9irYB
A4FUWY0QR8NUPbEihtDX1DuhfIR9bzG05am3GdoNJWbNPEcC9Vta7Q1DWjFzXNF8
NJW6q/SlZ1mAQCHq8p5dtBsRWsOH7gokScgyB7o0XBHnOmQ00bUbJ9WcIbA8FNCg
tJDPxBTl8kDqduwhStetZw10HrXspvSojb6+siJIFcah2p/hFc0Wxf0h1sz754wm
13q0t2BGGWippELLS9Xysuof+zbmwwA57FkJP53n0PsnKqhvKEo0ZyEMPkKu5z9p
XN40X/3PwrBxo4HoHut/N3HNwyJs7tb71/8AbmrT1tAAHUhDYc1dCpza8wF4wGnC
kFxFVOE+3rTKIZdTMndywoBpobY8KSLheKrpRGaeBv6QnFavph/1w4sd1EPGVA
CXNn35GjtB5bAE5dMkxbrEiaDi3DupuQFSxhNWzBPLVILWxBnjgDWaUhfVRSx50X
MzU/GSefZ61C4eynr9KG3F2EiRm12yNj/ORLZTm3dbfUxSp+mR0262nkj1UMcyLe
3eTwXK5yKH8pMN0uQ0PEB6CGJY19I5zryFtdNb5BaPNSGznwkgMnX4qPEG18UX1q
yKfz/hjcLXYyYbM4ey/xh3uDRWXPXAtMnJpXDyvfDMSK/DaFI2eN02fdZ1Hnr7xD
MRAKRFGR0NDirjxjYVGHkUeBCn9H+zz6bl0HdcNM132QtZHSYhIe6PSvmybZ/0F
R2uqR2uEJIFtoPAA+0F5hj26RBAoLeJhGddyvXfNp0X0Nun8Fwzpsjn6nPwoyPN0
hedCV10i5XCuH6J6ShJD1etim8A7dxKduX61p4ts/SHKN2wvnp95zZExvy9L3b9a
m/eWq28vri4i3MLcPbswFWkjBkgZ1DPuwwmv4c+6NeWyZSJMMK6ftZDuAKUfHwVR
VS+PHx4kT9vwg2KSzJKkbt9IaYDURNbGsPJbZftigBS0z267GG2mYSjasSxv+uUX
bLkgoHEixJuUbg/Jvsncnby7JwJErgDnLN7S2ZGLyAaetyWBDWbZYFy0SQX0WrfZ
hEzgZ/F7oLfAqD9P50+I20Sx18tHVCnRrAXaMU17I1EARminSw+G8QTS0v8Hd0L
EwwpYKZMmaXf87+KApqYTYK+fv31eI7qaBB+8Hxia26eg9xMa/eI256J8MGPApTu
3cwKCTDAG70GChrSIKZQJCNBZnbIq2gYWAYF2+BEVqsmY3mXXNcAuPxbC4UUJQJ
1ttVXZJpDrHqOrg17ew2WzNTnVdPwvQLxSJSZpA1Yx7xnHKX3+U+MzLXfukKg2E
LQ203o20Y0oaf7P0L7yg9X0A/qi0sz7QaNQQTaG49M5G/GIXy5YifzbteZia62RQ
GsCJfD8pibMs/rylN0kXpCXNwc5+gVJeb/9pAz+ZaAH3Bh8iHKtS13e1DmudMcFw
/CnZiD9e3fmFuYZHAMQT4PwfRCz6VczxsJhNYTURJ6wiqybSoDXgXkHrx1jq7ZA5
LJmpXcSxAWowgMM7bs0eQSzDCesSCFrT4AdsT02645pVS6nZex0P4MB0X7TPcB6x
6ke1mj53tpG5zYlBon1A0tWz9rNPGU2AGrOuAMgotao1+q8Nq3r5bamJ7idQSUzt
0w/vujhPnKU5Wt5XXBDaXl1+H5cfawdkDh8M+eaI1nGNQRhCI8+JNcRcLLMiZHD1
rcvKx38pksBWL1Eejze9y64GN0iA01tCdGTmIorxDjIJToeS0mqeDHTIiqFH2qsVA
O/zUWRE+3AnXrwivGePaCq9p0+ir4D/S8oZG0DJ6gQ29apgUJR/AxEd2w3g9vGC7
pnIp81vjZord15aGzSuM81+uk/By4PQ3kZm30t6vh0+/bSZK0VVo40w+wPf0na4F
Bj0AJi3s4oFwNLNq2qybjuEtS5ufImm5c9iA0+kIyX0MsLLJA3WJph0Ct+0dE73Z
89362hoH+JiDlp9jvsuECvaUIWss5Y815GXrmtVbk4bgvNLX1X8619Bj1PkMbMJj
eYst/uDoOYth5VSJo1IdQGxznCXARz6QBX/UdoEqMNzAM7VOHOK2J6Vpvn+WHxLW
hrIx6w3nEsfeikCm8s9sDkbrgJwmHT/WQDzffArAKuRXNczJlE01evLcz0YKnk/E
/IaFSs2dobuDDUXklmbxXYOW2Vk+VMt+svjEwCYLXp0hghufN1HIUqG9D//4RiB
/jrJ0y8ci5fn2vM+czragUNNAusuCI9RnPgSyPHLwMyAXLZ03kWFtB680K09cT6Z
k1temLL700k0VBU4411Sc7S568kYXByU60JZtbdwnChId0YTszQ5cq5P/3tn1Cbw
1HFc3yvlW2CLOB3wNmXo2jOmd48R2kmzV6Mc/C+P0VxIW0hh/gcVqt854WiQxVw6
a0Dr69oj59o1H/bPa5wVICK0+3CrucfQWLi3eRntGnQ2N23eZWFeyDZ+U63SDyw

Iubr9tRIwZNu2kvf2eHTLoLswoTF87SSbcHbzwpLeEbp250HodTkfl0KIAxcZMe/
zspTEUa0BysL/0z59X3Sk7lei4qpAP9u0GyvqK9iQw0N+G75v8VPWGwYDTsmAnb7
x/qZOpX3MS17i8f9rI75jYUpmU5l+HbOrPw6cywnvGKcjN+ElYE+VY1Eud/PL1hj
Q24GE8nc7EQnmKFuNXz0guDek/a7SMWgcp/VoPMD/1cI2Vr9Wwlhcf/FULqGR0uC
ANeBlaUgZvDIWXqdimYAFjFBvx+pYlghcAyzymoKnK9wjW1xeyscr7vN8GKARjCC
WLMiHuX3AK2FQUcWpzjuAhQh1eY1AbV0FKTk1pXLbfA526KxUDY9uEV+8M5iRpv6
uz4X01Pk7bwTSNkwGIRWT8SSbWA1VbGARsUinhFinhKmkvdc/CKDtPTdchkmcGEA
D+bIpuWKMhQdAnSCoi5XmcN+5q8PH7IvW6iz6WHGjiQNoqYadiTr+AZu98uRnU0H
vbYXr63tBK60XIjPFcuHMnk8x6aQpUYAWYuaN+EvVvtecStf340tuPg0XWdh9ghG
/MfFiQMLOn4gT+vq6PZPlriCHU4Q97qmdwThrQQsr7kY0zcEF4zOuDXNaccK2UNT
Va1j0a/Ucn25l2UtMW+QSiz9IryWBhBa1lqFdY0sgqYPMbnZx1fQ+DpNwmQ7E8XA
HES6WKGMZNZOJnpu443BPGHUnJk4SyrDKQwL2EfK5tsc0BoAGrGhKdSkdlAB9Z7/
rIfi5efz9HKv8rnHd2vxzXmdB6Lc3eKNC7ICNE5U9ow/Yd90aMBRIdK9f5imw3Uk
CL27LkV1x8aieahJTwwAVVBRZz27FgkmB1x2R42mj99zWZtecrSkGx8wj4/qscq
39wi/tD8tR4iyqzoP8TDNP2YVmkFnSVSOYXeEMsrazTbd0i/sxKqTtx5sZQi9f/J
7K99QYOGKJmhjiC15H/tA7kLD5HPC0fgPDB5m0lp31siMDij46r40RahUjpPdtPk
IgtxhWdiJ+h63rm6WFzoWRlFm/k9yxSsegOpYoCKgi24Z0H/84rtVOXfcmKz+in
+8mkwRVl7bQ7hKkNs9JwnQD37xx5HCw150wNivynBIGlP5ISsr2aRo+eids223FE
9R2TVNXtJp2Nmg6Y+LKbMdCUwaZ7w3vWT3sQmG0rn2nwb1ShnHvQ2Nlw7hAAEbqd
/I3dFrvVPxqm+Q60NVjXrActIlfcTM+LSuc9MCXjgaxXlTMyiWgm09m6UnEGtvWi
LGImq/0CHgW6YCT9bwLnPfkz2L1vk2p78gTUqlH77ixt8THE1WjBIB/GJ15LGIInF
vI1lsLQMkK355Ztg5wk5FhD47k/EFzQWKfyn6+V1u3hfwG0Q5+FRwgYRS5nfA32T
XxFAQIdL57tSXzSrQcDxIe6r2buKOW4glaHWF5kmbK8gchyes4fmvE+pL90s44SUK
ZqBkW3kjaGogZActlWZkq+0QcRYnti5KRyk7jzKT/9f1LLB4qdcrPwyotGKJWip5
pyiLwkxMgWxhociW9/3u1gPwu/K4w42zJQUtX3N5l7TvmPhfDU7L3ognCJeaZvbE
wEJ9KYb8JimYySr+I0rOQ12YVvm/Wq0ZCL9qb2E+Hbxxb9+1FvBt1WGP2zYnBVaY
RSuxr+TFu1IQtMgDjPD0glGiV8sCGXD1rSc4m6p8pSF1IrXNBEF26cianPaJV1DF
YSqqcopBNfM4zeIreRpp0Nhce6wKW7nhcxpwTnSrB+SZA8pjizo0xjSDllaX/wGr
ZDAeflXBwiC6cp9gWivHY2Pa1d3L09joVjfiFx5QxBc3vyYmJ1ATgoQIX6aLJq+/
Uh2hFTw//9lprqgpkKSdr/3TLKbXDlyY5ysVFK170AFUhbals6MbVrXaRHG34A0u
wTv2tsbFcq3qkqCrX7rf8mZXIyGEzbIHq++I1jEVSzwz2E9ruh4jr3lM5d9uus6C
VMysVTCbLnwGKefk1Hh20vSvF902US1PmbcwBFeoYy8XWdt+xHK8aIcbbj6xxBA4
tvBIsfAqCcKYovXdNtW09Ex00eAIA77NUmLaRPCYWsmgGJ5N1YgNyP0yrsxz/6Xc
2lTcTotmEqMjWCRMDwvQnGUSWY0Qe/DsjtXrVcPjSCBdxZ8DWjCYI8mmmyo4lu1X
PSCMXwcQDbGcvNHqzxy0eT72ZHL319aD7ealbqZ5got87H1fURQ/mkp/LRZyeu/
b9gAIL5UAQ+E+1NgQdY/meu0awNp3q0Wpkl0bqglYdEUm77vGO+DlDTQ3ruxeb/
IdBiVypb7YlJcNx5/03bf5JUyLpipeiwzXTeRH5vbzBKkmbSLFkWRW9H+AtI/DV1
OqhGyLon8JkPNO/1WC6c2ftQ2Kp73tT+dsQIObSrrkSXQ9nUaaPbStepczhPptwS
x4zxF8gsc68dZ00syjpcwiJaIm6gWseeB1bPW59IlinNHfHxq6lmt37n7a+VQCpC
oNvnfjGaVwoBW2SGX+Qsu6LQ/7ZBXbAn/ZfPABJ0inn7xycBCArV1NAir/CgrzUK
H3AhI+7f8UnG1JrOnMaJuIccp8LVzYlFIEleTOBLcKrk/5ye6dTR00sX/bWLJiZr
wFLUpA1SH4KxPWQGFe1x+LCuXBIo6Q0q3STUkkgD07afCs6xaEZH9as/9jP2jpG0
ZLiV5Ii8/zZ22vHI9tEjJfVjPNDEgo9++RTw1c0JasWvgUAJcWhRwRzgTeXm8luk
IXnX/Q2HHcQthgIYTdPvJ81uH9TXfuKiT7kDnmbjXGhaPE4uUtV5mokuF65d2Zry
nRYQTt7jEZ2Ve7+6h+AZi3KGW3xVvMibv2isGGI+tAUefrVAC1bKnRnj/3skzRz7
JyFIs0SEH51W6GiapYVwhwIya6Jbq2fCBY5c/0sEvj1jQU845P6KjLfCUJ1Ud0R7
aNP6L6piJ9V4b2vbVXcMzVXAkphV1pkiz3H/KyMy/7HU77R0srzWc1XPupAV9gA
4CaEA10qx5VRgSpko0jQa+UJ6hvc8K0whBx+Qq1D/GLAc5kL8nNdkLZfIy0/yLmh
+khKI9TEEEup5BJwGNw/DxZg+mnMG0wJdeT/y9oKqQBaJQHgk2xRPYvEGjyi1zrq
HDGjY6YMa1TwhxFNUSv8JoHbKU0WYjNDds1APqFbJq6EMs8HgVryDJjQT9ijrEE+
tWb+T1kPWxSWKR3sU6mXhVhQJVzchMJbKj0kohDdb/LaNzD0SQr5RH/4uH3G57B/
n8PhgNNrkQ1snGmqw2JLFSRXpvdL2GA3ne7azpYRgELMs1FSfh5tTrFrWtc2dsvH
bxxPxQY7dBCC6qW02kTNHubYBuR0Dau4SNBivvFAVaqRpQ150deTPm8G5vEukpFc
Uxh80cALRV0b5P3KjyIdCrDK3+i6Z7/dHko+MeSbrKpDZtVWWPteUnB6pDt3GN1o
WLrJ2KIV7u2Y6NseJyV3G89BPUthwgy+WDKheo6vnNf284JZxfIqviIZIyrZcQWA
EhW5/b4KymtMHaB54A4MnhYrqqGQm918bgPjvQOW+cd2uEGe5Dli+Z2BxyHDhCT0
SPOgJLUPATJR4shHRpoduH3RWhTOe89s89LTnIRAJr+m17r10sTYbXxLwswUzQ6l
I5VXww6/HTp5Je2G1xtgLvOKYypTIFzxiPwjLn3rqfYJNQwLQ8c9jWoviy3JSOb

xtwrY/fJ0mDceBFbUtgm/Gbeg5yXmN9Ek0gRcdV7FWNGHziHIUQa1knXdEhWDLuu
0hqFcTUlRYMeoZCpnyEt75c8rmwmnVVGhb3FyLrU09vVeyPvPuB0AiwK9dECvcz/
US+HkNoJSuDLc2/QVV2cJtJIb82c2AM1CaeMoTTjXMK9KyZOeWhBCYNULsR6FzeL
1GQwfJWcdiEEIbrvc/tkYHDnksSgDXxb14E5D2PWmkogtNAs+Uu0WLCz9AhhG9Zr
2YTTj1JA1vQ9Xq6XB/7c0qAXZx5dYqAJM1j7v0Ndget6bUUZluAEJzN5Q4xiK4Hk
BTJb/oSj1U12hMMsuQNeHVQYJQm1UpP43Nod6FdG1DsDSY/ZqMh7i6x4vqwJmJew
L1GdpjgOrqB7RzBwFHzeP84vles38HBgnEIdnBQvQUEOoIMAHPrBNu4LJJgpQ47r
3C0F7J/1+d1otCFcfCmWmrwSrT2cSFVEmndEK39/TU5vSlKdm3Xtn6FtXA9iYNXt
5f3UGBNuuLfpz2n9A9pLTY2h57Hw2nJT21gZI9pA8H3akoSokGacL5ztX00NYHBx
4aC0uNNDPXzXCGlztUjCKJyh+MhFSuFPjwRZNRgMintvJJlCs88A7x05v1B/+aEn
rz0eSyJoGa6AP1NJ0fE7MzSL3bTzd/pi9fH4m3Gui0e1/v907GPoEmdJ8b3LhIKi
awgN4ugc4+SNUoNF0U1Z8fxejeMkGBot+3Kbuzbyq2i2qRIf6/07owwFLA4urfEo
m/SvXwC+0069AqUVQf13Bre/gnf9DweYOBGis4bKuWxcug4xYict9010eDU/8xeg
df059nBd+CmbqR8yAFu6buJB0E64sSjwWYVp4XWM+HRXSbJKrPqpb18Z2hzFCVN7
Hq1YNQKqGV1bn6z1u008kY0gXY83qI21fWtbX7Rf+sj10uWdt6mkcq3Di0DamZNP
Kk9syvk6QndtHmHrivnXjWdMp6cjVnS8szBxBqiDKbvZH0rhfIILBd/jIm3QbjXY
tP0ooqqmIScHkWo+c5aSy7YUEXHNZ03DXWlyjAwYIf95gA752fPfaP7axmg7qFN/
d+KhAN5F+p5y+MYJYJmzEydWWuTNrAHjJXo1I+m6PKWm1Fpm5gUhrEyX6WFPxkga
IaF+Z36LenDmePleJ8YinC9FIzWa004BC2Qc/K1JpCVWuHHQj9nfuc401B6Q302D
A6HxBeE5vXH0Fp6KWWdhucGSWeM/TILi/uiWH41kvJVu6t+pGgOQ17+JHSDfPmgJ
oA3MVWdK5wPYekh6KtM2nLfp08Coj+s7xXffq1haCcJnw3/qcQK84FcQrYKXB6Ve
4lM+bYtZvjfBY/TCDb9UoKuYsRdg1tPk3ACFaVso1nsHh4WM3ID5NyVBzwISn7D5
78Scp6oFZQ+5Bil8dSTfLhkCWN9DYP6TT4aqGUZ1WYInbK5yMAIKMLN5heMjCziy
zvEsbjog9tCqiwSXLvz6CnqfB4swJe2rIiPi2dhR88Z825L5Fb/p6AUH/j/0kYrJ
9BITo8qSY0rz7Hac+WE+oPhL/BCcilVxZrDsGHhybup6qdJa1kjDaIadrJbe2Y/L
UoxPQomUoVzjPLYQ0IZFVx1CynBuJVtQzfGQ6HUAaBpFws3e19PlVikQOGiI7gad
aDAQrZ4zW1t7Wwfp1d8a9dNizwmmEn9VuycjLL7vFZ1Md1f3hJNFYFUS8dcS2ke
BHo6mMYE8zqEQ/MbS0TNFP7np1j0x/e1qbF227CWL4bdUCPD5F7fM01LR6uvJeKh
xgWLeGni+dtYAJ+x4Q8/Zp/zxq+djB1AuVa3pJWUENoE9qM0upvxIPTdihzWrEcE
y2tl6e053d65H8FrvJBQ9zr7D0B742IDzXsCo+jx5tiR714DrGMQteXTrz+1NFMQ
N0bnz4rCCFe//mcSlT8puhMhbe5wcvjA4bEpmghBjo0c0gegHkhPOPfRRF1VD+T
Z8PAarUtX17PM+mEZc+xQtI3mNuDaPHGcbUWk30XfX8ct4Na0TE4XaTEHKI6NaxR
7e6349X2JkULYoi7bFg2c1NZXDut+mnhtYYrPjdXbssljFZs/RBufDo2nWTHp01G
SYmlhr4N/TOrKfapzi91WUVltoGo+U5VyhXyt97KDCj0yEaCe3z3nNVhUAJGj2Dm
8ak/NmE+dShqxW0f7isCmr84lmUtQ/s/Qh3RUGKSf6qNoVZ2+pWhaXK+NuhKMnIq
MAF/NspdJ8r5uNhklb903MmzKuW26z3LgiVBfzkYecY57mre+iBo0zpioLBGk/pw
j1bXvQ/9Uo9frPPQqYHD/5M594sPZ+lu43ItvIoz0+SDcE9LlGQe09KXaGc8R8Py
fx13oQ9IRbZ3BJngc4E9taY1KNWnj2rZY3G0tjFAVPXR2N6ARgFBWc0GIICGJNc9
Hilw0rDaE8SHK0x4u6p67bY1R4qkpD5ejPHRU0Qe1IQ2I5oFJWwCqYYI5MeQ+DBx
oV0jflYsKAC14Vmc29p0xPh2tYJK/axLgSTCCP9a0bX2yS7g0onrmGyNm7qWJBXU
74C1ITUOpPhbd7QZfekBjuwt+D9SkhEOJ6Ij8lf/pv+JzUgjkpe+10xvHnfkIJqZ
IFbpokdcFUevEKWfHJQY08FYIlfHf91HQ/Lrb6MebrkW7bY1VKEROEAnj3m1SQNX
GypZBRrCPJoDxRUHDyfh2t5GDzDv9eakpIuBm/fm9NSPgPkIvXbJkBgWrD+WjMNB
aRzi6C/HcQj9+eFVR9DfTBAJ90gkws0F1/EmUMmTrBQzVj49MDb07TyPntK1NysZ
csPeXy86g4+xbW0IAar2rXiJjVbcTZuPFCR/NtcRXwe+Gdw4MyPfcM8Y6Wa/ByQ0
3XbZdfwy69MuYnKJ5IE22McGBEa3n0Dlpc23UeyDyxlF9jgsaktT1qIb+bFDE0YR
7aVZoyTzGZTWmw2Ae4rDQOW/SPq11roZ8vQxPeVnXVy4KJD/2JK5/sCXuRzXk4kX
0SVyOm0MeLnf+NWPIe4deeGaQAwT2jQvnmuJkXHWcGAunwa4GW25ETxccqekt6y
k3PBKBeZeJvovxsrteoYe0WHbPcvthlUkJfp2I9emnhTjELsqqvBEaS8DZ3nPBnNd
p8ug5WoUp9p1X6gf193Cj6I81B0KhtKzailXVRq9orNlac0yYieOKQhk+dpzIBDe
BqXB22FC225jWrKnwYz0VWFTyZfziarDDS+RjVjcwCD0/60Ksd11d0zbp0VxKkEu
qix/0Ngrilfw0Z4waYTL0u9ihN9KVHIGh0Fn9q0BU90ngirE14bkuSu4KvIMmtYt
3eZ03Nm+bwWzJzlo4yogz1TgH0SGnxyoibz0XzMqFgkVbWvqTnw9UZASvoLAyrS
SFctnu0oPlH9JrL+mfoU83prsRDMmOqudzyi5/xWh4IvamvvQsq5+3xsQr1duA+
W/HeZ8jx5hg05UfexS5hAcgNs4Wz2NVCC19fProSuYh9Caoz2PwlK87c/MliEqWc
jZ5oSk0+zwLXtp3xpv4MHwDzHwqV6Sdg+c0Ut16wLZp0vJVxPD5t1jBU9EW2vjff
Iq19LN50RLPQ7RpfCtJAIYUAuYGz0mwd66Q71d39Wx56wHA9TqQBTzNqI0CK6/mX
sRZKrMvLBTdHKK4Capu6ehFJgUt30ifib6DWV6v5HUG14Dt4z8Bj9a3R66NBLWLR

Z2FjeS1yZXBseQ0KRnJvbTogQWxpY2UgJmx002FsaWNlQHNTaW1lLmV4YW1wbGUu
Z3Q7DQpUhbzQm9iICZsdDtib2JAc21pbWUuZXhhbXBsZSZndDsNCkRhDGU6IFNh
dCwgMjAgRmViIDIwMjEgMTI6MTk6MDIgLTA1MDANCjwvcHJlPg0KPC9kaXY+PHA+
VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHkt
bGVnYWN5LXJlcGx5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGEgc2ln
bmVklWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUETDUyM3DQpL
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBBheWxvYWQgaXMg
YQ0KbXVsdG1wYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBjdB1c2VzIHRoZSBIZWfkZXIgaUUhJvdGVj
dGlvbiBzY2h1bWUgZnJvbSB0aGUgZlJhZnQNCndpdGggdGh1IGhjcF9zaHkgSGVh
ZGVyIENvbmZpZGVudG1hbiB0eSB0b2xpY3kgd2l0aCBhICJMZWdhY3kNCkRpc3Bs
YXkiIHBBcnQuPC9wPg0KPHA+PHR0Pi0tIDxicj5BbGljZTxicj5hbGljZUBzbWlt
ZS5leGFtcGx1PC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tZDNlLS0NCg0KLS1k
MzcNCkNvbRlbnQ0tVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRYYW5zMVYLUVU
Y29kaW5nOiBiYXNlNjQNCkNvbRlbnQ0tRGlzcG9zaXRpb246IGlubGluZQ0KDQpp
VkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQUFBQUFBVUNBWUFBUQUN0aVwTkbQUFj
RWxUFVZSNDJ1V1RPEgJBDQpNQWdTNz5bk8zVHBSdzIwZHFwYmZBU1FFak95d2l3
WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZld2taDQpZ3J6ZmNwV1wTDJq
bzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00v
dWxpDQp2ZFbMVFaMmTERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0KLS1k
MzctLQ0KoIIPjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIHvCNAQENBQAwtENMA5GA1UEChMESUVURjERMA8GA1UECXMITEFNUFNgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QYyBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcWU0MThaMDsxDTALBgNVBAOT
BE1FVEYxETAPBgNVBAStCEExBTBVTIFdHMRcwFQYDVQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfLwLjJj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLoAJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVGRNhbGljZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgXlvLir3hEUvZ23MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmk1RF7FOD7Pfb5v94M5274XYxW2W4uKgd7QGnUZROsvSYkGiWdp1JhqXwfDz8
A0enITGXnoEkaFvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHuZ1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBAQUAMFUDTALBgNVBAOTBE1FVEYx
ETAPBgNVBAStCEExBTBVTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFNgU1NBIEEN
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLZWhMQU1QYyBXRzEXMBUG
A1UEAxMQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sSHU
a4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUBYQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbB1fkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElNAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEADA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEFv2zLiThQYSHJeuKWqQENMgZmZmB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZ1
RAZef7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524

```
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
0KypQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfWCAQEwbDBVMQ0wCwYDVQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpq1zALBg1ghkgBZQMEAgGgATAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzE5MDJa
MC8GCSqGSIb3DQEJBDEiBCDmeJ6lsrSkjN4AZBIkFqDsd0GBqHEAIhAZzSPkodWm
CTANBgkqhkiG9w0BAQEFAASCAQA8+6A0jm2WrDdfvFYh00Q4Rpy+6ofiRnx5ji8I
a0iD6U77+KS/1W9c4rm5Sk2E1E7gZb/XL5D719X5aoiuF6KgyPrzNCL4G3Zz9zLY
11+7Cc+VsR8HcY9mgI5U34bmT1xZCHk3V+hTSUn+zE2XV5khxX0E50xGzkrSz39Y
TReERGZGPPXorUIc/MPPKVNE0uh1VUY3WVp9oECnY0BnZ8Ed91rzJWH9hbvUq+jx
22s5mbPGSi5napgEIr/vv66CuCSBK9oqUG4/dyd/hvLVgtZ3knoxn8VPXUgf8Yw6
my5/oStqc03Q9Sd176LsZ40tgc4kG789qHA1Tax4HGqU3bAi
```

C.3.16.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with `hpc_shy` (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-legacy-reply
Message-ID:
  <smime-signed-enc-complex-hp-shy-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:19:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
References: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
  <smime-signed-enc-complex-hp-shy-legacy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:19:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
  In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
  References: <smime-signed-enc-complex-hp-shy-legacy@example>
Content-Type: multipart/mixed; boundary="d37"; hp="cipher"

--d37
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="d3e"

--d3e
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
  hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-shy-legacy-reply
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
```


Date: Sat, 20 Feb 2021 12:19:02 -0500

This is the
smime-signed-enc-complex-hp-shy-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--

Alice
alice@smime.example
--d3e
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
hp-legacy-display="1"

```
<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-shy-legacy-reply
From: Alice &lt;alice@smime.example>
To: Bob &lt;bob@smime.example>
Date: Sat, 20 Feb 2021 12:19:02 -0500
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-shy-legacy-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--d3e--
```

--d37

Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQejOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAftPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--d37--

C.3.17. S/MIME Signed and Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 Header Protection ([RFC8551HP](#)) scheme with the hcp_baseline [Header Confidentiality Policy](#).

It has the following structure:

```

└─ application/pkcs7-mime [smime.p7m] 9580 bytes
  ↓ (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6082 bytes
    ↓ (unwraps to)
    └─ message/rfc822 1876 bytes
      └─ multipart/mixed 1828 bytes
        └─ multipart/alternative 1166 bytes
          └─ text/plain 392 bytes
            └─ text/html 490 bytes
              └─ image/png inline 232 bytes

```

Its contents are:

```

Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
Subject: [...]
Message-ID:
  <smime-enc-signed-complex-rfc8551hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:28:02 -0500
User-Agent: Sample MUA Version 1.0

MIIbnAYJKoZIhvcNAQcDoIIbjTCCG4kCAQAxxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBE1FVEYxETAPBgNVBAsTCExBTUVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElnRnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqSISIb3DQEBAQUABIIBAIGTjqXl+E6A5sPoSiC4rgKQPp/Sq9KlmiYZ
kHuhai6C1kyLR/I+dsQNTJb+T6nUMs6u0C8lHLMolShXNbmU0UFxbzTjBmz6qdb
gqzLeYdkT+l+EuFrsgQ8XtDNqIZHHo6u0c4lZWxdJ1kBGaatjQjzo7qA4fG1uQ/A
NDPZHozuhLE5/Q2+0CTbAawvfXDmA+Ss+Sh5vVxtw7ev0xNoRPzypAvcc/gLCly9
C5RJdy2ctavux6LmC89561I25uUHhgSxCaVT8lXhUMxvgCeN0nWBDp1n68Xy836V
d2LKSIEq0INfA400OrsujxP5WJaJm4xh+eSUQcCpPcJEGBMuWaUwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAMVD52+ksD3N5L7E1Kbclg44f
WmBMTTsrUeL+q+sqHAzPNf+7x2Yitv9X4QjctucZQNo09s41d7WiaV6TtMvCExcM
Vi+bu0jPHiei2WxtASZ9arH0W2+aB46Iw7UTbrw13EXSAN5IXFIyeQTl4mjte2Rd
Mxp300z42W0zsfAh+3mr6bNvoSiS2WUBvwpP36VfWir1GT1wf2Wdv8a0iCcSE0jIE
5oKEenck4jNNXxe3i30L3x3FR51piNpxcxo60iuJcyNpBnzjZ6FLzPDKyqPLzhDg
mBMG4XyMsNeL8fQ5YjjuuZ7xtUKQi8lEih5G1MeeLCy7IyPR1vzraIe42CNpwzCC
GG4GCSqSISIb3DQEHATAdBgIghkgBZQMEAAIEEFNM7bcQDJtZl9ZLfi1Ni2aAghhA

```

nYiY1WB73G0hddIjiceKCfuPFWFmUwC3zkyxz5Qgh/07UYL2YXPH/+W2xZnS11U5
eHN3eLqCmsRC2bRfPAPvda/ZW7J2GCEHYORRg44m1k7bLrQACA5PDn3T5cYT+syq
evYnIqK0tAcqo7cphQZ/n/uwdvKpWvkn8dQe0H8RTw+CsMPo9SezKr3hyJTENhre
Tswyoo5hTtSgHf1vSv51dKJMuKAGvXW7AaAImuNh6rtknzXS+VzUNVh0FvzgLUA
36SzeFdJ1NTrpM04p/Du00S9saLdxF001TMLaungoLMZgM60ZCCLi3z4CFuQyIlt
UB2viRGOfJhkePgWaoty6eLv11TXKCxb10ehMU7f8VowVwRWm62h0/SYvPBuGuXJ
7GEVYHlrp4aXR2KQbeMoyxxY5hUGKWzDg4zJc1r80IAZXc64s7SR01x5BVinXhSE
w4VGQ7Qv3CpolKQeuyQ14XK7/nzlkYWDXLFeuU528gHy42Xt+FaKR6ZE1FURPdr
0IIWN+Gdr28bpQomhbmhm71Sr7q3IIG3wXEh/qrxWf0yzSrrJluLcCAh9dyWM3e
vfuneXrnXTr9Tf1GW/rNygZoHMvrjpSRIrzEAqqCzt/Vs1+ds0TBHn5fs9E2poIW
9bXm54ucpXavu5ZafpHURetrXLMGPJ+IkyGGVrACwAsIDYm/aPSM4HA41DzHtkY8
q/HRYWR6So7r1YEO74bY2e+Ty0JhSapZ87b2I1JMkHUZeB3aAPswZeMdZoA0HF+K
HK2zXm1havuDecCc59q+DP4R0nfMbAU2ACTxvh+dJzX9GdifCUeh9NXn73fb8f50
7k3GRbg3TgoUDJmfU8wxeHtx7Dvay1baRLAW8CT0fyedJFGL7qhl3iz1hHp9Jjs
SzZpZ1LCP/Yv/06zNuP0RsR0WuaqYdK3qppgIoGta5Z+ZcHxLAh1rxr/mF1qxDoP
sFhG/UoPSLT/lyzYN4pbBqC/QRuC3gr0MMKHbM7G6gJppBW74se9w4IwIBmln02
f8T2FgobF7Z3ne1LRpLCDcaQHfVcyN1IRu9PJH5Kcc0hGYqIAH7t6JPRfcImNbtS
W8Y5bcZ0/1S5kY/Q9NpeAiUDVndt0qdYE0tcNSpPhi9TrtqULD5EpGJsc05Gmkcn
ATDL5nzJdLB7XvRQKi+FeWiZUz1r+IH7ik37WGkjZwwt+ClY1kAjgX39poUJTf+7
r/gaI0pg/vz881qZk6vgRQmIRwBv2GvLEfvMz00hf9vAwzYx3uj64/5aXJbsxr
PxpatoirJu+pF1nh6bPK+THYTnej2t1G1zLWuEvxZvHnUqlWNh4cRsuwm6Cf0H/2
kv0HY4Rcnjiz13aPMIU/zjg0rkfmPfZfofyPJfNsiXC1h8Cty0HKZC/nW1Lg0pJg
hm+FbvUIrvhPhMKMJgY3n0Qf6eEkwnZpWzQxp8wcaVNsP10GoBG3Lef1MbSnsIh
rUx60yXXdpxaIgrWJQpXkSd59z5VTIyEbJj8iil/GEqqXs0WMG0n1RE+o9sR21Za
+m65T7hsq0U776EWjZwcrb44rn/sW+mg+8+leuXL4UNADrm64qXvCcIkHrTpPRML
k/W71PtYybEx8eZRkEG3tIWog3HV8w+WRKS1smFYvFwx66eU9cFDnKoYJAQi7USq
fdkW/QLuXUJuGvpKGGWm8IJgOezbGPKbiYw+BTMJKEgxStAhAhVFP3m/47AUx9
bGiRMGgEBvprT9Iu7mydH0jU0//qRm6fUX0YJ5Xm80Ujk/wI/wOCdt066tw/d9L4
n2skZbRlMEDsja62427CHLCedZAWyyTaCdkj3QiC/vfj74okv+U7SsDyUWxnSK0p
pMZEsdV8qUpPrjT9Eh6BSD4B3SrGDuhSEdNuW60Qb2Yab0ZjWaurJeGqVn23A+tR
u92mwIBB4K/9w9LGv6NRRVoLuSZ7wxcERmM9aXg4f6UjPKijbPzADnPrahsZ4hb
TpbxZkU/U6KmNm0/19M5KZjFRM087dIA8K8e40eJoqGeCyTezC8SzuKy6w26bLQO
TonyUBgbpnRzPg3dx6A6Qfr+H7E1XXDTTWcoY9FCGPuYkkmjYgjRW/7phcASXgHz
76+C15RI/CdZh5q2hCZE7L9dqH03sX/12pyR/DCoGDN100x/u9xqBo6mxR3LTYf3
RP6TVLKnT70ynXdmYjaJMaMWj/+EKsip70TxZanpHeh74l0+YWpvKL5PQtxvSko+
EohJTUaPjxG6EJj4K7Xu4aq9UqW7c0fyYM1o0abQaB9ZY1K3aQdRwvY2D7//bCo9
56J84Dh1KfP1MkakehPJFY3FvParM9kRYxf7CnhVdQX2UkAi5xasZRK020ksUr0k
s0M1TvefRZbgaffX+DhtvubUvFlit7PVwj5Q0c5YiLELlgSqTpKKn0+IL0uX3H
pZmms25AZqtY8VZEjtUfv5XoZK/HtF646ipe0yawWi1JoNGSw50Cvz5zy9YtcfPI
Gz56LodAyQV17CHSZCRE9tTlyyFxsZzyfK+AggcahrD7sc83lpd3PiwAjUL0VCg
8EFNHILF3VT9+DsJGZJbqvoITgB51p0i4cdXgS3/yaZ0aESnZBAnEBUXtQQL9wqP
18UcDog+kvMK37AYeqGgoseh6ZvJXd5hIMj6WesXUTOQy6IGzZciDAPeNUdMmW0U
NivI9SL8uxbSXG8NB9Q63xHj6J8WjNaNzWZPER/qylfzQaP7uywTKXr4cVTVYwKG
TZGzt10ZnymvwWoH7LhJ5qS1pPqe/4gNiJCngBmRpeG0qDH0SFJ//3Lncg94gnJ
N8f9Y8zUkulr02LHsTuzz0I2YCZsP42ZgL66H3uy7MkvgYYF03IHRsim/evQqS/Z
WKpHRC02Cof8hta9pZQsR6WBWCxCUSEbgcBskZVg2iApVXVDgDYYPHI0KSUef1S
QKsXX1CT7IR4g//0MRP2RyKcrYiIkz09auKYex7CNYQYZfqueMKUuKw5gXjMZS/p
jV2Enoo1UG2kzAYFL2mRzdbaxeoqXVvbgErM4c7WKKomfoGIP6Kk4mOWwcEvPozJ
pNxUOCPIUBoRcXMuozp0u0bvU30EBRX+gJWYqRi9p1dnc9EXzm1MHX7Ui6xT6ZCv
DF7YhBWV2GvGC+YKR5IjPXEPO015PEngi3cNV9htahtQWK8DiYjR4B0tHQ0mZRL
NGWRyDbV60ac7pvl/wPwCEefySu2d4hvfIEn17B2oLKxowoJsEz0e0F+C23xR9n
HfMNe/Fd2JtxJ6WJfPymG/hvdYY5Fnt4V1NpK/guwMbJbYfuRbHhCb5AG0gbxiIX
bszWSiv/af5aFhQWh7eXZcSZoJ3PZIK2z6r9ALFaGy69Qiswbgop4VGs89kjBrZQ
42+eD859Xw2zr8YRuskKIraDl1jB2txZQYZQkHhZMjagEgc6scYEgikMTRyMDY2T
PgJtyLi11Vec6ZQ29/go9N/rIYDmYx1wN/eBM7SqVQqkhE6AerBhiGetml1gRn8i
BbCgc8ClQubVQ45XQzE3mhm5UnAbJWofEdHJabShy1hoMfuFQFXd4b4okMUFow9H
hTi3daOLjmqgo47E10HalXt4MItAhLXP9+GrhVE5vYN1h/cVRA94K8M1L+5HzT1f
18RglS8gLKV1D+BlXFw7JfS04vAtfv62ttuEinRUicte2rMKi4RKa0m7FYGiD36

Q1eGa9W69kkJ0xpykFAR6qX/UE0TVydER4+6f4/43Pu53DQs3HqoKsW65q1xb3vX
zci638qUL4lu2LjmxWmeBm8vRyhyY84QR95qI/RHoYWIxNSEXggcX2Evvow+c0rc6
s3C3KjD08EyT7CKtQ0yAp0HcWhFI3gLvgJf7kd4hvZ3IsqZ0TPpNhPo0Lw70wWtX
qX3akv8xPBPQ2DfUSuoJyhoMQLX3zVL2B17wm5Q+TqcjM6R56MGfvBGUMmbEIQ4
Wm4NY7I8LPN58UeKJ3A2pxhRXG/s/q8PMZUJeXL5QtYBonMFNnISS11T2cP8bB/G
LYTC3q8aejWKSg+mX15sovgxDGFFR/Ru2y/Rlx2Mk76tJPr+8nbCYVnNfDlZEkc
htdWl1m1ocXvtb4bjKyMkd9LqH3bdfBAApQquQ+6FG3wTedEsEvP0xvg3byYYXb/
E/nvvKhX5Dp90jNkh1GhGfDmoJwJCXutvvd+tnhIFFlarvqfo6zFCQXetwFgBEgg
SYXUugaiovw5r09/7fJs4+9Lwr8phsH1tNibweWGmh9o3GM8tGgxfha0tikRWx3y
MpKecxe9RWUufrUwScDYpTI7sjnqHAjm3qT4YCTnX0QsYeE14yXUo+ftU5WA4evq
xzNcaHo+61Y+/rgB6TFYIQg1tRINAp86EB930uKbJN6xga2QjICTZlvzF9aperRF
Tcmqws2kESiyyvzBGBVhgQSPn7fBkn1bAA8MLHhBQVhiA7h28biGv5g0nhipApDo
lRDXJh1q37N0fL0xQXDzuqUt44MMY9CqFZxERDTcq/dGHZtoKum6NHHZTbA9ugnT
ZzcFrk3yor5ahbjcsW0+44cq52TSRBZy4yGL14+oMD1TbePqRyKdpuUxNeaZmex
80fBFBDN1p095LRb85t0tLzXDALvhshpuWVn+sH8uC6c1rJ/x+LRP6idSiTD1glE
+yRzeG3YXa2LtLbE+PjDmFla9c0e089nNGvqYKoqjDYFdnAgX99stX2gJ5pZKuzn
k8lGBNH1/ytiRKM1NOVQSR0QuRniUn1M7UjAuvDt4Whp0yo6d4n5EG03IrAs/0ms
0fd5KwaQV2kM7gLVWC8EDFFPAQTLjVXnbqrJHnpnzB8+3Umdc7bbtThrHdvb0gXW
Qi2IOPME+CC4pY7QVjLdW7EUHtWzu577RVyJcGknH4qVtPSqnDk01fogprq080os
9UUNreV+Ie06Mk54JjGsw4yeKYTYl0zEuxZ2X1ec6ah5pDdofAln5u0wAMBVBodL
q388bcdVtmLWKd0TEc+3Jx+fGCUQfQJq18lpzx6gPm1h/61QXF9R5Jpc1fiA7gJ7
hpSLRkiQrXZ7tvpXRAFdk9xp/hyKfo8SBPYGZAKvt7H8Wv3akP3hPBhDsKdTg2yL
kZciqnm8fa+A8QM6fjHXF9CQ7kAKL5Kyzrn+hQ8gndovU5hKcML0OPRKC4881XGX
sHqQMP/36DGjEGXyGmmlCIDWiuIfHxQ9vaDZB9c5muWYbI00anAUBiPsuQYD0vap
vyxeONavr53nof0v/AlrMUBiEaJcokDU9Ljddqbm02DBwhqL7Qkju+fvg18+j0tB
8BuGwTTHFpvXY0wQARiFeonj4qM4PM/TmZYggqaWkSgqCfcMka0LoIEHLe3k927w
TKnKuorWmjDsm0PzWzekxVuEvwmMPWCKL/MRhDkbgm1tCrc58UsgdznEy2K15c/W
BPc9dhuzhyAP30tgN8NiPjANFymRYlZ1XRibTfrWbGZ4JkUr7rjLAJVhMb3a7TBB
16B12261Yu2cfbEpJNr/yTvG67xEB8dGA0etD85ZaKGctvTN4K13SsCEvkNydF7L
GjzW7UvGHNyQoPZ7c+rLLAvmQpLsbsvZDIidYvq7Gj05C+N3K/Kz1VL7RQ0abErj
I+xB11C/D+LOUjFfsZiphJjI57P6wAL3euP9Y6Ytr+SJQmndw6Nkq3t8l2S0FWMVz
zLeAvJ4SaRHy0ERQ/nrfGTIx2GmTZUvrsrn9KUtBn7dPLmyKqz13zYf55nLNA+Gc
LheU12GH5K4Qja3qKENpz0KpDXuEFyxA7iFvcKEqJm2f3fEJ2KfSDeNdNDFf642m
oX3Z7y3dls4iKds83wj0PORCo8j9ro03GxSCjmlgThnR5sM1bYrye6oh0pw3SjyB
8FAKn+qdH4Z/ndk/K/UqZ8MyDJAXuSQu6rHaEv9zz2K6HfyLqX83obnFYE3WNHzy
TFFLKqW31A5ZRtCUTN0D6LfZ0ikwrgB+pWzfzGvRbghK+sGKweMEFF2Cbn0z3A3g
bvC3sG6/rxBFZ/iU3Yd6hBiRmjquUojs19zSowRlkbUIRXZteaDnhz5qwcMpt3r0
iod4Z2QmnW8mJM0T8uX0MBIFwCjKRgqKHfjeTnT1NCpx0H5+6DJrj0mEPHf0B1o
nHKJor6EOMU4zsDAZHCcepPyvRfLTp7TvUf0D5RBkqNf6JfGoPTLQ6JC1QnMOPzS
S1FAodd2Qng3q5fQh9tiaohZdyf2hN+1b9bvac1LUB1SZM6mS/JenvA/+NVVoqdh
3IEAepXOHv6B0PxN7V/R4JtTgVIJTWbC3TyLdseAii+Y3yEFFKIUABGGd2mSpJNV
mPze3fiKmsfj+05kcKb7q+EB0/CDSU+upSFmRSq2YbyM+P5/1faoUz2Nny+ee5Z7
0YVfMt6jhWqZgvpdTavzbKiQ/aCQmmRnxEwRQ8fhbtXrnzdebHK7sFuqn5mtsfgR
jL/s+D5nQLkc+VtPslqa0XFAFz+iGLFuA2FDuWIkECu4qoMsE0EP+gbcQ1EbjaX2
oR82st4KqgDeBga/3GTqx5TN0nbn584ujZ+VAYy0UZjShlH+4NJY1GMRH1A1b3kA
hWtP//PnkX1aZFGWAHhiPIneG/ZCtRGUWqWUMn9DRd5BNMS7S/xl17KIF91FbLS
6b5f5R5J/wjdwCC8mH0CCNXrdWRID3vqVEyBvH4usBoA8v64+ttQIUSttweBoG6W
A12Qorxi8wZGqZ6qLp4glATHp2Ni1Aq90kP2cBfUNKP5GLdBD6102qoBlTuuRliA
T25cdgz1J0tHrFsKJ4t04Udb8PWSr5DuFINhjcDP/wMthFRhCrLSipJs0EzreASD
C1fuEYbwD2or7UiWaZC37ERT10VC+kyNS2j/bxNubKpXWg0H0TWT0LdXjCj30sDN
1lhPugAjjgZ0px8f+wyaucDEXq6ubMcMtE4QLng7ivqw7vJFs51FIigskVPRnB0ro
k6rPrEMP/zgVSEBt0ULp2CG0RdUnPCLTlGR/B9F3WRfjHhowbnYANAZU1LgR/doC
qEkgjxVKfThjV+Xf9BWU6sBAVvq/I805hdZEn6ALRDrSnusIwmfVTdkb16uSQD1p
MZjuGe+TkSpUY2CUIVucmmV6HCVJm4H+J3U9bsmQ0WeCtR1kDKLaquuqYCjJk1NB
vJ0aDR/0NJizyCpC4seGJ8gPRKV4VDvch3jCjN0XFc9sS3YQdJWS13NpYoZkBymg
CR6Gf4WX5Mt8yhWPBP2ZYCF9yj6B30Svd8UU/01/v3z3kH8gtni7rwq9YX5+S0x4
h5FKsYkYFbt+Llh9BEaHvYF7ENwT3IS6tIs+A5g06By708pPoEKrZc1MYA0pZste
nKRoIjNLjUnThyJFI5K6o98GGJ3REHJ3i83rfkWO31G5SVgYqk72m7j/dLJ28x68

dd4tLSA8YnIvPkFsaWN1PGJyLz5hbGljZUBzbWltZS5leGFtcGx1PC90dD48L3A+
PC9ib2R5PjwvaHRtBD4KLS1kYjYtLQoKLS0yNjYKQ29udGVudC1UeXB10iBpbWFn
ZS9wbmcKQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzZogYmFzZTY0CkNvbnRlbnQt
RGlzcG9zaXRpb246IGlubGluZQoKaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJR
QUFBQVVDQV1BQUFDtMlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQpNQWdTNzM5bk8z
VHBSdzIwZHFwYmZBU1FFak95d213WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtF
KzZLd2taCnNncnmpY3FWTXBMMmpvMDQ0N2dZRHB1QXJrK09uSkhrSWbBZ1RQUmlj
aWhBZjVZSnJ3N3ZqdjBaV1JXTS91bGkKdmRQZjFRWjJrREQ5eHBwZDh3QUFBQUJK
ULU1RXJrSmdnZz09CgotLTI2Ni0tCqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmX
Ss5CVIEh7j00Boq0MA0GCSqGSib3DQEBDQUAMFUXDTALBgNVBAoTBELFVEYxETAP
BgNVBAstCEExBTBVTIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFNUFMgU1NBIEN1cnRp
ZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1
NDE4WjA7MQ0wCwYDVQKKEwRJRVRGMREwDwYDVQKLEwhMQU1QUyBXRzEXMBUGA1UE
AxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSib3DQEBAAUAA4IBDWAwwgEKAoIB
AQCa1Sn6i8Gi44/oAVAn5Gnck4PHHNjrSfWUnne1N41KImVaTC3D9zFCrS3i4Pa9
ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT905NL
FflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCREZuTtMc1zy++MxQ
lqdn9WZLh0A0peNZKGMVwjeVy+8FkyZC3jX/Qcm+ZLCq1LqhBwDHDZ5qDTI12PVX
1X3K7/c0NxbvBbaU1/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AO
EksCAW1b+MD8QH9Yj7CFsmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNV
HSAEEDAOMAAGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUuZXhh
bXBzZTATBgNVHSEUDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBSAwHQYDVR00
BBYEFKJTQdVEPIAFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEWjnwHFwYn8Qko
ZTYaZxxodvRZMA0GCSqGSib3DQEBDQUAA4IBAQCBSXignLEynBakDKU68ro0RsyX
WAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsox/Ht9Ii6zyBZVjdaox644DsiL0QEP
4YMS7y4q94RFFdmdzEbDLYx9sfUhdTxDN00oHz53PYDBh4zE4Nar2inC0D+VM6R
GDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVtluLihne0Bp1GU
Tkr0mJBol6dSYa18Hw8/ANHpyEx156BJABb744gqoeuD9YSHjKK49+qYC9faFmQ
+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vRhZjVD6FYMIID
zzCCAreAwIBAgITN0EFee11f0Kpolw69Phqzppq1zANBgkqhkiG9w0BAQ0FADBV
MQ0wCwYDVQKKEwRJRVRGMREwDwYDVQKLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2Ft
cGx1IExBTVBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0xOTExMjFt
NjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMASGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWN1IEExvdmVsYWN1MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pd0/
KLpZbJOAER0sI7Aja07B1GuMUFJeStUlamNfCwDcDkY63PQWl+DILs7GxVwXurhY
dZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVBDpbP
4JFD9hsc8prDtpGmFk7rd0q8gqnHXBW2RZAelqzJOMayCQtwS1q7ktkNBR2wZX5I
Cjecf1YJfHx4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZ
wLSewbWXLJe3VMvbvQj0BMpEYlaJBUIKk01zQ1Pq90njlsJL0wIDAQABo4GvMIGs
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAAwDjAMBggpghkgBZQMCAATABMB4GA1UEEQX
MBWBE2FsaWN1QHNTaW11LmV4YW1wbGUwEwYDVR0LBAwwCgYIKwYBBQUHAWQwDgYD
VR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNV
HSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEA
c4miNqf0QaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roAKHAp
+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oA
JKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahIXRn/C9cy31wbqNsy9x
0fjPQg6+DqatiQpMz9EiaE6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnYxs1Fhd06
zZk9E8zw1c1ALGZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCdGNG/D0qyTb
Y4fgKieUhx/tHuzUzZxJjGCAgAwggH8AgEBMGwwVTENMASGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBzZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6aqdcwCwYJYIZI
AWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHATAcBgkqhkiG9w0BCQUx
DxcNMjEwMTcyODAYWjAvBgkqhkiG9w0BCQQUxIgQgzbXAB7rXfNs26yY0HvuE
D4KQ9RzsSF5fL551ZZY7AjgwdQYJKoZIhvcNAQEBBQAEEgEAA5y7DQLS7S+Vh2b
Ju5W9UwkHp6lUk/F7mJE80FRc8K6z8pcSn4xTr1CaLg7azQ0o/iNQEH2EVJqdy6
huwwtlaeiPa2gXwIHCKcLGH2bW3/R+sEsJZi7FryqTakOZ9eXcYRXoPWv6ncf+I
eA7j1QX3Z4Ln5pP9p+Uw7H1oroH2Y4e0yAqIMtYXnS+GKALTtbxTa1p2Y9dsHQLS

```
2cXbfUsU2zc5bstgKXZyTkjuKJ8ivbYJ2ttk79AOMosWkDBmgzKTTS/0Hptf09SD
mX58BvQt6GHQZ4TR2NVDvq3z+/CA1zsR5xmNH1C+uDh990Roy3w6CHmv4aTTmRM9
S+uZXg==
```

C.3.17.2. S/MIME Signed and Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="266"
Subject: smime-enc-signed-complex-rfc8551hp-baseline
Message-ID:
<smime-enc-signed-complex-rfc8551hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:28:02 -0500
User-Agent: Sample MUA Version 1.0

--266
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="db6"

--db6
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-enc-signed-complex-rfc8551hp-baseline
message.

This is an encrypted and signed S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 header protection
(RFC8551HP) scheme with the hcp_baseline Header Confidentiality
Policy.

--
Alice
alice@smime.example
--db6
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-enc-signed-complex-rfc8551hp-baseline</b>
message.</p>
<p>This is an encrypted and signed S/MIME message using PKCS#7
envelopedData around signedData. The payload is a
```

```
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 header protection
(RFC8551HP) scheme with the hcp_baseline Header Confidentiality
Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--db6--

--266
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUUEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--266--
```

Appendix D. Composition Examples

This section offers step-by-step examples of message composition.

D.1. New Message Composition

A typical MUA composition interface offers the user a place to indicate the message recipients, subject, and Body. Consider a composition window filled out by the user like so:

Composing New Message

To:

Alice <alice@example.net>

Subject:

Handling the Jones contract

Send

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.

Figure 1: Example Message Composition Interface

When Bob clicks "Send", his MUA generates values for the Message-ID, From, and Date Header Fields and converts the message Body into the appropriate format.

D.1.1. Unprotected Message

The resulting message would look something like this if it was sent without cryptographic protections:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

D.1.2. Encrypted with hcp_baseline and Legacy Display

Now consider the message to be generated if it is to be cryptographically signed and encrypted, using [HCP](#) hcp_baseline, and the legacy variable is set.

For each Header Field, Bob's MUA passes its name and value through hcp_baseline. This returns the same value for every Header Field, except that:

hcp_baseline("Subject", "Handling the Jones contract") yields "[...]".

D.1.2.1. Cryptographic Payload

The Cryptographic Payload that will be signed and then encrypted is very similar to the unprotected message in [Appendix D.1.1](#). Note the addition of:

- the hp="cipher" parameter for the Content-Type
- the appropriate HP-Outer Header Field for Subject
- the hp-legacy-display="1" parameter for the Content-Type
- the Legacy Display Element (the simple pseudo-header and its trailing newline) in the Main Body Part

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
  hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:08:43 -0500
HP-Outer: From: Bob <bob@example.net>
HP-Outer: To: Alice <alice@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <20230111T210843Z.1234@lhp.example>

Subject: Handling the Jones contract

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

D.1.2.2. External Header Section

The Cryptographic Payload from [Appendix D.1.2.1](#) is then wrapped in the appropriate Cryptographic Layers. For this example using S/MIME, it is wrapped in an `application/pkcs7-mime; smime-type="signed-data"` layer, which is in turn wrapped in an `application/pkcs7-mime; smime-type="enveloped-data"` layer.

Then, an external Header Section is applied to the outer MIME object, which looks like this:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: [...]
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
MIME-Version: 1.0
```

Note that the Subject Header Field has been obscured appropriately by `hcp_baseline`. The output of the CMS enveloping operation is base64 encoded and forms the Body of the message.

D.2. Composing a Reply

Next, we consider a typical MUA reply interface, where we see Alice replying to Bob's message from [Appendix D.1](#).

When Alice clicks "Reply" to Bob's signed-and-encrypted message with Header Protection, she might see something like this:

Replying to Bob ("Handling the Jones Contract")

To: Bob <bob@example.net>

Subject: Re: Handling the Jones contract

Send

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it's critical!
>
> Thanks,
> Bob
>
> --
> Bob Gonzalez
> ACME, Inc.

--
Alice Jenkins
ACME, Inc.

Figure 2: Example Message Reply Interface (Unedited)

Note that because Alice's MUA is aware of Header Protection, it knows what the correct Subject Header Field is, even though it was obscured. It also knows to avoid including the Legacy Display Element in the quoted/attributed text that it includes in the draft reply.

Once Alice has edited the reply message, it might look something like this:

Replying to Bob ("Handling the Jones Contract")

To: Bob <bob@example.net>

Subject: Re: Handling the Jones contract

Send

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it's critical!

I'll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.

Figure 3: Example Message Reply Interface (Edited)

When Alice clicks "Send", the MUA generates values for the Message-ID, From, and Date Header Fields, populates the In-Reply-To and References Header Fields, and also converts the reply Body into the appropriate format.

D.2.1. Unprotected Message

The resulting message would look something like this if it were to be sent without any cryptographic protections:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: Handling the Jones contract
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
```

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

```
> Please review and approve or decline by Thursday,
> it's critical!
```

I'll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.

Of course, this would leak not only the contents of Alice's message but also the contents of Bob's initial message, as well as the Subject Header Field! So Alice's MUA won't do that; it is going to create a signed-and-encrypted message to submit to the network.

D.2.2. Encrypted with `hcp_no_confidentiality` and Legacy Display

This example assumes that Alice's MUA uses `hcp_no_confidentiality`, not `hcp_baseline`. That is, by default, it does not obscure or remove any Header Fields, even when encrypting.

However, it follows the guidance in [Section 6.1](#) and will make use of the `HP-Outer` field in the Cryptographic Payload of Bob's original message ([Appendix D.1.2.1](#)) to determine what to obscure.

When crafting the Cryptographic Payload, its baseline [HCP](#) (`hcp_no_confidentiality`) leaves each field untouched. To uphold the confidentiality of the sender's values when replying, the MUA executes the following steps (for brevity, only Subject and Message-ID/In-Reply-To are shown):

- Extract the referenced Header Fields (see [Section 4.2](#)):
 - `refouter` contains:
 - Date: Wed, 11 Jan 2023 16:08:43 -0500
 - From: Bob <bob@example.net>
 - To: Alice <alice@example.net>
 - Subject: [...]
 - Message-ID: <20230111T210843Z.1234@lhp.example>

- `refprotected` contains:
 - `Date: Wed, 11 Jan 2023 16:08:43 -0500`
 - `From: Bob <bob@example.net>`
 - `To: Alice <alice@example.net>`
 - `Subject: Handling the Jones contract`
 - `Message-ID: <20230111T210843Z.1234@lhp.example>`
- Apply the response function:
 - `respond(refouter)` contains:
 - `From: Alice <alice@example.net>`
 - `To: Bob <bob@example.net>`
 - `Subject: Re: [...]`
 - `In-Reply-To: <20230111T210843Z.1234@lhp.example>`
 - `References: <20230111T210843Z.1234@lhp.example>`
 - `respond(refprotected)` contains:
 - `From: Alice <alice@example.net>`
 - `To: Bob <bob@example.net>`
 - `Subject: Re: Handling the Jones contract`
 - `In-Reply-To: <20230111T210843Z.1234@lhp.example>`
 - `References: <20230111T210843Z.1234@lhp.example>`
- Compute the ephemeral `response_hcp` (see [Section 6.1](#)):
 - Note that all Header Fields except `Subject` are the same.
 - `confmap` contains only `("Subject", "Re: Handling the Jones contract") -> "Re: [...]"`

Thus, all Header Fields that were signed are passed through untouched. The reply's `Subject` is obscured as `Subject: Re: [...]` if and only if the user does not edit the `Subject` line from that initially proposed by the MUA's reply interface. If the user edits the `Subject` line, e.g., to `Subject: Re: Handling the Jones contract ASAP`, the `response_hcp` will *not* obscure it and instead pass it through in the clear.

For stronger header confidentiality, the replying MUA should use a reasonable [HCP](#) (not `hcp_no_confidentiality`). Also recall that the local [HCP](#) is applied first and that `response_hcp` is only applied to what is left unchanged by the local [HCP](#).

D.2.2.1. Cryptographic Payload

Consequently, the Cryptographic Payload for Alice's reply looks like this:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: Handling the Jones contract
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
  hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:48:22 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: Re: [...]
HP-Outer: Message-ID: <20230111T214822Z.5678@lhp.example>
HP-Outer: In-Reply-To: <20230111T210843Z.1234@lhp.example>
HP-Outer: References: <20230111T210843Z.1234@lhp.example>

Subject: Re: Handling the Jones contract

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it's critical!

I'll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.
```

Note the following features:

- the `hp="cipher"` parameter to Content-Type
- the appropriate HP-Outer Header Field for Subject
- the `hp-legacy-display="1"` parameter for the Content-Type
- the Legacy Display Element (the simple pseudo-header and its trailing newline) in the Main Body Part

D.2.2.2. External Header Section

The Cryptographic Payload from [Appendix D.2.2.1](#) is then wrapped in the appropriate Cryptographic Layers. For this example using S/MIME, it is wrapped in an `application/pkcs7-mime; smime-type="signed-data"` layer, which is in turn wrapped in an `application/pkcs7-mime; smime-type="enveloped-data"` layer.

Then, an external Header Section is applied to the outer MIME object, which looks like this:


```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: [...]
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
  smime-type="enveloped-data"
MIME-Version: 1.0
```

Note that the Subject Header Field has been obscured appropriately even though `hcb_no_confidentiality` would not have touched it by default. The output of the CMS enveloping operation is base64 encoded and forms the Body of the message.

Appendix E. Rendering Examples

This section offers example Cryptographic Payloads (the content within the Cryptographic Envelope) that contain Legacy Display Elements.

E.1. Example text/plain Cryptographic Payload with Legacy Display Elements

Here is a simple one-part Cryptographic Payload (Header Section and Body) of a message that includes Legacy Display Elements:

```
Date: Fri, 21 Jan 2022 20:40:48 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Dinner plans
Message-ID: <text-plain-legacy-display@lhp.example>
MIME-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
  hp="cipher"
HP-Outer: Date: Fri, 21 Jan 2022 20:40:48 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <text-plain-legacy-display@lhp.example>

Subject: Dinner plans

Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
```

A compatible MUA will recognize the `hp-legacy-display="1"` parameter and render the Body of the message as:

Let's meet at Rama's Roti Shop at 8pm and go to the park from there.

A legacy decryption-capable MUA that is unaware of this mechanism will ignore the `hp-legacy-display="1"` parameter and instead render the Body including the Legacy Display Elements:

Subject: Dinner plans

Let's meet at Rama's Roti Shop at 8pm and go to the park from there.

E.2. Example text/html Cryptographic Payload with Legacy Display Elements

Here is a modern one-part Cryptographic Payload (Header Section and Body) of a message that includes Legacy Display Elements:

```
Date: Fri, 21 Jan 2022 20:40:48 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Dinner plans
Message-ID: <text-html-legacy-display@lhp.example>
MIME-Version: 1.0
Content-Type: text/html; charset="us-ascii"; hp-legacy-display="1";
  hp="cipher"
HP-Outer: Date: Fri, 21 Jan 2022 20:40:48 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <text-html-legacy-display@lhp.example>

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>Subject: Dinner plans</pre>
</div>
<p>
Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
</p>
</body>
</html>
```

A compatible MUA will recognize the `hp-legacy-display="1"` parameter and mask out the Legacy Display div, rendering the Body of the message as a simple paragraph:

Let's meet at Rama's Roti Shop at 8pm and go to the park from there.

A legacy decryption-capable MUA that is unaware of this mechanism will ignore the `hp-legacy-display="1"` parameter and instead render the Body including the Legacy Display Elements:

Subject: Dinner plans

Let's meet at Rama's Roti Shop at 8pm and go to the park from there.

Appendix F. Other Header Protection Schemes

Other Header Protection schemes have been proposed in the past. However, those typically have drawbacks such as sparse implementation, known problems with legacy interoperability (in particular with rendering), lack of clear signaling of sender intent, and/or incomplete cryptographic protections. This section lists such schemes known at the time of the publication of this document out of historical interest.

F.1. Original RFC 8551 Header Protection

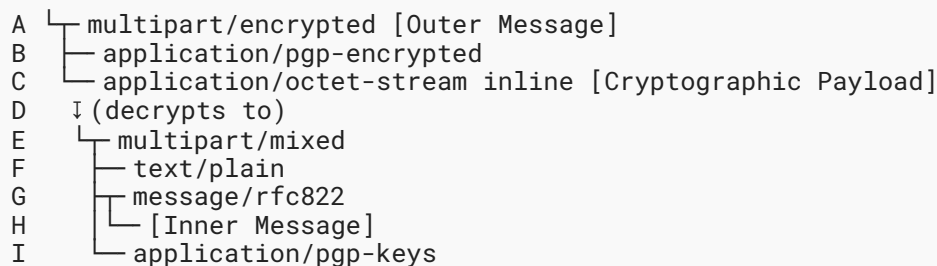
S/MIME [RFC8551] (as well as its predecessors [RFC5751] and [RFC3851]) defined a form of cryptographic Header Protection that has never reached wide adoption and has significant drawbacks compared to the mechanism in this document. See [Section 1.1.1](#) for more discussion of the differences and [Section 4.10](#) for guidance on how to handle such a message.

F.2. Pretty Easy Privacy (pEp)

The pretty Easy privacy (pEp) [PEP-GENERAL] project specifies two different MIME schemes that include Header Protection for Signed-and-Encrypted email messages in [PEP-EMAIL]: One scheme -- referred as pEp Email Format 1 (PEF-1) -- is generated towards MUAs not known to be pEp-capable, while the other scheme -- referred as PEF-2 -- is used between MUAs discovered to be compatible with pEp. Signed-only messages are not recommended in pEp.

Although the PEF-2 scheme is only meant to be used between PEF-2-compatible MUAs, PEF-2 messages may end up at MUAs unaware of PEF-2 (in which case, they typically render badly). This is due to signaling mechanism limitations.

As the PEF-2 scheme is an enhanced variant of the [RFC8551HP](#) scheme (with an additional MIME Layer), it is similar to the [RFC8551HP](#) scheme (see [Section 4.10](#)). The basic PEF-2 MIME structure looks as follows:



The MIME structure at part H contains the Inner Message to be rendered to the user.

It is possible for a normal MUA to accidentally produce a message that happens to have the same MIME structure as used for PEF-2 messages. Therefore, a PEF-2 message cannot be identified by the MIME structure alone.

The lack of a mechanism comparable to HP-Outer (see [Section 2.2](#)) makes it impossible for the recipient of a PEF-2 message to safely determine which Header Fields are confidential or not while forwarding or replying to a message (see [Section 6](#)).

Note: As this document is not normative for PEF-2 messages, it does not provide any guidance for handling them. Please see [\[PEP-EMAIL\]](#) for more guidance.

F.3. Autocrypt Protected Headers

[\[PROTECTED-HEADERS\]](#) describes a scheme similar to the Header Protection scheme specified in this document. However, instead of adding Legacy Display Elements to existing MIME parts (see [Section 5.2.2](#)), [\[PROTECTED-HEADERS\]](#) suggests injecting a new MIME element "Legacy Display Part", thus modifying the MIME structure of the Cryptographic Payload. These modified Cryptographic Payloads cause significant rendering problems on some common Legacy MUAs.

The lack of a mechanism comparable to `hp="cipher"` and `hp="clear"` (see [Section 2.1.1](#)) means the recipient of an encrypted message as described in [\[PROTECTED-HEADERS\]](#) cannot be cryptographically certain whether the sender intended for the message to be confidential or not. The lack of a mechanism comparable to HP-Outer (see [Section 2.2](#)) makes it impossible for the recipient of an encrypted message as described in [\[PROTECTED-HEADERS\]](#) to safely determine which Header Fields are confidential or not while forwarding or replying to a message (see [Section 6](#)).

Acknowledgements

Alexander Krotov identified the risk of From address spoofing (see [Section 10.1](#)) and helped provide guidance to MUAs.

Thore Göbel identified significant gaps in earlier draft versions of this document and proposed concrete, substantial improvements. Thanks to his contributions, the document is clearer, and the protocols described herein are more useful.

Additionally, the authors would like to thank the following people who have provided helpful comments and suggestions for this document: Berna Alp, Bernhard E. Reiter, Bron Gondwana, Carl Wallace, Claudio Luck, Daniel Huigens, David Wilson, Éric Vyncke, Hernani Marques, juga, Kelly Bristol, Krista Bennett, Lars Rohwedder, Michael StJohns, Nicolas Lidzborski, Orie Steele, Paul Wouters, Peter Yee, Phillip Tao, Robert Williams, Rohan Mahy, Roman Danyliw, Russ Housley, Sofia Balicka, Steve Kille, Volker Birk, Warren Kumari, and Wei Chuang.

Index

C H R

C

Compose [Table 5](#)

ComposeNoHeaderProtection [Table 5](#)

H

HCP [Section 1.7](#); [Section 1.7](#); [Section 3, Paragraph 2](#); [Section 3, Paragraph 5](#); [Section 3.1, Paragraph 3](#); [Section 3.1, Paragraph 9](#); [Section 3.1.1, Paragraph 1](#); [Section 3.2, Paragraph 2](#); [Section 3.2, Paragraph 3](#); [Section 3.2.1, Paragraph 3](#); [Section 3.2.2, Paragraph 1](#); [Section 3.2.2, Paragraph 4](#); [Section 3.3, Paragraph 1](#); [Section 3.4.1, Paragraph 1](#); [Section 3.4.2, Paragraph 1](#); [Section 3.4.2, Paragraph 2.1.1](#); [Section 3.4.2, Paragraph 2.3.1](#); [Section 3.4.2, Paragraph 2.4.1](#); [Section 3.4.2, Paragraph 3](#); [Section 4.8.2, Paragraph 3](#); [Section 5.2.1, Paragraph 4.5.2.2.1.1](#); [Section 6.1, Paragraph 5](#); [Section 6.1, Paragraph 7](#); [Section 6.1.1, Paragraph 7.8.1](#); [Section 6.1.1, Paragraph 8](#); [Section 8.2, Paragraph 1](#); [Section 8.2, Paragraph 4](#); [Section 8.2, Paragraph 5](#); [Section 8.2, Paragraph 6](#); [Section 9.2, Paragraph 2](#); [Section 9.2, Paragraph 3](#); [Section 11.2, Paragraph 1](#); [Section 11.2.1, Paragraph 1](#); [Section 11.2.3, Paragraph 1](#); [Section 11.2.3, Paragraph 2](#); [Section 11.3, Paragraph 2](#); [Section 11.4, Paragraph 2](#); [Section 12, Paragraph 1](#); [Table 5](#); [Appendix D.1.2, Paragraph 1](#); [Appendix D.2.2, Paragraph 3](#); [Appendix D.2.2, Paragraph 6](#)

Header Confidentiality Policy [Section 1.2, Paragraph 4](#); [Section 1.7](#); [Section 3, Paragraph 2](#); [Section 3.1, Paragraph 1](#); [Section 3.2.1, Paragraph 1](#); [Section 3.2.2, Paragraph 1](#); [Section 3.3, Paragraph 1](#); [Section 3.4, Paragraph 1](#); [Section 3.4.1, Paragraph 2](#); [Section 3.4.2, Paragraph 1](#); [Section 4, Paragraph 5.4.1](#); [Section 5.2, Paragraph 2.2.1](#); [Section 6.1, Paragraph 5](#); [Section 6.1, Paragraph 7](#); [Section 6.1.1, Paragraph 3](#); [Section 8.2, Paragraph 1](#); [Section 9.2, Paragraph 1](#); [Section 11.2.1, Paragraph 3](#); [Section 12.3](#); [Appendix C.2, Paragraph 1](#); [Appendix C.3.1, Paragraph 1](#); [Appendix C.3.2, Paragraph 1](#); [Appendix C.3.3, Paragraph 1](#); [Appendix C.3.4, Paragraph 1](#); [Appendix C.3.5, Paragraph 1](#); [Appendix C.3.6, Paragraph 1](#); [Appendix C.3.7, Paragraph 1](#); [Appendix C.3.8, Paragraph 1](#); [Appendix C.3.9, Paragraph 1](#); [Appendix C.3.10, Paragraph 1](#); [Appendix C.3.11, Paragraph 1](#); [Appendix C.3.12, Paragraph 1](#); [Appendix C.3.13, Paragraph 1](#); [Appendix C.3.14, Paragraph 1](#); [Appendix C.3.15, Paragraph 1](#); [Appendix C.3.16, Paragraph 1](#); [Appendix C.3.17, Paragraph 1](#)

HeaderFieldProtection [Section 4.10.2, Paragraph 2.2.1](#); [Table 5](#)

HeaderSetsFromMessage [Section 4.3.1, Paragraph 4.2.1](#); [Section 4.10.2, Paragraph 2.2.1](#);
[Section 4.10.2, Paragraph 2.4.1](#); [Table 5](#)

R

ReferenceHCP [Table 5](#)

RFC8551HP [Section 1.1, Paragraph 1](#); [Section 1.1, Paragraph 2](#); [Section 1.1.1, Paragraph 1](#); [Section 1.1.1, Paragraph 2](#); [Section 1.1.1, Paragraph 5](#); [Section 1.1.1, Paragraph 7](#);
[Section 1.1.1, Paragraph 8](#); [Section 4.10, Paragraph 1](#); [Section 4.10, Paragraph 2](#);
[Section 4.10.1, Paragraph 1](#); [Section 4.10.1, Paragraph 3](#); [Section 4.10.1, Paragraph 5](#);
[Section 4.10.2, Paragraph 1](#); [Section 4.10.2, Paragraph 2.1.1](#); [Appendix C.2.5, Paragraph 1](#); [Appendix C.2.6, Paragraph 1](#); [Appendix C.3.17, Paragraph 1](#); [Appendix F.2, Paragraph 3](#)

Authors' Addresses

Daniel Kahn Gillmor

American Civil Liberties Union
125 Broad St.
New York, NY 10004
United States of America
Email: dkg@fifthhorseman.net

Bernie Hoeneisen

pEp Project
Oberer Graben 4
CH- 8400 Winterthur
Switzerland
Email: bernie@ietf.hoeneisen.ch
URI: <https://pep-project.org/>

Alexey Melnikov

Isode Ltd
14 Castle Mews
Hampton, Middlesex
TW12 2NP
United Kingdom
Email: alexey.melnikov@isode.com