Stream: Internet Engineering Task Force (IETF)
RFC: 9964
Category: Standards Track
Published: April 2026
ISSN: 2070-1721
Authors: M. Prorock *Tradeverifyd*
O. Steele *Tradeverifyd*

RFC 9964
ML-DSA for JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE)

Abstract

This document specifies JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for the Module-Lattice-Based Digital Signature Standard (ML-DSA), a Post-Quantum Cryptography (PQC) digital signature scheme defined in US NIST FIPS 204.

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/rfc9964.

Copyright Notice

Table of Contents

1. Introduction

This document specifies how to use ML-DSA keys and signatures as described in [FIPS-204] in conjunction with JOSE and COSE. A new key type named Algorithm Key Pair (AKP) is defined to express public and private keys for use with algorithms not limited to those registered in this document. Similarly, a new thumbprint algorithm is defined for AKP to ensure these keys can be compared according to the procedures defined in [RFC7638] and [RFC9679].

2. Terminology

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.

Some examples in this specification are truncated using "..." for readability.

3. AKP Type

This section specifies a generic cryptographic key structure for use with algorithms not limited to those registered in this document. The Algorithm Key Pair (AKP) type is used to express public and private keys for use with algorithms. The concept of public and private information classes for key pairs originates from Section 8.1 of [RFC7517]. The parameters for public and private information classes contain byte strings in a format specified by the `alg` value. The `alg` JSON Web Key (JWK) parameter or COSE Key Common parameter is **REQUIRED** for all AKP keys. The `pub` parameter contains public information and is **REQUIRED**. The `priv` parameter contains private information and **MUST NOT** be present in public keys. Some algorithms may require or recommend additional structure or length checks for associated key type parameters.

When AKP keys are expressed as JWKs, the key parameters are base64url encoded. When AKP keys are expressed as COSE keys, no encoding is needed.

This document introduces the `AKP` key type in [IANA.jose]:

An example truncated private key for use with ML-DSA-44 in JWK format is provided below:

```
{
   "kid": "T4xl70S7MT6Zeq6r9V9fPJGVn76wfnXJ21-gyo0Gu6o",
   "kty": "AKP",
   "alg": "ML-DSA-44",
   "pub": "unH59k4Ru...DZgbTP07e7gEWzw4MFRrndjbDQ",
   "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
}
```

Figure 1: The All-Zeros ML-DSA-44 JWK

This document introduces the `AKP` key type in [IANA.cose]:

An example truncated private key for use with ML-DSA-44 in COSE_Key format is provided below:

```
{
   / kid /   2: h'b8969ab4b37da9f068...6f0583bf5b8d3a8059a',
   / kty /   1: 7, / AKP /
   / alg /   3: -48, / ML-DSA-44 /
   / pub  / -1: h'ba71f9f64e11baeb589...3830546b9dd8db0d',
   / priv / -2: h'00000000000000...0000000000000000'
}
```

Figure 2: The All-Zeros ML-DSA-44 COSE Key

4. ML-DSA Private Keys

Note that US NIST [FIPS-204] defines 2 expressions for private keys: a seed, and a private key that is expanded from the seed.

Unlike [RFC9881], which supports the expanded private key format to maximize interoperability with existing implementations, this document specifies ML-DSA private key information using only the seed format. The seed format was chosen to provide a single, compact representation that is consistent across both COSE and JOSE, simplifying key management and reducing storage requirements.

For the ML-DSA private keys described in this document, the `priv` parameter **MUST** be the seed and **MUST** have a length of 32 bytes.

This specification intentionally does not define a means of utilizing the expanded private key representation defined by US NIST FIPS so as to increase interoperability by having a single ML-DSA private key representation for COSE and JOSE.

See the Security Considerations of this document for details.

5. ML-DSA Algorithms

The ML-DSA Signature Scheme is parameterized to support different security levels.

In this document, the abbreviations ML-DSA-44, ML-DSA-65, and ML-DSA-87 are used to refer to ML-DSA with the parameter choices given in Table 1 of [FIPS-204].

This document has registered the ML-DSA-44, ML-DSA-65, and ML-DSA-87 algorithms in [IANA.jose] and [IANA.cose].

In accordance with Section 3 of this document, ML-DSA key parameters have the following additional constraints:

The `pub` parameter is the ML-DSA public key as described in Section 5.3 of US NIST [FIPS-204].

The size of `pub` and the associated signature for each of these algorithms is defined in Table 2 of US NIST [FIPS-204] and repeated here for convenience:

Algorithm	Private Key	Public Key	Signature Size
ML-DSA-44	2560	1312	2420
ML-DSA-65	4032	1952	3309
ML-DSA-87	4896	2592	4627

Table 1: Sizes (in Bytes) of Keys and Signatures of ML-DSA

Note that `priv` size is always 32 bytes and that KeyGen_internal is called to produce the expanded private keys for "Private Key" in the table above.

See Section 4 and ML-DSA Private Keys for further details.

These algorithms are used to produce signatures as described in Algorithm 2 of US NIST [FIPS-204].

The ctx parameter **MUST** be the empty string for ML-DSA-44, ML-DSA-65, and ML-DSA-87.

Signatures are encoded as byte strings using the algorithms defined in Section 7.2 of US NIST [FIPS-204].

When producing JSON Web Signatures, the signature byte strings are base64url encoded and the encoded signature size is larger than described in the table above. When producing COSE signatures, no encoding is needed; see Section 4 of [RFC9052] for more details on how COSE signatures are created.

Table 2 of [FIPS-204] describes the ML-DSA key and signature sizes. ML-DSA produces significantly larger public keys and signatures compared to traditional algorithms. This size increase can create challenges for deployments with limited bandwidth, memory, or processing capacity. ML-DSA may not be suitable for use cases requiring small keys or signatures. Use of thumbprints as described in [RFC7638] and [RFC9679] can reduce the need to repeat public key representations.

6. AKP Thumbprints

Although this document specifies how to represent ML-DSA keys using AKP, the AKP key type and thumbprint computations are suitable for use with algorithms other than ML-DSA.

When computing the COSE Key Thumbprint as described in [RFC9679], the required parameters for AKPs are:

- "kty" (label: 1, data type: int, value: 7)
- "alg" (label: 3, data type: int, value: int)
- "pub" (label: -1, value: bstr)

The COSE Key Thumbprint is produced according to the process described in Section 3 of [RFC9679].

When computing the JWK Thumbprint as described in [RFC7638], the required parameters for AKPs are:

- "kty"
- "alg"
- "pub"

Their lexicographic order, per Section 3.3 of [RFC7638], is:

- "alg"
- "kty"
- "pub"

The JWK Key Thumbprint is produced according to the process described in Section 3 of [RFC7638].

See the `kid` values in the JWK and COSE Key examples in Appendix A for examples of AKP thumbprints.

7. Security Considerations

The security considerations of [RFC7515], [RFC7517], and [RFC9053] apply to this specification as well.

A detailed security analysis of ML-DSA is beyond the scope of this specification; see [FIPS-204] for additional details. Implementers should also refer to the security considerations in [RFC9881] for additional guidance on ML-DSA deployment considerations, including discussions on randomized versus deterministic signing approaches.

7.1. Private Key Compromise

The seed and the private key expanded from the seed require the same level of protection. If an unauthorized party obtains the seed, or the expanded private key, they can forge signatures. This undermines the authenticity and integrity guarantees provided by ML-DSA, as attackers could impersonate the legitimate signer or alter signed data without detection.

7.2. Rationale for Not Supporting HashML-DSA

This document does not specify algorithms for use with HashML-DSA as described in Section 5.4 of [FIPS-204]. As the verify routines are different, future support for HashML-DSA would require the registration of additional algorithms. Section 8.3 of [RFC9881] explains the rationale for disallowing HashML-DSA, including the increased complexity and compatibility concerns with existing implementations.

7.3. Validation of Keys

When an AKP algorithm requires or encourages that a key be validated before being used, all algorithm-related key parameters **MUST** be validated.

Section 7.2 of [FIPS-204] describes the encoding of ML-DSA keys and signatures. For Algorithms 22 and 23 (pkEncode and pkDecode), the inputs need to be within the ranges given in the algorithms. For the ML-DSA algorithms registered in this document, the `priv` key parameter is the seed, and therefore, the seed length check **MUST** be performed. The length of the seed is 256 bits, which is 32 bytes. However, when the `priv` parameter is expanded using KeyGen_internal, the skEncode and skDecode algorithms **MUST** be used. [FIPS-204] notes "skDecode should only be run on inputs that come from trusted sources" and that "as the seed can be used to compute the private key, it is sensitive data and shall be treated with the same safeguards as a private key".

7.4. Mismatched AKP Parameters

When using an AKP key with an algorithm, it is possible that the public and private information class parameters have been tampered with or mismatched. Depending on the algorithm and implementation, the consequences of using mismatched parameters can range from operations failing to private key compromise.

8. IANA Considerations

8.1. Additions to Existing Registries

8.1.1. New COSE Algorithms

IANA has registered the following entries in the "COSE Algorithms" registry. The following completed registration actions are provided as described in [RFC9053] and [RFC9054].

8.1.1.1. ML-DSA-44

Name: ML-DSA-44

Value: -48

Description: CBOR Object Signing Algorithm for ML-DSA-44

Capabilities: `[kty]`

Change Controller: IETF

Reference: RFC 9964

Recommended: Yes

8.1.1.2. ML-DSA-65

Name: ML-DSA-65

Value: -49

Description: CBOR Object Signing Algorithm for ML-DSA-65

Capabilities: `[kty]`

Change Controller: IETF

Reference: RFC 9964

Recommended: Yes

8.1.1.3. ML-DSA-87

Name: ML-DSA-87

Value: -50

Description: CBOR Object Signing Algorithm for ML-DSA-87

Capabilities: `[kty]`

Change Controller: IETF

Reference: RFC 9964

Recommended: Yes

8.1.2. New COSE Key Types

IANA registered the following entry in the "COSE Key Types" registry. The following completed registration template is provided as described in [RFC9053].

8.1.2.1. AKP

Name: AKP

Value: 7

Description: COSE Key Type for Algorithm Key Pairs

Capabilities: `[kty(7)]`

Change Controller: IETF

Reference: RFC 9964

8.1.3. New COSE Key Type Parameters

IANA has registered the following entries in the "COSE Key Type Parameters" registry. The following completed registration templates are provided as described in [RFC9053].

8.1.3.1. AKP Public Key

Key Type: 7

Name: pub

Label: -1

CBOR Type: bstr

Description: Public key

Reference: RFC 9964

8.1.3.2. AKP Private Key

Key Type: 7

Name: priv

Label: -2

CBOR Type: bstr

Description: Private key

Reference: RFC 9964

8.1.4. New JOSE Algorithms

IANA has registered the following entries in the "JSON Web Signature and Encryption Algorithms" registry. The following completed registrations are provided as described in [RFC7518].

8.1.4.1. ML-DSA-44

Algorithm Name: ML-DSA-44

Algorithm Description: ML-DSA-44 as described in US NIST FIPS 204

Algorithm Usage Location(s): alg

JOSE Implementation Requirements: Optional

Change Controller: IETF

Specification Document(s): RFC 9964

Algorithm Analysis Documents(s): [FIPS-204]

8.1.4.2. ML-DSA-65

Algorithm Name: ML-DSA-65

Algorithm Description: ML-DSA-65 as described in US NIST FIPS 204

Algorithm Usage Location(s): alg

JOSE Implementation Requirements: Optional

Change Controller: IETF

Specification Document(s): RFC 9964

Algorithm Analysis Documents(s): [FIPS-204]

8.1.4.3. ML-DSA-87

Algorithm Name: ML-DSA-87

Algorithm Description: ML-DSA-87 as described in US NIST FIPS 204

Algorithm Usage Location(s): alg

JOSE Implementation Requirements: Optional

Change Controller: IETF

Specification Document(s): RFC 9964

Algorithm Analysis Documents(s): [FIPS-204]

8.1.5. New JOSE Key Types

IANA has registered the following entry in the "JSON Web Key Types" registry. The following completed registration is provided as described in [RFC7518] and [RFC7638].

8.1.5.1. AKP

"kty" Parameter Value: AKP

Key Type Description: Algorithm Key Pair

JOSE Implementation Requirements: Optional

Change Controller: IETF

Specification Document(s): RFC 9964

8.1.6. New JWK Parameters

IANA has registered the following entry in the "JSON Web Key Parameters" registry. The following completed registrations are provided as described in [RFC7517] and [RFC7638].

8.1.6.1. AKP Public Key

Parameter Name: pub

Parameter Description: Public key

Used with "kty" Value(s): AKP

Parameter Information Class: Public

Change Controller: IETF

Specification Document(s): RFC 9964

8.1.6.2. AKP Private Key

Parameter Name: priv

Parameter Description: Private key

Used with "kty" Value(s): AKP

Parameter Information Class: Private

Change Controller: IETF

Specification Document(s): RFC 9964

9. References

9.1. Normative References

[FIPS-204] NIST, "Module-Lattice-Based Digital Signature Standard", NIST FIPS 204, DOI 10.6028/NIST.FIPS.204, August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>.

[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>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/info/rfc7518>.

[RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <https://www.rfc-editor.org/info/rfc7638>.

[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>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/info/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/info/rfc9053>.

[RFC9054] Schaad, J., "CBOR Object Signing and Encryption (COSE): Hash Algorithms", RFC 9054, DOI 10.17487/RFC9054, August 2022, <https://www.rfc-editor.org/info/rfc9054>.

[RFC9679] Isobe, K., Tschofenig, H., and O. Steele, "CBOR Object Signing and Encryption (COSE) Key Thumbprint", RFC 9679, DOI 10.17487/RFC9679, December 2024, <https://www.rfc-editor.org/info/rfc9679>.

9.2. Informative References

[IANA.cose] IANA, "CBOR Object Signing and Encryption (COSE)", <https://www.iana.org/assignments/cose>.

[IANA.jose] IANA, "JSON Object Signing and Encryption (JOSE)", <https://www.iana.org/assignments/jose>.

[RFC9881] Massimo, J., Kampanakis, P., Turner, S., and B. E. Westerbaan, "Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", RFC 9881, DOI 10.17487/RFC9881, October 2025, <https://www.rfc-editor.org/info/rfc9881>.

Appendix A. Examples

A.1. JOSE

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "T4xl70S7MT6Zeq6r9V9fPJGVn76wfnXJ21-gyo0Gu6o",
    "kty": "AKP",
    "alg": "ML-DSA-44",
    "pub": "unH59k4RuutY-
pxvu24U5h8YZD2rSVtHU5qRZsoBmBMcRPgmu9VuNOVdteXi1zNIXjnqJg_GAAxepLqA00Vc3lO0bz
RIKu39VFD8Lhuk8l0V-cFEJC-
zm7UihxiQMMUEmOFxe3x1ixkKZ0jqmqP3rKryx8tSbtcXyfea64QhT6XNje2SoMP6FViBDxLHBQo2
dwjRls0k5a-
XSQSu2OTOiHLoaWsLe8pQ5FLNfTDqmkrawDEdZyxr3oSWJAsHQxRjcIiVzZuvwxYy1zl2STiP2vy_
fTBaPemkleynQzqPg7oPCyXEE8bjnJbrfWkbNNN8438e6tHPIX4l7zTuzz98YPhLjt_d6EBdT4Mld
sYe-
Y4KLyjaGHcAlTkk9oa5RhRwW89T0z_t1DSO3dvfKLUGXh8gd1BD6Fz5MfgpF5NjoafnQEqDjsAAhr
CXY4b-
Y3yYJEdX4_dp3dRGdHG_rWcPmgX4JG7lCnser4f8QGnDriqiAzJYEXeS8LzUngg_0bx0lqv_KcyU5
IaLISFO0xZSU5mmEPvdSoDnyAcV8pV44qhLtAvd29n0ehG259oRihtljTWeiu9V60a1N2tbZVl5mE
qSK-6_xZvNYA1TCdzNctvweH24unV7U3wer9XA9Q6kvJWDVJ4oKaQsKMrCSMlteBJMRxWbGK7ddUq
6F7GdQw-3j2M-qdJvVKm9UPjY9rc1lPgol25-
oJxTu7nxGlbJUH-4m5pevAN6NyZ6lfhbjWTKlxkrEKZvQXs_Yf6cpXEwpI_ZJeriq1UC1XHIpRkDw
dOY9MH3an4RdDl2r9vGl_IwlKPNdh_5aF3jLgn7PCit1FNJAwC8fIncAXgAlgcXIpRXdfJk4bBiO8
9GGccSyDh2EgXYdpG3XvNgGWy7npuSoNTE7WIyblAk13UQuO4sdCbMIuriCdyfE73mvwj15xgb07R
ZRQtFGlFTmnFcIdZ90zDrWXDbANntv7KCKwNvoTuv64bY3HiGbj-NQ-
U9eMylWVpvr4hrXcES8c9K3PqHWADZC0iIOvlzFv4VBoc_wVflcOrL_SIoaNFCNBAZZq-2v5lAgpJ
TqVOtqJ_HVraoSfcKy5g45p-qULunXj6Jwq21fobQiKubBKKOZwcJFyJD7F4ACKXOrz-
HIvSHMCWW_9dVrRuCpJw0s0aVFbRqopDNhu446nqb4_EDYQM1tTHMozPd_jKxRRD0sH75X8ZoToxF
SpLBDbtdWcenxj-
zBf6IGWfZnmaetjKEBYJWC7QDQx1A91pJVJCEgieCkoIfTqkeQuePpIyu48g2FG3P1zjRF-
kumhUTfSjo5qS0YiZQy0E1BMs6M11EvuxXRsHClLHoy5nLYI2Sj4zjVjYyxSHyPRPGGo9hwB34yWx
zYNtPPGiqXS_dNCpi_zRZwRY4lCGrQ-
hYTEWIK1Dm5OlttvC4_eiQ1dv63NiGkLRJ5kJA3bICN0fzCDY-
MBqnd1cWn8YVBijVkgtaoascjL9EywDgJdeHnXK0eeOvUxHHhXJVkNqcibn8O4RQdpVU60TSA-
uiu675ytIjcBHC6kTv8A8pmkj_4oypPd-F92YIJC741swkYQoeIHj8rE-
ThcMUkF7KqC5VORbZTRp8HsZSqgiJcIPaouuxd1-8Rxrid3fXkE6p8bkrysPYoxWEJgh7ZFsRCPDW
X-yTeJwFN0PKFP1j0F6YtlLfK5wv-c4F8ZQHA_-
yc_gODicy7KmWDZgbTP07e7gEWzw4MFRrndjbDQ",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws":
"eyJhbGciOiJNTC1EU0EtNDQiLCJraWQiOiJUNHhsNzBTN01UNlplcTZyOVY5ZlBKR1ZuNzZ3Zm5Y
SjIxLWd5bzBHdTZvIn0.SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb
3V0IHlvdXIgZG9vci4.knI1Q_9CIzLH5Xy94Kkc7WVKqZcAgtJ3mNf0GUj1uLA6YXAWFJfXkh-
zQxUtEl3UIC7zPCiUwKTDR6ZsuUmFj8Ctb_6aH64hElN7weS_1m5okCy8GqHNL2lsfclCH3Y2f4QN
P-
DLVS1XsuboDA7Dw3ir2IdYKIfWJyIU7ROHgd24nuun1zJbxcLJC2EKt2M8R0wZudcIE9nm5oPzYXq
0z-hPsKoXp9leVYkqgMmO9Lo8SP_1YYIEth3B8v-
GuP249KDTFRKPjISmK4aPCknjtjihHsQVv2XePXxKExatHl4qhsiiW-y-
EJXa1Kfw4WYpLA7B4_5Ids--
cIJmIx7f6xxAWKh5qoBWq1QIOaaFuzsAraRW3NOEuzThew1En85gI3GcRTZGp-
VDGyxHm0Al04cyWo2bxAVOF0fbDc265iP2mCNw6Qg10jIJeAhGB4OAMYcBUWJAG0l1MN1U_koEmGh
5dXKnQTRl461ea_Cq3DLkcA2Dj2woWUFyDTmQ8oO_yheASfJacyRm7_suj88z5XFNo8F53P8OxTG9
xUPlrwvH-
TAq7AH3NU4SNXApyVKTU3zhx1tJ34nlTILcTujXVJVo_f0DZfUxr6JSCYqvy4z1Kl0wDQzd55aopy
FtQxvOPhcCHbAN34g2Ug750Jm835fl7NOxcqoMbuTcgH68kr37M-
Pdh2K9WazXUJgCupgdIWW8WjfOjmTiF59CrVtfVtK2qDzF40OENCfqtNPQlZe5cN5p0P8arj4USB8
```

```
HCPh7NdqQBAeWrw0wsYhdiM39lrSkA8mLRYMhZnqKGCTPCrHXDdEjRKYRNaqIUT44laYl5c27K0v-
ozjKPu6tzEhkYSC4XZ3LehEFtmAzOE0mHbhKMgXqjoPJjOrGIPibX3jwK8_Q5RmMOXtXo8R3vXfBa
UdQoLeeyywNYE0nIcsl4z5a8_utwEFiVf0VK2pdviyiOPVSi3zOMAmqz6gFhVy8aMMQOWZAEAuTyD
w7ZWG6diwptmrgSXZotW63I19S2ZH7keCXRIq_pFLuYhOuG6dD4MkouILRdC9bXZMLrNDq7COpUOO
86aQVlYd0pR935WpUw-
V6obSRnHlRFZSmUSIB7h1Q0ImciRzojN93Xhw7qpzGzdzDEO3OOTayXaSG_0YHQyy-
eH4hBbmgt_LBx120g1eY4XHeHFRfTfetHkL5ZZusX1jQ_nk9ez4XBG_6hRtTNSuVBsYlH8-KUuR5-
qTP8dkvRf8Wk2hHoUr2sz5YO_xDFCMMTrt8ahiMyfjo5ih5Fwo3riFbFUGKibniTLXspFd4spcNK_
WchlZLRgkPK4jh6Z_X8JJkHxvQhpyouHQFyGxgBrl24x-_EB1zbWMhJthmm8DiKt-nzKaJz8Cju1-
HwCpg76CRqRsEz2hyKEpbb4M5KQSj3AsENCroVmQ5QIv3K2XNRkve4vjBmP6sV2b6GSY_UeRvPElA
7SUgBGTKbn-c0aYhBuB8plPhRTBa55_cFqAmNmavF1-fdMktJuIaH2f-
K0zZCzbHw54998T7kIWgyMsyGCAvynEB_khOqwT7tCjg5HQ8SIjdnRYW0kjZfjt5LJbGA-
PnRo8gPVQVGeYDP2vsSXhNJY94AitKCY1srcSsuYDrhNBKrnoJ1uEsMPVHsgFw_ZHMyAEaVQughSN
W4fm8q6_1Nv4zLutDITzmAL6a6i6-
WS6QRIs_4VUtwr5cXXIFDDeHVWeGcNivQ6W9urEUP4crguiq7z_DTiYaGfUksub-
T7mw0zU8ZoOSd5pUTpJLv-
IYIUAl6CscHvunnRLEKqpW1Sa1dcFZs5VP4AfR3mg7wX4Vlq1AHnpFxE2L1LZiKoTc9jDEOvTDkxr
86gMkwMm6RdyPF_q48AVJ1br8Qp88-4B84X52zZ5cw-IJYe-HiVJ29LpeYm340_rWivpy-
UB5i9TKlMrxf94y1okzZTPbP3_v1_XX0nE7RTLz98EA96euJ7l3EpbEqks7mh6i1FJNnvvlM_u29s
YobJ6PUT-
i1VlQnF_JBARKEz74pBXm1l5Y5Lo15rsIlaQHinUBCO8fHCHI59LAfKusN4JmodDqLYwkWijEL_sf
rC6LtrbXqpM1pw09zSrs_tS1RQ-LnWHuPrU5KLCzv53JKrh8lU_cdBowe_F-
Ib_Ui4bQ2FME-0mnyG0XijHUsrGMZ9dfowvIkr83JpqwlFOZAwMmSGPNPEJRw9kDshjotndUB5S1U
Cfv_U4IoVn7WgvxeCS-
BBxqyWfh7YTdf73EnmGwVYxVjlXaHCeeTZmUacnT4MQUAcbFjTq6BBlboAQGWP2FZWpd6HNnruv74
4VeWmfgLk9z5567wFhwuXMkmE2xvDo4wP80xutjUfsePx5YkLxhY1XsWqTZr19tInxJWWq8RLZsWP
mtq5wZ5ucBMasCLpOABenYZdSAcQNhC73wLS0Z2s1HQhBoIl7lr1p372LZs_Seu1u_8Fo7DoJqRpK
aNoc2_JUMmn7TUZS8zLyzxgeq8R8iNbRP20DwDBNXocsTDBKaQrtB-
QiEPySQtJa4G61XeNZyh5aGzfoWZ9OmjZG9pbbehcqwIrt-
ESjPyeT6sfSrvOfTZr7fBXwpUs2rS4BrlNse5g_h8CQiik8aaOTOEPkXiyg4s5DewRlgDZHS-3g-
YXPUIBNO62_HxknkMpkJvKW-
tkvDbgtxvy4nG80ul6W_KeRsoEKDTRYNKZWxXjZITNa0h6agnwNCJKEbFg3Qhre394c0i60mfP9YI
gKTXrCX3Yt2eX-6mPzYmLbSbV5jH69v6WZqYV2WAj-9DU0diR4hOfYQaJnBZhTtKb-
SQsYiFuN1BDJ3v9eM9K8hq91NBdCHVa-Thk9Dov-
JkcTZnZGRRyW5yXHUV4NOEltBXh8GkjjDvs5Yo3u-2rPCXjK1aGPSI1W8BaUJLQY5sbfAVCAuUHBv
-Vlh5Qamt-lgeKguhqTSuy-tjabOb5kiBOG7xGQt3z-XYXtnWFDCii-5h11XfZsQ-
xQxy8gSfdMz4hDK9Nw_VQt6fzWiQY0Th_dHzVki0MUfVfsDUjgblhD6j0wgbs3zdj-
GM3rtt8oit0wXx11bIOaOKgf07tP0wimVXMRqRWe7LCUAKTE5PkRKU1x_h4iusrzi5uwKDhc4SmRw
m6KssNrmCAkiNDZCREVKd3yMnrjA4PAGDzdKWVplcHJ6jKmrsbrEztHd9QAAAAAAAAAAAAAAAABIfM
EQ",
  "raw_to_be_signed":
"65794a68624763694f694a4e54433145553045744e4451694c434a72615751694f694a554e48
68734e7a42544e3031554e6c706c63545a794f5659355a6c424b52315a754e7a5a335a6d35595
36a49784c576435627a424864545a76496e302e53585469674a6c7a494745675a4746755a3256
796233567a49474a3163326c755a584e7a4c434247636d396b627977675a323970626d6367623
3563049486c76645849675a473976636934",
  "raw_signature":
"92723543ff422332c7e57cbde0a91ced654aa9970082d27798d7f41948f5b8b03a6170161497
d7921fb343152d125dd4202ef33c2894c0a4c347a66cb949858fc0ad6ffe9a1fae2112537bc1e
4bfd66e68902cbc1aa1cd2f696c7dc9421f76367f840d3fe0cb552d57b2e6e80c0ec3c378abd8
87582887d6272214ed138781ddb89eeba7d7325bc5c2c90b610ab7633c474c19b9d70813d9e6e
683f3617ab4cfe84fb0aa17a7d95e55892a80c98ef4ba3c48fff5618204b61dc1f2ff86b8fdb8
f4a0d315128f8c84a62b868f0a49e3b638a11ec415bf65de3d7c4a1316ad1e5e2a86c8a25becb
e1095dad4a7f0e166292c0ec1e3fe4876cfbe708266231edfeb1c4058a879aa8056ab540839a6
85bb3b00ada456dcd384bb34e17b0d449fce6023719c453646a7e5431b2c479b4025d387325a8
d9bc4054e1747db0dcdbae623f6982370e90835d2320978084607838031870151624O1b497530
dd54fe4a049868797572a7413465e3ad5e6bf0aadc32e4700d838f6c285941720d3990f283bfc
a178049f25a732466effb2e8fcf33e5714da3c179dcff0ec531bdc543e5af0bc7f9302aec01f7
```

```
354e12357029c95293537ce1c75b49df89e54c82dc4ee8d7549568fdfd0365f531afa252098aa
fcb8cf52a5d300d0cdde796a8a7216d431bce3e17021db00ddf8836520ef9d099bcdf97e5ecd3
b172aa0c6ee4dc807ebc92bdfb33e3dd8762bd59acd7509802ba981d2165bc5a37ce8e64e2179
f42ad5b5f56d2b6a83cc5e343843427eab4d3d09597b970de69d0ff1aae3e14481f0708f87b35
da90040796af0d30b1885d88cdfd96b4a403c98b458321667a8a1824cf0ab1d70dd12344a6113
5aa88513e3895a625e5cdbb2b4bfea338ca3eeeadcc48646120b85d9dcb7a1105b66033384d26
1db84a3205ea8e83c98ceac620f89b5f78f02bcfd0e5198c397b57a3c477bd77c1694750a0b79
ecb2c0d604d2721cb25e33e5af3fbadc0416255fd152b6a5dbe2ca238f5528b7cce3009aacfa8
05855cbc68c310396640100b93c83c3b6561ba762c29b66ae0497668b56eb7235f52d991fb91e
097448abfa452ee6213ae1ba743e0c928b882d1742f5b5d930bacd0eaec23a950e3bce9a41595
8774a51f77e56a54c3e57aa1b4919c79511594a6512201ee1d50d0899c891ce88cdf775e1c3ba
a9cc6cddcc310edce3936b25da486ff4607432cbe787e2105b9a0b7f2c1c75db4835798e171de
1c545f4df7ad1e42f9659bac5f58d0fe793d7b3e17046ffa851b53352b9506c6251fcf8a52e47
9faa4cff1d92f45ff16936847a14af6b33e583bfc4314230c4ebb7c6a188cc9f8e8e62879170a
37ae215b15418a89b9e24cb5eca45778b2970d2bf59c86564b46090f2b88e1e99fd7f092641f1
bd0869ca8b87405c86c6006b976e31fbf101d736d632126d8669bc0e22adfa7cca689cfc0a3bb
5f87c02a60efa091a91b04cf6872284a5b6f83392904a3dc0b04342ae8566439408bf72b65cd4
64bdee2f8c198feac5766fa19263f51e46f3c4940ed25200464ca6e7f9cd1a62106e07ca653e1
45305ae79fdc16a0263666af175f9f74c92d26e21a1f67fe2b4cd90b36c7c39e3df7c4fb9085a
0c8cb3218202fca7101fe484eab04fbb428e0e4743c4888dd9d1616d248d97e3b792c96c603e3
e7468f203d541519e6033f6bec49784d258f78022b4a098d6cadc4acb980eb84d04aae7a09d6e
12c30f547b20170fd91ccc8011a550ba0852356e1f9bcabaff536fe332eeb43213ce600be9aea
2ebe592e90448b3fe1552dc2be5c5d72050c378755678670d8af43a5bdbab1143f872b82e8aae
f3fc34e261a19f524b2e6fe4fb9b0d3353c668392779a544e924bbfe218214025e82b1c1efba7
9d12c42aaa56d526b575c159b3954fe007d1de683bc17e1596ad401e7a45c44d8bd4b6622a84d
cf630c43af4c3931afcea0324c0c9ba45dc8f17fab8f00549d5bafc429f3cfb807ce17e76cd9e
5cc3e20961ef87895276f4ba5e626df8d3fad68afa72f940798bd4ca94caf17fde32d68933653
3db3f7fefd7f5d7d2713b4532f3f7c100f7a7ae27b9771296c4aa4b3b9a1ea2d4524d9efbe533
fbb6f6c6286c9e8f513fa2d559509c5fc904044a133ef8a415e6d65e58e4ba35e6bb0895a4078
a750108ef1f1c21c8e7d2c07cabac378266a1d0ea2d8c245a28c42ffb1fac2e8bb6b6d7aa9335
a70d3dcd2aecfed4b5450f8b9d61ee3eb53928b0b3bf9dc92ab87c954fdc741a307bf17e21bfd
48b86d0d85304fb49a7c86d178a31d4b2b18c67d75fa30bc892bf37269ab09453990303264863
cd3c4251c3d903b218e8b677540794b55027effd4e08a159fb5a0bf17824be041c6ac967e1ed8
4dd7fbdc49e61b0558c558e55da1c279e4d999469c9d3e0c41401c6c58d3aba04195ba0040658
fd85656a5de87367aeebfbe3855e5a67e02e4f73e79ebbc05870b97324984db1bc3a38c0ff34c
6eb6351fb1e3f1e5890bc616355ec5aa4d9af5f6d227c49596abc44b66c58f9adab9c19e6e701
31ab022e938005e9d865d4807103610bbdf02d2d19dacd47421068225ee5af5a77ef62d9b3f49
ebb5bbff05a3b0e826a46929a368736fc950c9a7ed35194bcccbcb3c607aaf11f2235b44fdb40
f00c1357a1cb130c129a42bb41f908843f2490b496b81bad5778d672879686cdfa1667d3a68d9
1bda5b6de85cab022bb7e1128cfc9e4fab1f4abbce7d366bedf057c2952cdab4b806b94db1ee6
0fe1f024228a4f1a68e4ce10f9178b2838b390dec119600d91d2fb783e6173d420134eeb6fc7c
649e4329909bca5beb64bc36e0b71bf2e271bcd2e97a5bf29e46ca042834d160d2995b15e3648
4cd6b487a6a09f034224a11b160dd086b7b7f787348bad267cff582202935eb097dd8b76797fb
a98fcd898b6d26d5e631faf6fe9666a615d96023fbd0d4d1d891e2139f6106899c16614ed29bf
9242c62216e375043277bfd78cf4af21abdd4d05d08755af93864f43a2ff8991c4d99d9191472
5b9c971d457834e125b415e1f069238c3bece58a37bbedab3c25e32b56863d22355bc05a5092d
0639b1b7c054202e50706ff95961e506a6b7e96078a82e86a4d2bb2fad8da6ce6f992204e1bbc
4642ddf3f97617b675850c28a2fb9875d577d9b10fb1431cbc8127dd333e210caf4dc3f550b7a
7f35a2418d1387f747cd5922d0c51f55fb0352381b9610fa8f4c206ecdf3763f86337aedb7ca2
2b74c17c75d5b20e68e2a07f4eed3f4c229955cc46a4567bb2c25002931393e444a535c7f8788
aeb2bce2e6ec0a0e17384a64709ba2acb0dae608092234364244454a777c8c9eb8c0e0f0060f3
74a595a6570727a8ca9abb1bac4ced1ddf5000000000000000000000000121f3044",
  "raw_public_key":
"ba71f9f64e11baeb58fa9c6fbb6e14e61f18643dab495b47539a9166ca0198131c44f826bbd5
6e34e55db5e5e2d733485e39ea260fc6000c5ea4ba80d3455cde53b46f34482aedfd5450fc2e1
ba4f25d15f9c144242fb39bb52287189030c50498e1717b7c758b190a6748ea9aa3f7acaaf2c7
cb526ed717c9f79aeb84214fa5cd8ded92a0c3fa1558810f12c7050a367708d196cd24e5af974
904aed8e4ce8872e8696b0b7bca50e452cd7d30ea9a4adac0311d672c6bde8496240b07431463
```

```
708895cd9bafc31632d7397649388fdafcbf7d305a3de9a495eca7433a8f83ba0f0b25c413c6e
39c96eb7d691b34d37ce37f1eead1cf217e25ef34eecf3f7c60f84b8edfdde8405d4f832576c6
1ef98e0a2f28da187700953924f686b94614705bcf53d33fedd4348edddbdf28b5065e1f20775
043e85cf931f829179363a1a7e7404a838ec00086b0976386fe637c98244757e3f769ddd44674
71bfad670f9a05f8246ee50a7b1eaf87fc4069c3ae2aa2033258117792f0bcd49e083fd1bc749
6abff29cc94e4868b21214ed316525399a610fbdd4a80e7c80715f29578e2a84bb40bdddbd9f4
7a11b6e7da118a1b658d359e8aef55eb46b5376b5b655979984a922beebfc59bcd600d5309dcc
d72dbf0787db8ba757b537c1eafd5c0f50ea4bc9583549e2829a42c28cac248c96d78124c4715
9b18aedd754aba17b19d430fb78f633ea9d26f54a9bd50f8d8f6b73594f828976e7ea09c53bbb
9f11a56c9507fb89b9a5ebc037a37267a95f85b8d64ca97192b10a66f417b3f61fe9ca57130a4
8fd925eae2ab5502d571c8a51903c1d398f4c1f76a7e11743976afdbc697f23094a3cd761ff96
85de32e09fb3c28add453490300bc7c89dc01780096071722945775f264e1b0623bcf4619c712
c838761205d87691b75ef360196cbb9e9b92a0d4c4ed62326e5024d77510b8ee2c7426cc22eae
209dc9f13bde6bf08f5e7181bd3b459450b451a51539a715c21d67dd330eb5970db00d9edbfb2
822b036fa13bafeb86d8dc78866e3f8d43e53d78cca5595a6faf886b5dc112f1cf4adcfa87580
0d90b48883af97316fe1506873fc157e570eacbfd222868d14234101966afb6bf9940829253a9
53ada89fc756b6a849f70acb9838e69faa50bba75e3e89c2adb57e86d088ab9b04a28e6707091
72243ec5e0008a5ceaf3f8722f487302596ffd755ad1b82a49c34b3469515b46aa290cd86ee38
ea7a9be3f103610335b531cca333ddfe32b14510f4b07ef95fc6684e8c454a92c10dbb5d59c7a
7c63fb305fe881967d99e669eb632840582560bb403431d40f75a4954908482278292821f4ea9
1e42e78fa48caee3c836146dcfd738d117e92e9a15137d28e8e6a4b4622650cb413504cb3a335
d44beec5746c1c294b1e8cb99cb608d928f8ce3563632c521f23d13c61a8f61c01df8c96c7360
db4f3c68aa5d2fdd342a62ff3459c116389421ab43e8584c45882b50e6e4e96db6f0b8fde890d
5dbfadcd88690b449e64240ddb2023747f308363e301aa77757169fc6150628d5920b5aa1ab1c
8cbf44cb00e025d7879d72b479e3af5311c785725590da9c89b9fc3b8450769554eb44d203eba
2bbaef9cad2237011c2ea44eff00f299a48ffe28ca93ddf85f76608242ef8d6cc24610a1e2078
fcac4f9385c314905ecaa82e553916d94d1a7c1ec652aa08897083daa2ebb1775fbc471ae2777
7d7904ea9f1b92bcac3d8a3158426087b645b1108f0d65fec93789c053743ca14fd63d05e98b6
52df2b9c2ff9ce05f1940703ffb273f80e0e2732eca9960d981b4cfd3b7bb8045b3c3830546b9
dd8db0d"
}
```

Figure 3: ML_DSA_44

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "Suiu29qbfuaBaR4Ats-c6XQBePB_OpAxAwcTR_0KXVM",
    "kty": "AKP",
    "alg": "ML-DSA-65",
    "pub":
"QksvJn5Y1bO0TXGs_Gpla7JpUNV8YdsciAvPof6rRD8JQquL2619cIq7w1YHj22ZolInH-
YsdAkeuUr7m5JkxQqIjg3-2AzV-yy9NmfmDVOevkSTAhnNT67RXbs0VaJkgCufSbzkLudVD-
_91GQqVa3mk4aKRgy-wD9PyZpOMLzP-
opHXlOVOWZ067galJN1h4gPbb0nvxxPWp7kPN2LDlOzt_tJxzrfvC1PjFQwNSDCm_l-
Ju5X2zQtlXyJOTZSLQlCtB2C7jdyoAVwrftUXBFDkisElvgmoKlwBks23fU0tfjhwc0LVWXqhGtFQ
x8GGBQ-
zol3e7P2EXmtIClf4KbgYq5u7Lwu848qwaItyTt7EmM2IjxVth64wHlVQruy3GXnIurcaGb_qWg76
4qZmteoPl5uAWwuTDX292Sa071S7GfsHFxue5lydxIYvpVUu6dyfwuExEubCovYMfz_LJd5zNTKMM
atdbBJg-
Qd6JPuXznqc1UYC3CccEXCLTOgg_auB6EUdG0b_cy-5bkEOHm7Wi4SDipGNig_ShzUkkot5qSqPZn
d2I9IqqToi_0ep2nYLBB3ny3teW21Qpccoom3aGPt5Zl7fpzhg7Q8zsJ4sQ2SuHRCzgQ1uxYlFx21
VUtHAjnFDSoMOkGyo4gH2wcLR7-z59EPPNl51pljyNefgCnMSkjrBPyz1wiET-
uqi23f8Bq2TVk1jmUFxOwdfLsU7SIS30WOzvwD_gMDexUFpMlEQyL1-
Y36kaTLjEWGCi2tx1FTULttQx5JpryPW6lW5oKw5RMyGpfRliYCiRyQePYqipZGoxOHpvCWhCZIN4
meDY7H0RxWWQEpiyCzRQgWkOtMViwao6Jb7wZWbLNMebwLJeQJXWunk-gTEeQaMykVJobwDUiX-
E_E7fSybVRTZXherY1jrvZKh8C5Gi5VADg5Vs319uN8-
dVILRyOOlvjjxclmsRcn6HEvTvxd9MS7lKm2gI8BXIqhzgnTdqNGwTpmDHPV8hygqJWxWXCltBSSg
Y6OkGkioMAmXjZjYq_Ya9o6AE7WU_hUdm-
wZmQLExwtJWEIBdDxrUxA9L9JL3weNyQtaGItPjXcheZiNBBbJTUxXwIYLnXtT1M0mHzMqGFFWXVK
sN_AIdHyv4yDzY9m-tuQRfbQ_2K7r5eDOL1Tj8DZ-
s8yXG74MMBqOUvlglJNgNcbuPKLRPbSDoN0E3BYkfeDgiUrXy34a5-vU-
PkAWCsgAh539wJUUBxqw90V1Du7eTHFKDJEMSFYwusbPhEX4ZTwoeTHg--8Ysn4HCFWLQ00pfBCte
qvMvMflcWwVfTnogcPsJb1bEFVSc3nTzhk6Ln8J-MplyS0Y5mGBEtVko_WlyeFsoDCWj4hqrgU7L-
ww8vsCRSQfskH8lodiLzj0xmugiKjWUXbYq98x1zSnB9dmPy5P3UNwwMQdpebtR38N9I-
jup4Bzok0-JsaOe7EORZ8ld7kAgDWa4K7BAxjc2eD540Apwxs-VLGFVkXbQgYYeDNG2tW1Xt20-
XezJqZVUl6-IZXsqc7DijwNInO3fT5o8ZAcLKUUlzSlEXe8sIlHaxjLoJ-
oubRtlKKUbzWOHeyxmYZSxYqQhSQj4sheedGXJEYWJ-Y5DRqB-xpy-
cftxL10fdXIUhe1hWFBAoQU3b5xRY8KCytYnfLhsFF4O49xhnax3vuumLpJbCqTXpLureoKg5PvWf
npFPB0P-ZWQN35mBzqbb3ZV6U0rU55DvyXTuiZOK2Z1TxbaAd1OZMmg0cpuzewgueV-
Nh_UubIqNto5RXCd7vqgqdXDUKAiWyYegYIkD4wbGMqIjxV8Oo2ggOcSj9UQPS1rD5u0rLckAzsxy
ty9Q5JsmKa0w8Eh7Jwe4Yob4xPVWWbJfm916avRgzDxXo5gmY7txdGFYHhlolJKdhBU9h6f0gtKEt
biUzhp4IWsqAR8riHQs7lLVEz6P537a4kL1r5FjfDf_yjJDBQmy_kdWMDqaNln-MlKK8eENjUO-
qZGy0Ql4bMZtNbHXjfJUuSzapA-
RqYfkqSLKgQUOW8NTDKhUk73yqCU3TQqDEKaGAoTsPscyMm7u_8QrvUK8kbc-
XnxrWZ0BZJBjdinzh2w-QvjbWQ5mqFp4OMgY94__tIU8vvCUNJiYA1RdyodlfPfH5-
avpxOCvBD6C7ZIDyQ-6huGEQEAb6DP8ydWIZQ8xY603DoEKKXkJWcP6CJo3nHFEdj_vcEbDQ-
WESDpcQFa1fRIiGuALj-
sEWcjGdSHyE8QATOcuWl4TLVzRPKAf4tCXx1zyvhJbXQu0jf0yfzVpOhPun4n-
xqK4SxPBCeuJOkQ2VG9jDXWH4pnjbAcrqjveJqVti7huMXTLGuqU2uoihBw6mGqu_WSlOP2-
XTEyRyvxbv2t-z9V6GPt1V9ceBukA0oGwtJqgD-
q7NXFK8zhw7desI5PZMXf3nuVgbJ3xdvAlzkmm5f9RoqQS6_hqwPQEcclq1MEZ3yML5hc99TDtZWy
9gGkhR0Hs3QJxxgP7bEqGFP-
HjTPnJsrGaT6TjKP7qCxJlcFKLUr5AU_kxMULeUysWWtSGJ9mpxBvsyW1Juo",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws":
"eyJhbGciOiJNTC1EU0EtNjUiLCJraWQiOiJTdWl1MjlxYmZ1YUJhUjRBdHMtYzZYUUJlUEJfT3BB
eEF3Y1RSXzBLWFZNIn0.SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb
3V0IHlvdXIgZG9vci4.zmO9_0bLgJAegoVNymfRo4nGPK5lVtSFGnDbzfzYAD5mUEXpaBUg4itvZ8
```

```
rAUZi4HLb59QqDQSBSpMXC0axajXOMV_YttfmwGgC6FMyaMRZkx-
A92bGiNLutqX9jcwRLJqXjMkUGhz2YpHe_mV9QpxokRCH9K6jkyFZp4hZIwFXhRt1z0OGIa5rOoHK
sxOCAUZhTXKiASb3vk9lUASW0-Y58WKT4rVmst7_dvk7FVbe9A9I21IH-
Tqlg1zSMoI8ozh1aBSG92uPursBd5KRcOlJwhNUYJDgHScIHXM6Hzk6u98W5orKPHu1rDIK7rHJI4
Zrui4wBjmQLsPE01LcZHRx4zexDCTMCGSojbL1FiT9CU3oUep4oWOytTEAf2eCi3qDD0iSrp5IslC
ueoNjtGOFSnUKlsnCeiZF-
tNqTy1KpJ3ErTaNPcCzCvsEalhJwFa7NOWyQOEJUzcLaPY_VEFwcCX1Gk4bEI-1rLDiyZqkXgny-
U2oRnll0d3u-e2S_Rg-
_eL1H_XEbPs_km-822G7JY9li4muZ5KVvfQf_5hza1V4GweqvmeWuZL1gBU2HPS7x1tWL798ALOk1
rMnxsvBOPiSLxAEdPoIuw0_qMlKjTavJcDFaihgCgGMUk5SjU65IWQS9t4rgxv9Idu0OCsozo9iCB
qrVcnaOwUpkMhV6KeiXA7kQNcegVaMio40cjSyMiEkhGIOEOf8L6eohOh_bPPRYs-8NrZ-
VOBJCa0ubJcDU1cTuGNCa7nWWxAqfVjcMyNDx9XHBYBnSOcFNfMP7S9nvqw3KC50U_t2PH5SfwS9w
4DLvcgrlEP_gwSgOXuf-
i0tRGLQly3IMB7O8QOnkofyFaCUDZeurFkGTpoBfT6lzbJznQAMIDPNcWUsRlNTXsH7atC1nxl4xD
JLmmPLCxiErfxbCW5gMWox0kLDwfsFj57hsXG75cZ4jiBbq9b0VjD7Vkf8xlc06ExdzBhGXz8oJia
T5WHDsuzGtrFmh6diN1cO4Cxjr6KdNE8IlyxsfXxQ4AI-0ke3gMyi0DOGeHgHuNc-
JHD7oZ6njUMSTBkR1aUMNT7n_2nfFTDCdqW1HaMsMwIHfLOk6dayKXE1oMqY5Op8S5k_SAaknR0vN
xmhlTA5h3bZJ28NZxM6R7D00_eBEYrH20rmRP7G7kXKzLvmWeaKAh4oQHiqjVhgauiePDRiMmjx0O
hdQnMCtO8PWbx06SiviRn_5hswdVV08B48MVHqbM2AxCLLJYinC2Ep0302Uo0DI-
rTNZ1Znn58kM7VCskcxDLsH9AYvPz-HQr3H7Xg0ElwjYn-
jJXgZ_cdnLFt4_TuKQdpw_qhvyrNjOx0Mdc-1PrwoWqpA9sSv_pS5lwI2qNVHI2Vj2mZHByod1QUe
OQExf3SBjP_FHEAUzUu1OK8M-1SQZGzJT2su3a6ZnMnp0U5qdXyMONFoI2jJ2hDjt7QEQsLx-
rvaLxZMJtc2z0MHdwJGAC_kug7XjH3SWQZzBu7zzreIaSwr2A2oobeZiAydwb8LX2QsY9Jr_NphGA
MAqzrpkuaMyBd_pFTKMp9s0GYxwyG1ZD9uRuPI9imA4CS7bt-O8YvbWg6eQ-
qa9OqDlxNt3Xc32TniQFVxVxN6PDY33XXU-Rpvd1w47NZ48nkyJzjD8Xlbvk9p2ynxWHr-
Sto5HXZdru4j8ETUW7ri3mEG1m_dxAbAe2kVbsBp2I1vQppugbmRexuMRLdYFIKqNm0qpQoWTr_k2
t5KHnWolrSbFH7Usm8Pwyi4sNhh4_yRHADO2q2o19zCCx2plDSMeYI74CQPRGLlK_GLM4E5Bzfny3
E2eaE5_gQBTSGNHpQtJB0ipPwDjqsjDCXqXupCkRta1vxng4coi2-
vWYvKu6mq9HhdovHAaWrZRyvuPPI4ZDN_NkmfQR8HogR6NLVhLlRp1cwMArSSDA3f8Qlnjdbaeutx
RXvFnCCjBk79ws8VGdWAuRmIWgoEFeVAVxkJjJ07zOW8I3kNfB6pnxsZmJwWAGqWc1UlPmkNBstmS
XinAzbdl-W-
kn1XRDuhzTafHnkCbKS5XgJKsWD2FrhcnCaxxRxuxIGxijofjD4ihmJoYDFh1FYs9IcC-
szEfMSekanWOIZCHd1fVzTSbLr5bNaOXR2sO1muFX7w22m8pBVD3fyOHK2JnK4FBCnEBrruMIDaqq
u8Z4xesAHKfxY67w-25eUuvVCGL3xpXSyp90684ICkG4STztP1shLVsxKDA-37sKKplqemERlMPY4
vDM1Np8JlVawbSGIuom20g6p2KV_zpIPwx9vd1nAiaeZbryf3N5gtL-dOq-
c6uZhTCx9OLBtLGE3BcAmn5JFjMGQFxyTL07BluNu24Kf-lttGj9jzbwPZYrok-
SnMilXGFEqB3D3cKCOlWjsgg_3cUW1uMp4KlWQvkimV9Pd7cY70w607jcYBJ3MlFZ8EeWeYPZ9qu6
xwidA8XlLHxXxfLIJOgfpU8MTppfxdnMhqNSvH_Hx57oDphbUks5K1Z8-O4dSnNqQ-
ZWbhaAydYQFDKuUF6HYTAvaWhJmACxhTkTp2t6-P3bev-
FcdFIdszJC9LxWtJ96LY_GV4Qvp0hiIdyP1BukWNHtsXK2Rxres3_4Cndg2BOGxVcKZ9YpQDCUy76
GRbTCenqjD-SG5sVUEVha5yxbKArPr2-
Xpgk8cuZBRSAdmPNRdxCgUtldfCLeL7xhJvryMouxfQ75PMBaImHcsMd95075ePt_VkClUaUj55Y9
E81FbOEchPfud2w3TtSvRPvB8-RgY8sLJUAclxcUGE4PnKSZJ7TIBUtHD6uyZ0-
nC5KGxbXZsBEzUeHns4ix0Wmo6-6vAM4PGK3qRA1VAhtKXyvNcAfVccVi8KJMK9Mz2eIOXPATvyRy
34Ltrcg8tcgK0ftYqEWYpAZ2fVpZBXcYfTIinuLN0-
qLra388EZuu59jvmRD7mUv1msMWVMGVeBoNP3lJaJGGWK8iYyu4q7Grq-6WXr5qCz_7kwAtVJdb-
zW8U3jLJ3tRSYlyjlpzeVAGjDQ6Yni5y9x4BF-5QUqcoGMLLglyx2WOCELT8IW7nsV21QnqqAbtCz
Z76UtEdmUuEOTyqiKQZ0lrjMRm3YrCvJKxtR5thhTRka708NzBvwSRs-JxGG__EWjHhT-
aB4VL3IL_oz3mt3iQoszfA-
SzHcKU1laZMBuUCyxks6KiJgQGZRPXyaxxDtqZdaRP8Ic5CmuPeyu3kafi0L6LFijsUxnSGxTpgu7
hfvcmowQijfE9_ylvg8k_EbI2miG11giODVCYb7k9Yjyriwc9dSUUZ7XoiS24hWYUX6BGGQNN3wVH
PkDkOVSDBYTjto99ulquryx4K_UMCu9sQVNxBfMh8tLN7O9-
MXlnJbHfKfqFHiPGdIYOBpwuqJdAJiyiuSG3gJxMG_wuwNkBWoO--iOm6PIarCyvL8_P-
tuUfT4zIgjJJ3o6YJhbo-
q2K82ZFmHuILyzfDSGtHDZpZIR7XnRQWet90cJEHL5k653kvyEHJg0iUiE0iwNA5d_4gBq3vmw1J7
4hwAHx0Z_iYEcPS6hDGow8M8D7UJTZDkUV_86zj2YqGm_QC_aAeD__NP6sa61bI9-
gTOzvYc0JiExKTDjOK9fIvHaV-
HN4xr2vWner8o6jPyETvGM8D7aEezlUVOEFwALmhJPSMAq_Fk9JlcIUuC-
```

```
ITJZNtNz9Awfiru3wkPja1bXN76WAuRHjia0x5ptgMCy2py_vSHZybfIS85ZjsOQ-
i_e_niBzhyzXwzBaLEyEitbF4ZQx5c88lXKDMpe9tirAI6XAcqLf4UZkD8Wm2YV7hhVfxLQ1AWLek
WE9DZljCtE-
SbS1EWNGR8faXKCvaZznRyoqdWz8IN3w7KvaA_ZrEKkIXkkreztG6pI06DlDHCl_sU6rCOoyQf6y1
AY77Ob4SdkSRoBHGgR6Uv-
LrxHpyJ6trzccu0kqxubHrkW2yHcqe6enVf43zYwWKUeJJZ10bt3a92ziSne-3aj6v3guiKoJoLnV
_9h8rUF6zorTWE-
Tq58tYfb5SmGf4iCJ5cy9LTY0COIfwJtPkUmyBCZwUhWJnV24P5pOZPe_CckQ28xv5J7Zf4Bvqrq_
rhubFEhTJ5JvdMfz8Whc56WSHX7GRKEMqXVp3pHohBvOyT9BmotzIlibVklJy4gzkzUcjJJOld-
BOaM_cnMiHpoyKXSJAXTNwXngzEpbvDP2Y0fnrgqDpO3RR3gINaZLRmeG0WI4wWBMMfw8PHjpyV17
C_1hmfRI-
darbZcX7PD3N4Rw4lBACyk_wnOHBcAS-5cLZEzNmFmhc4iO4msz_seQ1N0drbB0NoUVWBmcY3pGC9
TiY6f6Pn-FBUnQkuBhIyPtgAAAAAAAAAABgwVHCUv",
  "raw_to_be_signed":
"65794a68624763694f694a4e54433145553045744e6a55694c434a72615751694f694a546457
6c314d6a6c78596d5a3159554a68556a524264484d74597a5a5955554a6c55454a66543342426
5454633593152535 87a424c57465a4e496e302e53585469674a6c7a494745675a4746755a3256
796233567a49474a3163326c755a584e7a4c434247636d396b627977675a323970626d6367623
3563049486c76645849675a473976636934",
  "raw_signature":
"ce63bdff46cb80901e82854dca67d1a389c63cae6556d4851a70dbcdfcd8003e665045e96815
20e22b6f67cac05198b81cb6f9f50a83412052a4c5c2d1ac5a8d738c57f62db5f9b01a00ba14c
c9a311664c7e03dd9b1a234bbada97f6373044b26a5e3324506873d98a477bf995f50a71a2444
21fd2ba8e4c85669e21648c055e146dd73d0e1886b9acea072acc4e0805198535ca88049bdef9
3d9540125b4f98e7c58a4f8ad59acb7bfddbe4ec555b7bd03d236d481fe4ea960d7348ca08f28
ce1d5a0521bddae3eeaec05de4a45c3a527084d51824380749c2075cce87ce4eaef7c5b9a2b28
f1eed6b0c82bbac7248e19aee8b8c018e640bb0f134d4b7191d1c78cdec43093302192a236cbd
45893f42537a147a9e2858ecad4c401fd9e0a2dea0c3d224aba7922c942b9ea0d8ed18e1529d4
2a5b2709e89917eb4da93cb52a927712b4da34f702cc2bec11a96127015aecd396c90384254cd
c2da3d8fd5105c1c097d469386c423ed6b2c38b266a917827cbe536a119e5974777bbe7b64bf4
60fbf78bd47fd711b3ecfe49bef36d86ec963d962e26b99e4a56f7d07ffe61cdad55e06c1eaaf
99e5ae64bd60054d873d2ef1d6d58befdf002ce935acc9f1b2f04e3e248bc4011d3e822ec34fe
a3252a34dabc970315a8a18028063149394a353ae485904bdb78ae0c6ff4876ed0e0aca33a3d8
8206aad572768ec14a6432157a29e89703b91035c7a055a322a38d1c8d2c8c88492118838439f
f0be9ea213a1fdb3cf458b3ef0dad9f953812426b4b9b25c0d4d5c4ee18d09aee7596c40a9f56
370cc8d0f1f571c16019d239c14d7cc3fb4bd9efab0dca0b9d14fedd8f1f949fc12f70e032ef7
20ae510ffe0c1280e5ee7fe8b4b5118b425cb720c07b3bc40e9e4a1fc8568250365ebab164193
a6805f4fa9736c9ce74003080cf35c594b1194d4d7b07edab42d67c65e310c92e698f2c2c6212
b7f16c25b980c5a8c7490b0f07ec163e7b86c5c6ef9719e238816eaf5bd158c3ed591ff3195cd
3a131773061197cfca0989a4f95870ecbb31adac59a1e9d88dd5c3b80b18ebe8a74d13c225cb1
b1f5f1438008fb491ede03328b40ce19e1e01ee35cf891c3ee867a9e350c49306447569430d4f
b9ffda77c54c309da96d4768cb0cc081df2ce93a75ac8a5c4d6832a6393a9f12e64fd201a9274
74bcdc668654c0e61ddb649dbc359c4ce91ec3d34fde04462b1f6d2b9913fb1bb9172b32ef996
79a280878a101e2aa356181aba278f0d188c9a3c743a17509cc0ad3bc3d66f1d3a4a2be2467ff
986cc1d555d3c078f0c547a9b33603108b2c96229c2d84a74df4d94a340c8fab4cd6756679f9f
2433b542b247310cbb07f4062f3f3f8742bdc7ed7834125c23627fa3257819fdc7672c5b78fd3
b8a41da70fea86fcab3633b1d0c75cfb53ebc285aaa40f6c4affe94b9970236a8d547236563da
6647072a1dd5051e3901317f74818cffc51c4014cd4bb538af0cfb5490646cc94f6b2eddae999
cc9e9d14e6a757c8c38d1682368c9da10e3b7b40442c2f1fabbda2f164c26d736cf4307770246
002fe4ba0ed78c7dd259067306eef3ceb788692c2bd80da8a1b799880c9dc1bf0b5f642c63d26
bfcda61180300ab3ae992e68cc8177fa454ca329f6cd06631c321b5643f6e46e3c8f62980e024
bb6edf8ef18bdb5a0e9e43ea9af4ea8397136ddd7737d939e240557157137a3c3637dd75d4f91
a6f775c38ecd678f279322738c3f1795bbe4f69db29f1587afe4ada391d765daeee23f044d45b
bae2de6106d66fddc406c07b69156ec069d88d6f429a6e81b9917b1b8c44b7581482aa366d2aa
50a164ebfe4dade4a1e75a896b49b147ed4b26f0fc328b8b0d861e3fc911c00cedaada8d7dcc2
0b1da994348c79823be0240f4462e52bf18b3381390737e7cb713679a139fe04014d218d1e942
d241d22a4fc038eab230c25ea5eea42911b5ad6fc678387288b6faf598bcabba9aaf4785da2f1
c0696ad9472bee3cf23864337f36499f411f07a2047a34b5612e5469d5cc0c02b4920c0ddff10
```

```
9678dd6da7aeb71457bc59c20a3064efdc2cf1519d580b919885a0a0415e5405719098c9d3bcc
e5bc23790d7c1ea99f1b19989c16006a967355253e690d06cb664978a70336dd97e5be927d574
43ba1cd369f1e79026ca4b95e024ab160f616b85c9c26b1c51c6ec481b18a3a1f8c3e22866268
603161d4562cf48702faccc47cc49e91a9d63886421ddd5f5734d26cbaf96cd68e5d1dac3b59a
e157ef0db69bca41543ddfc8e1cad899cae050429c406baee3080daaaabbc678c5eb001ca7f16
3aef0fb6e5e52ebd50862f7c695d2ca9f74ebce080a41b8493ced3f5b212d5b3128303edfbb0a
2a996a7a611194c3d8e2f0ccd4da7c26555ac1b48622ea26db483aa76295ff3a483f0c7dbddd6
702269e65baf27f737982d2fe74eabe73ab998530b1f4e2c1b4b184dc17009a7e49163306405c
724cbd3b065b8dbb6e0a7fe96db468fd8f36f03d962ba24f929cc8a55c6144a81dc3ddc2823a5
5a3b2083fddc516d6e329e0a95642f922995f4f77b718ef4c3ad3b8dc601277325159f0479679
83d9f6abbac7089d03c5e52c7c57c5f2c824e81fa54f0c4e9a5fc5d9cc86a352bc7fc7c79ee80
e985b524b392b567cf8ee1d4a736a43e6566e1680c9d6101432ae505e8761302f6968499800b1
853913a76b7af8fddb7aff8571d14876ccc90bd2f15ad27de8b63f195e10be9d218887723f506
e916347b6c5cad91c6b7acdffe029dd83604e1b155c299f58a500c2532efa1916d309e9ea8c3f
921b9b155045616b9cb16ca02b3ebdbe5e9824f1cb990514807663cd45dc42814b6575f08b78b
ef1849bebc8ca2ec5f43be4f30168898772c31df79d3be5e3edfd59029546948f9e58f44f3515
b3847213dfb9ddb0dd3b52bd13ef07cf91818f2c2c9500725c5c5061383e7292649ed320152d1
c3eaec99d3e9c2e4a1b16d766c044cd47879ece22c745a6a3afbabc03383c62b7a9103554086d
297caf35c01f55c7158bc28930af4ccf67883973c04efc91cb7e0bb6b720f2d7202b47ed62a11
6629019d9f5696415dc61f4c88a7b8b374faa2eb6b7f3c119baee7d8ef9910fb994bf59ac3165
4c195781a0d3f794968918658af22632bb8abb1ababee965ebe6a0b3ffb93002d54975bfb35bc
5378cb277b514989728e5a737950068c343a6278b9cbdc78045fb9414a9ca0630b2e0972c7658
e0842d3f085bb9ec576d509eaa806ed0b367be94b4476652e10e4f2aa229067496b8cc466dd8a
c2bc92b1b51e6d8614d191aef4f0dcc1bf0491b3e271186fff1168c7853f9a07854bdc82ffa33
de6b77890a2ccdf03e4b31dc294d65699301b940b2c64b3a2a22604066513d7c9ac710eda9975
a44ff087390a6b8f7b2bb791a7e2d0be8b1628ec5319d21b14e982eee17ef726a304228df13df
f296f83c93f11b2369a21b5d6088e0d50986fb93d623cab8b073d75251467b5e8892db8856614
5fa04619034ddf05473e40e43954830584e3b68f7dba5aaeaf2c782bf50c0aef6c41537105f32
1f2d2cdecef7e31796725b1df29fa851e23c674860e069c2ea89740262ca2b921b7809c4c1bfc
2ec0d9015a83befa23a6e8f21aac2caf2fcfcffadb947d3e332208c9277a3a60985ba3eab62bc
d991661ee20bcb37c3486b470d9a59211ed79d14167adf747091072f993ae7792fc841c983489
4884d22c0d03977fe2006adef9b0d49ef8870007c7467f89811c3d2ea10c6a30f0cf03ed42536
4391457ff3ace3d98a869bf402fda01e0fffcd3fab1aeb56c8f7e8133b3bd873426213129 30e3
38af5f22f1da57e1cde31af6bd69deafca3a8cfc844ef18cf03eda11ece551538417000b9a124
f48c02afc593d26570852e0be21325936d373f40c1f8abbb7c243e36b56d737be9602e4478e26
b4c79a6d80c0b2da9cbfbd21d9c9b7c84bce598ec390fa2fdefe7881ce1cb35f0cc168b132122
b5b178650c7973cf255ca0cca5ef6d8ab008e9701ca8b7f8519903f169b6615ee18557f12d0d4
058b7a4584f436658c2b44f926d2d4458d191f1f697282bda6739d1ca8a9d5b3f08377c3b2af6
80fd9ac42a4217924adeced1baa48d3a0e50c70a5fec53aac23a8c907facb5018efb39be12764
491a011c6811e94bfe2ebc47a7227ab6bcdc72ed24ab1b9b1eb916db21dca9ee9e9d57f8df363
058a51e249675d1bb776bddb38929defb76a3eafde0ba22a82682e757ff61f2b505eb3a2b4d61
3e4eae7cb587dbe529867f8882279732f4b4d8d023887f026d3e4526c81099c14856267576e0f
e693993defc2724436f31bf927b65fe01beaaeafeb86e6c51214c9e49bdd31fcfc5a1739e9648
75fb19128432a5d5a77a47a2106f3b24fd066a2dcc89626d5925272e20ce4cd47232493a577e0
4e68cfdc9cc887a68c8a5d22405d33705e78331296ef0cfd98d1f9eb82a0e93b7451de020d699
2d199e1b4588e3058130c7f0f0f1e3a72575ec2ff58667d123e75aadb65c5fb3c3dcde11c3894
1002ca4ff09ce1c17004bee5c2d913336616685ce223b89accffb1e43537476b6c1d0da145560
66718de9182f53898e9fe8f9fe141527424b81848c8fb6000000000000000000060c151c252f",
  "raw_public_key":
"424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942ab8bdbad
7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd366
7e60d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693
868a460cbec03f4fc99a4e30bccffa8a475e5395396674ebb81a94937587880f6dbd27bf1c4f5
a9ee43cdd8b0e53b3b7fb49c73adfbc2d4f8c54303520c29bf97e26ee57db342d957c89393652
2d0942b41d82ee3772a00570adfb545c1143922b0496f826a0a970064b36ddf534b5f8e1c1cd0
b5565ea846b45431f0618143ece89777bb3f61179ad20295fe0a6e062ae6eecbc2ef38f2ac1a2
2dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb8a999ad7a83e5
e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0b84c44b9b0a
```

```
8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a08
3f6ae07a114746d1bfdccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99dd
d88f48aaa4e88bfd1ea769d82c10779f2ded796db542971ca289b76863ede5997b7e9ce183b43
ccec278b10d92b87442ce0435bb1625171db5554b470239c50d2a0c3a41b2a38807db070b47bf
b3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d708844febaa8b6ddff01ab64d59358e6
505c4ec1d7cbb14ed2212df458ecefc03fe03037b1505a4c9444322f5f98dfa91a4cb8c45860a
2dadc7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891c9078f62a8a9646a
31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef0656
6cb34c79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d545365785
ead8d63aef64a87c0b91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fa1
c4bd3bf177d312ee52a6da023c05722a8738274dda8d1b04e99831cf57c87282a256c565c296d
0524a063a3a41a48a83009978d98d8abf61af68e8013b594fe151d9bec199902c4c70b4958420
1743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c94d4c57c0860b9d7b53d4cd
261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43fd8aeebe5e0ce2f54e3f03
67eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e0894ad7cb
7e1ae7ebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b3
e1117e194f0a1e4c783efbc62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b055f4e7a2070f
b096f56c415549cde74f3864e8b9fc27e3299724b4639986044b55928fd6972785b280c25a3e2
1aab814ecbfb0c3cbec0914907ec907f25a1d88bce3d319ae8222a35945db62af7cc75cd29c1f
5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a24d3e26c68e7bb10e459f2577b900
80359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346dad5b55eddb4f977b
326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a51177bcb089476b18
cba09fa8b9b46d94a2946f358e1decb1998652c58a90852423e2c85e79d19724461627e6390d1
a81fb1a72f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783b
8f718676b1defbae98ba496c2a935e92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea6
dbdd957a534ad4e790efc974ee89938ad99d53c5b680775399326834729bb37b082e795f8d87f
52e6c8a8db68e515c277bbea82a7570d4280896c987a0608903e306c632a223c55f0ea3682039
c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f0487b2707b86286f8c4f5565
9b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153d87a7f482d284b5b894
ce1a78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509b2fe475
6303a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdaa40f91a987
e4a922ca81050e5bc3530ca85493bdf2a825374d0a8310a6860284ec3ec732326eeeffc42bbd4
2bc91b73e5e7c6b599d016490637629f3876c3e42f8db590e66a85a7838c818f78fffb4853cbe
f09434989803545dca87657cf7c7e7e6afa71382bc10fa0bb6480f243eea1b861101006fa0cff
3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8ffbdc11b0d0f961120e971015a
d5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8b425f1d73caf84
96d742ed237f4c9fcd5a4e84fba7e27fb1a8ae12c4f0427ae24e910d951bd8c35d61f8a678db0
1caea8ef789a95b62ee1b8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5b
bf6b7ecfd57a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177f
79ee5606c9df176f025ce49a6e5ff51a2a412ebf86ac0f40471c96ad4c119df230be6173df530
ed656cbd8069214741ecdd0271c603fb6c4a8614ff878d33e726cac6693e938ca3fba82c4995c
14a2d4af9014fe4c4c50b794cac596b52189f66a7106fb325b526ea"
}
```

Figure 4: ML_DSA_65

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "tRn1JNIkgMsABVQBlXeDHxAIcclh-2IX0UdDEzPt5XU",
    "kty": "AKP",
    "alg": "ML-DSA-87",
    "pub":
"5F_8jMc9uIXcZi5ioYzY44AylxF_pWWIFKmFtf8dt7Roz8gruSnx2Gt37RT1rhamU2h3LOUZEkEB
BeBFaXWukf22Q7US8STV5gvWi4x-
Mf4Bx7DcZa5HBQHMVlpuHfz8_RJWVDPEr-3VEYIeLpYQxFJ14oNt7jXO1p1--
mcv0eQxi-9etuiX6LRRqiAt7QQrKq73envj9pkUbaIpqL2z_6SWRFln51IXv7yQSPmVZEPYcx-
DPrMN4Q2slv_-fPZeoERcPjHoYB4TO-ahAHZP4xluJncmRB8xdR-
_mm9YgGRPTnJ15X3isPEF5NsFXVDdHJyTT931NbjeKLDHTARJ8iLNLtC7j7x3XM7oyUBmW0D3EvT3
4AdQ6eHkzZz_JdGUXD6bylPM1PEu7nWBhW69aPJoRZVuPnvrdh8P51vdMb_i-
gGBEzl7OHvVnWKmi4r3-iRauTLmn3eOLO79ITBPu4CZ6hPY6lfBgTGXovda4lEHW1Ha04-
FNmnp1fmKNlUJiUGZOhWUhg-6cf5TDuXCn1jyl4r2iMy3Wlg4o1nBEumOJahYOsjawfhh_Vjir7pd
5aUuAgkE9bQrwIdONb788-YRloR2jzbgCPBHEhd86-
YnYHOB5W6q7hYcFym43lHb3kdNSMxoJJ6icWK4eZPmDITtbMZCPLNnbZ61CyyrWjoEnvExOB1iP6b
7y8nbHnzAJeoEGLna0sxszU6V-izsJP7spwMYp1Fxa3IT9j7b9lpjM4NX-
Dj5TsBxgiwkhRJIiFEHs9HE6SRnjHYU6hrwOBBGGfKuNylAvs-mninLtf9sPiCke-
Sk90usNMEzwApqcGrMxv_T2OT71pqZcE4Sg8hQ2MWNHldTzZWHuDxMNGy5pYE3IT7BCDTGat_iu1x
QGo7y7K3Rtnej3xpt64br8HIsT1Aw4g-QGN1bb8U-6iT9kre1tAJf6umW0-SP1MZQ2C261-
r5NmOWmFEvJiU9LvaEfIUY6FZcyaVJXG__V83nMjiCxUp9tHCrLa-
P_Sv3lPp8aS2ef71TLuzB14gOLKCzIWEovii0qfHRUfrJeAiwvZi3tDphKprIZYEr_qxvR0YCd4QL
UqOwh_kWynztwPdo6ivRnqIRVfhLSgTEAArSrgWHFU1WC8Ckd6T5MpqJhN0x6x8qBePZGHAdYwz8q
a9h7wiNLFWBrLRj5DmQLl1CVxnpVrjW33MFso4P8n060N4ghdKSSZsZozkNQ5b7O6yajYy-
rSp6QpD8msb8oEX5imFKRaOcviQ2D4TRT45HJxKs63Tb9FtT1JoORzfkdv_E1bL3zSR6oYbTt2Stn
pz-7kVqc8KR2N45EkFKxDkRw3IXOte0cq81xoU87S_ntf4KiVZaszuqb2XN2SgxnXBl4EDnpehPmq
kD92SAlLrQcTaxaSe47G28K-8MwoVt4eeVkj4UEsSfJN7rbCH2yKl2XJx5huDaS0xn2ODQyNRmgk-
5I9hXMUiZDNLvEzx4zuyrcu2d0oXFo3ZoUtVFNCB__TQCf2x27ej9GjLXLDAEi7qnl9Xfb94n0Ife
VyGte3-j6NP3DWv8OrLiUjNTaLv6Fay1yzfUaU6LI86-Jd6ckloiGhg7kE0_hd-
ZKakZxU1vh0Vzc6DW7MFAPky75iCZlDXoBpZjTNGo5HR-mCW_ozblu60U9zZA8bn-
voANuu_hYwxh-
uY1sHTFZOqp2xicnnMChz_GTm1Je8XCkICYegeiHUryEHA6T6B_L9gW8S_R4ptMD0Sv6b1KHqqKeu
bwKltCWPUsr2En9iYypnz06DEL5Wp8KMhrLid2AMPpLI0j1CWGJExXHpBWjfIC8vbYH4YKVl-
euRo8eDcuKosb5hxUGM9Jvy1siVXUpIKpkZt2YLP5pEBP_EVOoHPh5LJomrLMpORr1wBKbEkfom7n
pX1g817bK4IeYmZELI8zXUUtUkx3LgNTckwjx90Vt6oVXpFEICIUDF_LAVMUftzz6JUvbwOZo8iAZ
qcnVslAmRXeY_ZPp5eEHFfHlsb8VQ73Rd_p8XlFf5R1WuWiUGp2TzJ-
VQvj3BTdQfOwSxR9RUk4xjqNabLqTFcQ7As246bHJXH6XVnd4DbEIDPfNa8FaWb_DNEgQAiXGqa6n
7l7aFq5_6Kp0XeBBM0sOzJt4fy8JC6U0DEcMnWxKFDtMM7q06LubQYFCEEdQ5b1Qh2LbQZ898tegm
eF--
EZ4F4hvYebZPV8sM0ZcsKBXyCr585qs00PRxr0S6rReekGRBIvXzMojmid3dxc6DPpdV3x5zxlxaI
BxO3i_6axknSSdxnS04_bemWqQ3CLf6mpSqfTIQJT1407GB4QINAAC9Ch3AXUR_n1jr64TGWzbIr8
uDcnoVCJlOgmlXpmOwubigAzJattbWRi7k4QYBnA3_4QMjt73n2Co4-
F_Qh4boYLpmwWG2SwcIw2PeXGr2LY2zwkPR4bcSyx1Z6UK5trQpWlpQCxgsvV_RvGzpN22RtHoihP
H74K0cBIzCz7tK-
jqeuWl1A7af7KmQ66fpRBr5ykTLOsa17WblkcIB_jDvqKfEcdxhPWJUwmOo4TIQS-
xH8arLOy_NQFG2m14_yxwUemXC-QxLUYi6_FIcqwPBKjCdpQtadRdyftQSKO0SP-
GxUvamMZzWI780rXuOBkq5kyYLy9QF9bf_-
bL6QLpe1WMCQlOeXZaCPoncgYoT0WZ17jB52Xb2lPWsyXYK54npszkbKJ4OIqfvF8xqRXcVe22VwJ
uqT9Uy4-4KKQgQ7TXla7Gdm2H7mKl8YXQlsGCT2Ypc8O4t0Sfw7qYAuaDGf752Hbm3fl1bupcB2hu
IPlIaDP6IRR9XvTYIW2flbwYfhKLmoVKnG85uUi2qtqCjPOIuU3-peT0othfmwKQXaoOqO-
V4r6wPL1VHxVFtIYmEdVt0RccUOvpOVR_OAHG9uHOzTmueK5557Qxp0ojtZCHyN-
hgoMZJLrvdKkTCxPNo2-
mZQbHoVh2FnThZ9JbO49dB8lKXP4_MU5xAnjXMgKXtbfI8w6ZWATE_XWgf2VQMUpGp4wpy44yWQTx
Hxh_4T9540BGwG0FU0bkgrwA_erseGZnepqdmz5_ScCs84O5Xr5MbYhJLCGGxY6O5GqS-
```

```
ooB2w0Mt87KbbE4bpYje9CAHH8FX3pDrJyLsyasA3zxmk4OmGpG7Z70ofONJtHRe56R5287vFmuaz
EEutXn81kNzB-3aJT1ga3vnWZw4CSvFKoWYSA7auLgrHSHFZdITfOrgtmQmGbFhM9kSBdY1UCnpzf
65oos3PZWRa2twfUxxLAnPNtrxpRGyvtsapw7ljUagZmuyh3hLCjhAxYmnoE1dbyIWvpCqSlEtVjL
1yb_nuLEzgvmZuV02fHxGuWgHTOMVGXpf81Rce3eoBK3lapW1wkzezlk3tcA2bZOtA9qbxdsbVR37
kemzQ9K1e3Y0OWhtSj",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws":
"eyJhbGciOiJNTC1EU0EtODciLCJraWQiOiJ0Um4xSk5Ja2dNc0FCVlFCbFhlREh4QUljY2xoLTJJ
WDBVZERFelB0NVhVIn0.SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb
3V0IHlvdXIgZG9vci4.hmMrKkUgZwGPQV_WUoXUVq_Z9WOenDZbfMmHpKritl0btWi29TC8eIyQyT
1FAuW2kg3h6ALsvCrjX5tn3QKFQZYC0sBdRt0VNiDm0BjyJ4jWcomSCgb0-cGXaLlODAz-
njGridYfO1DpGMwHHshuKuvECv4qnX3XgZPE-6C8La43TZrYO8brzBXGiuyGMLq-
TSmXavOeiadtpp6iTUqJDBgQSYvPB6PvipeCPlQH2ZQi8qkraxspi0lgy8Jh2aRYj44DX2ZKq-Ml-
hfBJB4iHRpWmwPpEH7Ed4LkBIlaqZoPccrPgpGQpyz4_FcahrJc8CGGtTO5I34o5BcuZej7WOQvJ6
mRmvYqIrYwoLs-3_YFZkVdX4KU38oprMvAHjObOhy_vZZArMnCgfYlCKrANbhOZG8O0BXgqow5Bqv
_oRIztGQZMrivp_1CS0hELarwkwjdqyH5R747ndV26IQkeyn6y9daXRZIWxaC9KmAaDSm5-
YsRVpiAAr0QmfaV51z065_r5qZmOMFIBERVi9Bbm_Z7ipJkoIL2SqVsePATfHeWB8huFpVFxdeEkJ
UPDuBtthax0HhxpRuECpFNJf2xA70Hp5C5VZIsi5EO21HuRpixiNKmXP5whhsn_uv_B7R4f4DX6X6
A53lFrUfpFIrTfOQvBAvmEUUTSGcPeT-
F7f_1lz34uFyN3ZT4FCeCh4n4yyZY1fSPVMNtOfK8GrLrRoWdi8gMk30oTKgb9zFkFU7uZhVEVRV8
6A_060bgFSHWDz5dlXLfyCoJsbsHlO9WBibTCkrMv6lnjh4czprro2prRtJAJB2jVwS1dv2mo4wP1
lFYqY63yM9I9deU4fxy6mkwig7XwcVJskg8jX_0agATqmrKfYWMI4yGQ9fciYacgN8X2uSHqiPU1c
gQ8VUGsSAsw4POdZpmcUt_DacVLT8-
qwnq6NWpm8bqm_uUQu3JjqcHKLz7zWKopeLG_ZY7a45IqUQpwbMg9ICE1ZNTe5nsMHAJnevgLfWk1
4wnvVQyRVvlSvatdUTg0EjBc6P35a4lY12vIOq2ENpA-
m52TfXeXxXK0vtZfT9SY33thi4EfZABWL_jQyiio6b6Akrh6_PgQ-
bh2H2Fpu8Z3GImrbHodcbnqFpmKYlMLwxDHnKPxY7PpyyV8HsWfEjqVlAX56stAIIG4_owwzMZMcF
wgucAP176TwjaXJqm9v2-
DXisD2cNjyGlJ_rec670rv61thjiJF2uZrB9Z2zoQVYnc3Y9sJMMPPmunUcXpNVZWSsPlFDoPa1AB
oFnRbP8rO-qbNGP5N7xY2DuPRYOp3CdyxeyDPmGBC2556FNeLRj-
PhPAkd61fgXsQZyS9N2jHmFUIKbL8o-
e3bQnqW7ebEn7zAjS_LQ2DtgIdIneUu84hh8AduoW9ky_aOpqvBUmdnHUwZHQiSSdeCPnEOssVBbu
Dd3gbcQf_VWvplwcjTTrJPsqqZpirjfVGPFUCVAz6kD0vhFcvTdQt6DGqys61xg_VOfj6wxpKsXuX
Duqwaeb4KpGniHx-23nECgKG86N_1BBX8RRAvYnksxIIxIxgyrng-
y44CV9FL_wGfP0Plx6JjSUFOL1gDZTc5NrAPoOztEo1FbJ2Lq8gqBR9Ku9Yza3aYANAJQvAraTXzA
0t1j6qcmh-WtXeI1GE-8neOJtlRVbzT5RvPiRJZAVmu9Pg97wbLLQNPJoqIYp-
c9mieGsDxAi75C2M1ArRnCa4kJJXrupgzQzzFefWyaRkIvC2MP9MwB_Z_NY3mp3opcNlT1TdKLr1s
ncLUkk3qJ0Pwyr-5dsKrC6aenapBHO7G0OnA0qTi8-Oy91VqJYYcVjcOUQaxNeMtnk-
pLJL7j3MzqNiDkc-OfR19fcWvDmmd9Z8wtj20khL4mTDn7qTUo-
PsVR7GnpqkImmEmE8sa4ZlPHa4_IcZGFbdcwp9xuOndINlzWGrIKywFPQ1x26zXDEa7fOx5f01aX8
dIU_KWNAGdaZxPIlqLW5qbC6dipSqf9NwblZLJs5DCiLV8nHS-
QM26xQJVUNH22n_3Z_8z1SA8AX8d7j0-
g1Pf7NZC8e8Ipnm4B3YGpA7nn471aTbJb4OUamfgys17MV_hPDK_f7FF7NXp06-
dtVYDmcs-87ZkrDuluOkUaRivKULwjEtSbiiKZAKirGfAOuwyCbbzygEpqYvEztABSmDYd_F_autk
lob_0deKuvvRYFpVCaxeaYQ7WIkpfBbMxeh9Qci7kPfgyB5H9ajWEJV3fgRk10Q1RaWyTUddQ_jWa
luiDa3GD_t39sUrG7QhXc2Oz1NPPNoY6-
A4jFbFCtXSF1muztqy0xaworcNiHY18yeL4Cw2iYLJ1Q3O4NnFo3E-
wIXmYF4CLxZifr2Jkd6Ix1w-
wlsN6vyCcDs8JeAgeJn0_Oahk1mgvRhVz8FFeidSdFqJBxGKbfZ32F_auJwrsLyjN_ShxTSFofyKQ
y2XCfoVMko4eu5o6md66xBmjZvTvItXL7f-
eD0JxISBsBkZG3mFrApZKbdpI1lEa681ZbCxRTYpxUR7McTbs0Q5S9PCN5ElUz_axfeupIIbCTE4S
0-
ZQuIdQcQ2pn1j-4t2c04jtLE6WFI-1ASBCedlZmrZUiRegbezE01hMiFnfN32BhBu7ZcnlBCdWwj9
hUfpEduJIgaA3acXhysGs40nqRzR9imvX9CBQYJZjrCHr-
wORF6svmvF5FADRgwbM7Cc9puJgLBiQwXrhD43B6kjX_OXi5O2UNZFkAPr0WONBJsip8CgR6pt1u_
mIKlIrYM9kM-idJGGT0DZ9UU4LMx0-9_2KCCkjDqgYN1rS9DA__GP9tS3dJ-
XLSlk2URQuoHm4Xubv4vwgjUS7JzAxcQWHB0HtHFoZ3-tYVw_GRbRwyODm3E-N5O3L_R-
```

```
pva9fvlPjkCNMrf2IlxAxBKML1gCxsSqhFr5yoPeW40LTxMF_dYPNLjC3l7mRRl_wfY_FhvayI7hr
gCYfMgWeb-cXyx5eXumt9lMFOD3dQtEG1IUbdE7pVXG-
barWK0Zl43DtQMNQzoCK_BLxfCsambyRRcI6E4QTfqe5lWtVf8Wi4KproenWyCjjzEjJQdWw4g-
ae_bjGjfZCp38RgsXtWgI_tuzKyRF5WwjyN9VEoRXd8W2DctmBejHF2XDYzbMFkJ-384SokPX6int
nlqBGMs0ssxriJhsFOA-vgDra6REx3DUMb8_u_Umc-zp4E6isX4D-
eRYgElmj0ez945nqxp3YliO8mRLMW6E4OupLthfw4vmK3YqTAuXcnGxYrf7JqAkMfz5uAPi0SqPWD
QZq7ycu9BmkMXAIhMb19XBDjL7hZGDwDRrn9yBBcYlPaFPNXjMJWJH_xxUKNsTFGg5-
J_WdxXi8Zn6tDMxbxqqjIpw_FUaM00jJ2MhpbkzhEx7X85pBR47ScRgr6WJpf4ZLSFuV7NT1WI3PI
Ba_bYeCiq29fp3ShM-1bRFdJG_lGZd97TuAMF_QU6-KDXBv5i8kUZ1NXdJUz-
YaA0RRVNFgMGM5n0pKB5IFncAPK-taTzHLIZJ9uuBdP2y2Hxwbw8YQlmy2-
MT5XE5Ae_9kxuvIIlSzjpfLN9012HSnX4tZ8x3aWwof3E7s3jjzw7qbBtoUkYYpIGVOKf2EpmhEqe
vSlXYWpBYN3X2ZYjsrA9CL9PTvrPdyWLwKBmfh7cDJbjNXJSQLeKL7oHzicrllABzR9Ckkz7b24XG
V1Klcat_Og4oB9qxiO2zJZWz2GDTAL0hosUlHLWnrQYvqFzzdIOzGlifwIyGgoRNb44IRMzzsErxu
oqkdjZewVc4PzruHRlV3cWK6M7ZUiWLtxtMzas2sfAERy8BdS7ISLzj5PERoWyYXSW-898WD3ze5M
JcpSsAYNEmPCBtdxF9l-
Qz1LxuDa8hOCQ2Wzef1a2WFF5pCBaZRcAK_kef65xRst6WFpjWZGCLZUqHBhFDLEOd7Ikbw7d9V8d
c4nAO65NQcxfT9JDUZadS2jmQJip8GLD4P9lGS1Ry-8rHCnMN7zXDp43TfyYhSgv9uj4xKi2wmAMM
YBl0n2RNemx8nt-
K_dknGgYYGOybDkg2uAUoXdxP33KfiRjbRpYqZVAiq0S45QLAIxxGiDJoZRnyIscdM6lryQtXj0PO
67vRf6ifxC3wLv97HHUKergpXcAg-4_rNj_Zx_xiHMfCAe2q3DG1a_DcSmu5u1OPkBHmzHB9Vs8HV
0E2-z44sl3Exqb5L8pMYpDnZ7QW-Qb1-S-
zoESUy__AKhkRWPC7GmvmJJJHur6SRGSK0X2KyszkEYoe-8NhwpvLrYnNuVk7QknBS91KH2q8C0B8
FKqcY40S5ILkImP9iOGIXYl5ZVRleoDBpH9BootWH2az5l7c_e-vfBGs7XpudoAq5wzhe_-
AMBvKPCm0BoCX5B_NGUasXvEWobqUb61mpKCuVJdzVtexk-
m8Jfvmdc8ooPJEYD_oosY5_S1LuHoc7GHLnoYdDVb2FhIPhOJCLQCef-
Y3dtNThqOEo534Zg7R72nSeSQhdQ1hcBUsc50U2oF9OlOnV9z5hsfNwIxdUO9bdoXRYFmosmtpmDf
GxAem0s5iPJ0EJ_8szlaX2pi6k6VP-ci-n7J8pEBwL2R3c-
ei2iqB7JdLi7Gg6iXVMpQIFTxswh0HbgGtyZXgR_-
AM91XRszm_kAlqAHTAJ7B-0Z5bJgMGEY2StBdhGzel_gNPVaxemC3DT0904GbCU2Z3avUHcedebI0
2_MdILdQxyXbw145KjqC15CqeaG--6x6WzpAuSjrFQRuz6Z5UyibW6Ay9R3P25c-
gwmaRM8rPW5YkQtQdfzrtvGZ6wyhIcBXvbpU02OoChfRDF4xI2LvnaW3g6hQIUGe5lueI13ArYRAh
ZC0LHKPuVfv5OKeMqxYRtcN3YK6Ddc1t61rsA7MU1cAKzOGsiQ7aNyNBQHOV6z-W4-
ws_DnZKYRMz0D_hwbeHO0ZKhciXng5VDCX4hyb47LExmO5N1mfihN3iHEkX_19rIgunfkSb9gd9B_
AaazAttBEPPLtbsoZneQXBRl3PWiDpC_yXiLTWAd13AOBYHzBMKeJ4hplUqsAGTaGSztbpvV92wz_
YX9kMEucHMu5hoM-
TJbuWoheiiiKSFBNRK_g_rqXZo1UZjDOnHpHGJxOnlJBPp94Zvwh8sKLOpOd4qeOMLbnYKiag00al
5x_3fBXq-
KI0Y31OJfgDdCaKAQ0DUX71HN6XDOlvU1Iwh48iASJHdQGDmjhcS8YoeX9omwPiYhcbGJGzEVrn3H
7h24eIf_7bVRpicMhjwghB0xtqTT0eVam1l8kr1-5kem7Dr2Kyqm2HpEwbi3KPXKYDXQRbHElEhaz
MCYr2wnjx_Bx2ai2uZa8uQyjN1zh1cjWHH0TicL2eAyc6YPKfKpmc5QwLrgT0ddQDhvXkCkN50fOR
1Sbl56iFoAL8goFl3QA5wBk51vsDsquEt7nlz6sGTHzknENb-eEayrXnw-
Q5FueFwqzoJpUrEYDXTxgOU8XVhrPv0Ot-
BO6ORfzn3_1gREcHjhrc6RdF01NNqyzyVG0BdckywvAnzUGskWdCfP62dKdx46lAIRVPd3xG4tVia
Q79GAeMVnqSeCLXbOyqfnJwhOT2fgQzLwxcj1tqGBBd3Pfx2d5-10WiL_mis0ven6golqaLq1EQsv
eb9AJpkYgJxdBeyHZXxNLMh4_XAuK1ZIs9F8Cz1vFEVcAFipev-cFyRvsdcNI2-
HK2nOGkypEcuVATyLtA0jKeyPtE4TJ3_l8KXltEZjWycQAd_8Tj9is3wisC8bfzjll8UBjFZp-
rzmCr8kA4cZih9gl27TiCmhyKhgMfDUIUmuDL_Rn9DLxEAT3Ebl1SW0ToCciNtKTH9oO-wnkPd-
jg1HCooLcg-
K_QkOTptJNZRFbXpooKqwH5Z9qsCxurZxnS_MscnE0qTa4EqrlpiDnj4FBs4q9SEPlKequfYzFmjQ
is1iwsReutf6pHmsvRmz9gx5vd6NMIkI05IeLNDElvlOGD04m1vR4ZISdmdHaAgaW9_AUPGx0vP1R
qe36cvebwUYSnzdbZ7y1s7PH7GXF5r7zNEzY9bHmXvsjb3N_u9BkenwkQfZGS6ez0AAAAAAAAAAAL
GSAlKzg7Qw",
  "raw_to_be_signed":
"65794a68624763694f694a4e54433145553045744f4463694c434a72615751694f694a30556d
3478536b354a6132644e63304643566c46436246686c5245683451556c6a5932786f4c544a4a5
74442565a455246656c42304e566856496e302e53585469674a6c7a494745675a4746755a3256
796233567a49474a3163326c755a584e7a4c434247636d396b627977675a323970626d6367623
3563049486c76645849675a473976636934",
```

```
  "raw_signature":
"86632b2a452067018f415fd65285d456afd9f5639e9c365b7cc987a4aae2b65d1bb568b6f530
bc788c90c93d4502e5b6920de1e802ecbc2ae35f9b67dd0285419602d2c05d46dd153620e6d01
8f22788d67289920a06f4f9c19768b94e0c0cfe9e31ab89d61f3b50e918cc071ec86e2aebc40a
fe2a9d7dd78193c4fba0bc2dae374d9ad83bc6ebcc15c68aec8630babe4d29976af39e89a76da
69ea24d4a890c1810498bcf07a3ef8a97823e5407d99422f2a92b6b1b298b4960cbc261d9a458
8f8e035f664aabe325fa17c1241e221d1a569b03e9107ec47782e404895aa99a0f71cacf82919
0a72cf8fc571a86b25cf02186b533b9237e28e4172e65e8fb58e42f27a9919af62a22b630a0bb
3edff60566455d5f8294dfca29accbc01e339b3a1cbfbd9640acc9c281f62508aac035b84e646
f0ed015e0aa8c3906abffa11233b4641932b8afa7fd424b48442daaf09308ddab21f947be3b9d
d576e884247b29facbd75a5d16485b1682f4a9806834a6e7e62c455a62000af44267da579d73d
3ae7faf9a9998e305201111562f416e6fd9ee2a4992820bd92a95b1e3c04df1de581f21b85a55
17175e1242543c3b81b6d85ac741e1c6946e102a453497f6c40ef41e9e42e55648b22e443b6d4
7b91a62c6234a9973f9c2186c9ffbaffc1ed1e1fe035fa5fa039de516b51fa4522b4df390bc10
2f9845144d219c3de4fe17b7ffd65cf7e2e172377653e0509e0a1e27e32c996357d23d530db4e
7caf06acbad1a16762f20324df4a132a06fdcc590553bb99855115455f3a03fd3ad1b80548758
3cf97655cb7f20a826c6ec1e53bd58189b4c292b32fea59e3878733a6bae8da9ad1b490090768
d5c12d5dbf69a8e303f594562a63adf233d23d75e5387f1cba9a4c2283b5f071526c920f235ff
d1a8004ea9ab29f616308e32190f5f72261a72037c5f6b921ea88f53572043c5541ac480b30e0
f39d66999c52dfc369c54b4fcfaac27aba356a66f1baa6fee510bb7263a9c1ca2f3ef358aa297
8b1bf658edae3922a510a706cc83d20213564d4dee67b0c1c02677af80b7d6935e309ef550c91
56f952bdab5d51383412305ce8fdf96b8958d76bc83aad8436903e9b9d937d7797c572b4bed65
f4fd498df7b618b811f6400562ff8d0ca28a8e9be8092b87afcf810f9b8761f6169bbc6771889
ab6c7a1d71b9ea16998a62530bc310c79ca3f163b3e9cb257c1ec59f123a959405f9eacb40208
1b8fe8c30ccc64c705c20b9c00fd7be93c2369726a9bdbf6f835e2b03d9c363c86949feb79ceb
bd2bbfad6d863889176b99ac1f59db3a105589dcdd8f6c24c30f3e6ba751c5e93556564ac3e51
43a0f6b5001a059d16cff2b3bea9b3463f937bc58d83b8f4583a9dc2772c5ec833e61810b6e79
e8535e2d18fe3e13c091deb57e05ec419c92f4dda31e615420a6cbf28f9eddb427a96ede6c49f
bcc08d2fcb4360ed8087489de52ef38861f0076ea16f64cbf68ea6abc15267671d4c191d08924
9d7823e710eb2c5416ee0ddde06dc41ffd55afa65c1c8d34eb24fb2aa99a62ae37d518f154095
033ea40f4be115cbd3750b7a0c6ab2b3ad7183f54e7e3eb0c692ac5ee5c3baac1a79be0aa469e
21f1fb6de710280a1bce8dff50415fc45102f62792cc48231231832ae783ecb8e0257d14bff01
9f3f43e5c7a26349414e2f580365373936b00fa0eced128d456c9d8babc82a051f4abbd6336b7
69800d00942f02b6935f3034b758faa9c9a1f96b57788d4613ef2778e26d95155bcd3e51bcf89
12590159aef4f83def06cb2d034f268a88629f9cf6689e1ac0f1022ef90b633502b46709ae242
495ebba9833433cc579f5b2691908bc2d8c3fd33007f67f358de6a77a2970d953d5374a2ebd6c
9dc2d4924dea2743f0cabfb976c2ab0ba69e9daa411ceec6d0e9c0d2a4e2f3e3b2f7556a25861
c56370e5106b135e32d9e4fa92c92fb8f7333a8d88391cf8e7d1d7d7dc5af0e699df59f30b63d
b49212f89930e7eea4d4a3e3ec551ec69e9aa4226984984f2c6b86653c76b8fc87191856dd730
a7dc6e3a7748365cd61ab20acb014f435c76eb35c311aedf3b1e5fd35697f1d214fca58d00675
a6713c896a2d6e6a6c2e9d8a94aa7fd3706e564b26ce430a22d5f271d2f90336eb1409554347d
b69ffdd9ffccf5480f005fc77b8f4fa0d4f7fb3590bc7bc2299e6e01dd81a903b9e7e3bd5a4db
25be0e51a99f832b35ecc57f84f0cafdfec517b357a74ebe76d5580e672cfbced992b0ee96e3a
451a462bca50bc2312d49b8a229900a8ab19f00ebb0c826dbcf2804a6a62f133b4005298361df
c5fdabad925a1bff475e2aebef4581695426b179a610ed6224a5f05b3317a1f50722ee43df832
0791fd6a3584255ddf811935d10d51696c9351d750fe359a96e8836b7183feddfdb14ac6ed085
77363b3d4d3cf36863af80e2315b142b57485d66bb3b6acb4c5ac28adc3621d8d7cc9e2f80b0d
a260b2754373b8367168dc4fb021799817808bc5989faf626477a231d70fb096c37abf209c0ec
f0978081e267d3f39a864d6682f461573f0515e89d49d16a241c4629b7d9df617f6ae270aec2f
28cdfd28714d21687f2290cb65c27e854c928e1ebb9a3a99debac419a366f4ef22d5cbedff9e0
f427121206c064646de616b02964a6dda48d6511aebcd596c2c514d8a71511ecc7136ecd10e52
f4f08de44954cff6b17deba92086c24c4e12d3e650b88750710da99f58fee2dd9cd388ed2c4e9
6148fb501204279d9599ab6548917a06decc4d3584c8859df377d81841bbb65c9e5042756c23f
6151fa4476e24881a03769c5e1cac1ace349ea47347d8a6bd7f42050609663ac21ebfb039117a
b2f9af1791400d18306ccec273da6e2602c1890c17ae10f8dc1ea48d7fce5e2e4ed9435916400
faf458e34126c8a9f02811ea9b75bbf9882a522b60cf6433e89d246193d0367d514e0b331d3ef
7fd8a0829230ea818375ad2f4303ffc63fdb52ddd27e5cb4a593651142ea079b85ee6efe2fc20
8d44bb27303171058707 41ed1c5a19dfeb58570fc645b470c8e0e6dc4f8de4edcbfd1fa9bdaf5
```

```
fbe53e390234cadfd8897103104a30bd600b1b12aa116be72a0f796e342d3c4c17f7583cd2e30
b797b991465ff07d8fc586f6b223b86b80261f32059e6fe717cb1e5e5ee9adf65305383ddd42d
106d4851b744ee95571be6daad62b4665e370ed40c350ce808afc12f17c2b1a99bc9145c23a13
84137ea7b9956b557fc5a2e0aa6ba1e9d6c828e3cc48c941d5b0e20f9a7bf6e31a37d90a9dfc4
60b17b56808fedbb32b2445e56c23c8df5512845777c5b60dcb6605e8c71765c36336cc16427e
dfce12a243d7ea29ed9e5a8118cb34b2cc6b88986c14e03ebe00eb6ba444c770d431bf3fbbf52
673ece9e04ea2b17e03f9e4588049668f47b3f78e67ab1a7762588ef2644b316e84e0eba92ed8
5fc38be62b762a4c0b977271b162b7fb26a02431fcf9b803e2d12a8f583419abbc9cbbd06690c
5c022131bd7d5c10e32fb859183c0346b9fdc8105c6253da14f3578cc256247ff1c5428db1314
6839f89fd67715e2f199fab433316f1aaa8c8a70fc551a334d23276321a5b933844c7b5fce690
51e3b49c460afa589a5fe192d216e57b353d562373c805afdb61e0a2ab6f5fa774a133ed5b445
7491bf94665df7b4ee00c17f414ebe2835c1bf98bc914675357749533f98680d1145534580c18
ce67d29281e481677003cafad693cc72c8649f6eb8174fdb2d87c706f0f184259b2dbe313e571
3901effd931baf208952ce3a5f2cdf74d761d29d7e2d67cc77696c287f713bb378e3cf0eea6c1
b68524618a4819538a7f61299a112a7af4a55d85a90583775f66588ecac0f422fd3d3beb3ddc9
62f028199f87b70325b8cd5c94902de28bee81f389cae594007347d0a4933edbdb85c65752a57
1ab7f3a0e2807dab188edb32595b3d860d300bd21a2c5251cb5a7ad062fa85cf37483b31a589f
c08c8682844d6f8e0844ccf3b04af1ba8aa476365ec157383f3aee1d1955ddc58ae8ced952258
bb71b4ccdab36b1f004472f01752ec848bce3e4f111a16c985d25bef3df160f7cdee4c25ca52b
0060d1263c206d77117d97e433d4bc6e0daf213824365b379fd5ad96145e6908169945c00afe4
79feb9c51b2de961698d664608b654a870611432c439dec891bc3b77d57c75ce2700eeb935073
17d3f490d465a752da3990262a7c18b0f83fd9464b5472fbcac70a730def35c3a78dd37f26214
a0bfdba3e312a2db098030c6019749f644d7a6c7c9edf8afdd9271a061818ec9b0e4836b80528
5ddc4fdf729f8918db46962a655022ab44b8e502c0231c468832686519f222c71d33a96bc90b5
78f43ceebbbd17fa89fc42df02eff7b1c750a7ab8295dc020fb8feb363fd9c7fc621cc7c201ed
aadc31b56bf0dc4a6bb9bb538f9011e6cc707d56cf07574136fb3e38b25dc4c6a6f92fca4c629
0e767b416f906f5f92fb3a04494cbffc02a191158f0bb1a6be6249247babe9244648ad17d8aca
cce4118a1efbc361c29bcbad89cdb9593b4249c14bdd4a1f6abc0b407c14aa9c638d12e482e42
263fd88e1885d89796554657a80c1a47f41a28b561f66b3e65edcfdefaf7c11aced7a6e76802a
e70ce17bff80301bca3c29b4068097e41fcd1946ac5ef116a1ba946fad66a4a0ae54977356d7b
193e9bc25fbe675cf28a0f244603fe8a2c639fd2d4bb87a1cec61cb9e861d0d56f616120f84e2
422d009e7fe63776d35386a384a39df8660ed1ef69d2792421750d6170152c739d14da817d3a5
3a757dcf986c7cdc08c5d50ef5b7685d16059a8b26b699837c6c407a6d2ce623c9d0427ff2cce
5697da98ba93a54ff9c8be9fb27ca440702f647773e7a2da2a81ec974b8bb1a0ea25d53294081
53c6cc21d076e01adc995e047ff8033dd5746cce6fe4025a801d3009ec1fb46796c980c184636
4ad05d846cde97f80d3d56b17a60b70d3d3dd3819b094d99ddabd41dc79d79b234dbf31d20b75
0c725dbc35e392a3a82d790aa79a1befbac7a5b3a40b928eb15046ecfa67953289b5ba032f51d
cfdb973e83099a44cf2b3d6e58910b5075fcebb6f199eb0ca121c057bdba54d363a80a17d10c5
e312362ef9da5b783a85021419ee65b9e235dc0ad84408590b42c728fb957efe4e29e32ac5846
d70ddd82ba0dd735b7ad6bb00ecc5357002b3386b2243b68dc8d0501ce57acfe5b8fb0b3f0e76
4a611333d03fe1c1b7873b464a85c8979e0e550c25f88726f8ecb13198ee4dd667e284dde21c4
917ff5f6b220ba77e449bf6077d07f01a6b302db4110f3cbb5bb286677905c1465dcf5a20e90b
fc9788b4d601dd7700e0581f304c29e278869954aac0064da192ced6e9bd5f76c33fd85fd90c1
2e70732ee61a0cf9325bb96a217a28a22921413512bf83faea5d9a355198c33a71e91c62713a7
94904fa7de19bf087cb0a2cea4e778a9e38c2db9d82a26a0d346a5e71ff77c15eaf8a234637d4
e25f80374268a010d03517ef51cde970ce96f535230878f220122477501839a385c4bc628797f
689b03e262171b1891b3115ae7dc7ee1db87887ffedb551a6270c863c20841d31b6a4d3d1e55a
9b597c92bd7ee647a6ec3af62b2aa6d87a44c1b8b728f5ca6035d045b1c494485accc098af6c2
78f1fc1c766a2dae65af2e4328cdd738757235871f44e270bd9e03273a60f29f2a999ce50c0ba
e04f475d40386f5e40a4379d1f391d526e5e7a885a002fc828165dd0039c01939d6fb03b2ab84
b7b9e5cfab064c7ce49c435bf9e11acab5e7c3e43916e785c2ace826952b1180d74f180e53c5d
586b3efd0eb7e04ee8e45fce7dffd604447078e1adce91745d3534dab2cf2546d0175c932c2f0
27cd41ac9167427cfeb674a771e3a94021154f777c46e2d562690efd18078c567a927822d76ce
caa7e727084e4f67e04332f0c5c8f5b6a18105ddcf7f1d9de7ed745a22ff9a2b34bde9fa82896
a68bab5110b2f79bf40269918809c5d05ec87657c4d2cc878fd702e2b5648b3d17c0b3d6f1445
5c0058a97aff9c17246fb1d70d236f872b69ce1a4ca911cb95013c8bb40d2329ec8fb44e13277
fe5f0a5e5b446635b271001dffc4e3f62b37c22b02f1b7f38e597c5018c5669fabce60abf2403
87198a1f60976ed38829a1c8a86031f0d42149ae0cbfd19fd0cbc44013dc46e5d525b44e809c8
```

```
8db4a4c7f683bec2790f77e8e0d470a8a0b720f8afd090e4e9b493594456d7a68a0aab01f967d
aac0b1bab6719d2fccb1c9c4d2a4dae04aab9698839e3e0506ce2af5210f94a7aab9f6331668d
08acd62c2c45ebad7faa479acbd19b3f60c79bdde8d308908d3921e2cd0c496f94e183d389b5b
d1e19212766747680 81a5bdfc050f1b1d2f3f546a7b7e9cbde6f05184a7cdd6d9ef2d6cecf1fb
197179afbccd13363d6c7997bec8dbdcdfeef4191e9f09107d9192e9ecf400000000000000000
b1920252b383b43",
  "raw_public_key":
"e45ffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b468cfc82bb929
f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f124d5e60bd68b8
c7e31fe01c7b0dc65ae470501cc565a6e1dfcfcfd12565433c4afedd511821e2e9610c45275e2
836dee35ced69d7efa672fd1e4318bef5eb6e897e8b451aa202ded042b2aaef77a7be3f699146
da229a8bdb3ffa496445967e75217bfbc9048f9956443d8731f833eb30de10dac96fffe7cf65e
a0445c3e31e8601e133be6a100764fe3196e267726441f31751fbf9a6f5880644f4e7275e57de
2b0f105e4db055d50dd1c9c934fddf535b8de28b0c74c0449f222cd2ed0bb8fbc775ccee8c940
665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee7581856ebd68f268459
56e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab932e69f778e2c
eefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a3655098
941993a1594860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8da
c1f861fd58e2afba5de5a52e020904f5b42bc0874e35befcf3e6119684768f36e008f04712177
cebe627607381e56eaaee161c1729b8de51dbde474d48cc68249ea27162b87993e60c84ed6cc6
423cb3676d9eb50b2cab5a3a049ef131381d623fa6fbcbc9db1e7cc025ea0418b9dad2cc6ccd4
e95fa2cec24feeca70318a751716b7213f63edbf65a63338357f838f94ec071822c2485124888
5107b3d1c4e924678c7614ea1af038104619f2ae372940becfa69e29cbb5ff6c3e20a47be4a4f
74bac34c133c00a6a706accc6ffd3d8e4fbd69a99704e1283c850d8c58d1e5753cd9587b83c4c
346cb9a58137213ec10834c66adfe2bb5c501a8ef2ecadd1b677a3df1a6deb86ebf0722c4f503
0e20f9018dd5b6fc53eea24fd92b7b5b4025feae996d3e48fd4c650d82dbad7eaf93663969851
2f26253d2ef6847c8518e8565cc9a5495c6fff57cde7323882c54a7db470ab2daf8ffd2bf794f
a7c692d9e7fbd532eecc1d7880e2ca0b3216128be28b4a9f1d151fac97808b0bd98b7b43a612a
9ac865812bfeac6f47460277840b52a3b087f916ca7cedc0f768ea2bd19ea21155f84b4a04c40
00ad2ae0587154d560bc0a477a4f9329a8984dd31eb1f2a05e3d918701d630cfca9af61ef088d
2c5581acb463e439902e5d425719e956b8d6df7305b28e0ff27d3ad0de2085d292499b19a3390
d4396fb3bac9a8d8cbead2a7a4290fc9ac6fca045f98a614a45a39cbe24360f84d14f8e472712
aceb74dbf45b53d49a0e4737e476ffc4d5b2f7cd247aa186d3b764ad9e9cfeee456a73c291d8d
e3912414ac43911c372173ad7b472af35c6853ced2fe7b5fe0a89565ab33baa6f65cdd928319d
7065e040e7a5e84f9aa903f7648094bad07136b16927b8ec6dbc2bef0cc2856de1e795923e141
2c49f24deeb6c21f6c8a9765c9c7986e0da4b4c67d8e0d0c8d466824fb923d8573148990cd2ef
133c78ceecab72ed9dd285c5a3766852d54534207ffd34027f6c76ede8fd1a32d72c30048bbaa
797d5df6fde27d087de5721ad7b7fa3e8d3f70d6bfc3ab2e252335368bbfa15acb5cb37d4694e
8b23cebe25de9c925a221a183b904d3f85df9929a919c54d6f87457373a0d6ecc1403e4cbbe62
0999435e80696634cd1a8e4747e9825bfa336e5bbad14f73640f1b9febe800dbaefe1630c61fa
e635b074c564eaa9db189c9e7302873fc64e6d497bc5c29080987a07a21d4af210703a4fa07f2
fd816f12fd1e29b4c0f44afe9bd4a1eaa8a7ae6f02a5b4258f52caf6127f62632a67cf4e8310b
e56a7c28c86b2e277600c3e92c8d23d42586244c571e90568df202f2f6d81f860a565f9eb91a3
c78372e2a8b1be61c5418cf49bf2d6c8955d4a482a9919b7660b3f9a4404ffc454ea073e1e4b2
689ab2cca4e46bd7004a6c491fa26ee7a57d60f35edb2b821e6266442c8f335d452d524c772e0
353724c23c7dd15b7aa155e91442022140c5fcb0153147edcf3e8952f6f0399a3c88066a72756
c9409915de63f64fa797841c57c796c6fc550ef745dfe9f179457f94755ae5a2506a764f327e5
50be3dc14dd41f3b04b147d454938c63a8d69b2ea4c5710ec0b36e3a6c72571fa5d59dde036c4
2033df35af056966ff0cd1204008971aa6ba9fb97b685ab9ffa2a9d1778104cd2c3b326de1fcb
c242e94d0311c3275b12850ed30ceead3a2ee6d060508411d4396f5421d8b6d067cf7cb5e8267
85fbe119e05e21bd879b64f57cb0cd1972c2815f20abe7ce6ab34d0f471af44baad179e906441
22f5f33288e689ddddc5ce833e9755df1e73c65c5a201c4ede2ffa6b19274927719d2d38fdb7a
65aa43708b7fa9a94aa7d3210253d78d3b181e1020d0000bd0a1dc05d447f9f58ebeb84c65b36
c8afcb83727a1508994e826957a663b0b9b8a003325ab6d6d6462ee4e106019c0dffe10323b7b
de7d82a38f85fd08786e860ba66c161b64b0708c363de5c6af62d8db3c243d1e1b712cb1d59e9
42b9b6b4295a5a500b182cbd5fd1bc6ce9376d91b47a2284f1fbe0ad1c048cc2cfbb4afa3a9eb
9697503b69feca990eba7e9441af9ca44cb3ac6b5ed66e591c201fe30efa8a7c471dc613d6254
c263a8e132104bec47f1aacb3b2fcd4051b69b5e3fcb1c147a65c2f90c4b5188bafc521cab03c
```

```
12a309da50b5a7517727ed41228ed123fe1b152f6a6319cd623bf34ad7b8e064ab993260bcbd4
05f5b7fff9b2fa40ba5ed5630242539e5d96823e89dc818a13d16675ee3079d976f694f5acc97
60ae789e9b3391b289e0e22a7ef17cc6a4577157b6d95c09baa4fd532e3ee0a290810ed35e56b
b19d9b61fb98a97c617425b06093d98a5cf0ee2dd127f0eea600b9a0c67fbe761db9b77e5d5bb
a9701da1b883e521a0cfe88451f57bd36085b67e56f061f84a2e6a152a71bce6e522daab6a0a3
3ce22e537fa9793d28b617e6c0a4176a83aa3be578afac0f2f5547c5516d218984755b7445c71
43afa4e551fce0071bdb873b34e6b9e2b9e79ed0c69d288ed6421f237e860a0c6492ebbdd2a44
c2c4f368dbe99941b1e8561d859d3859f496cee3d741f252973f8fcc539c409e35cc80a5ed6df
23cc3a65601313f5d681fd9540c5291a9e30a72e38c96413c47c61ff84fde78d011b01b4154d1
b920af003f7abb1e1999dea6a766cf9fd2702b3ce0ee57af931b62124b0861b163a3b91aa4bea
28076c3432df3b29b6c4e1ba588def420071fc157de90eb2722ecc9ab00df3c669383a61a91bb
67bd287ce349b4745ee7a479dbceef166b9acc412eb579fcd6437307edda253d606b7be7599c3
8092bc52a8598480edab8b82b1d21c565d2137ceae0b6642619b16133d91205d6355029e9cdfe
b9a28b373d95916b6b707d4c712c09cf36daf1a511b2bedb1aa70ee58d46a0666bb287784b0a3
840c589a7a04d5d6f2216be90aa4a512d5632f5c9bfe7b8b13382f999b95d367c7c46b968074c
e315197a5ff3545c7b77a804ade56a95b5c24cdece5937b5c0366d93ad03da9bc5db1b551dfb9
1e9b343d2b57b763439686d4a3"
}
```

Figure 5: ML_DSA_87

A.2. COSE

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "key":
"a5025820b8969ab4b37da9f0684e42647eb8a0be8b5b661ebf5d76f0583bf5b8d3a8059a0107
03382f20590520ba71f9f64e11baeb58fa9c6fbb6e14e61f18643dab495b47539a9166ca01981
31c44f826bbd56e34e55db5e5e2d733485e39ea260fc6000c5ea4ba80d3455cde53b46f34482a
edfd5450fc2e1ba4f25d15f9c144242fb39bb52287189030c50498e1717b7c758b190a6748ea9
aa3f7acaaf2c7cb526ed717c9f79aeb84214fa5cd8ded92a0c3fa1558810f12c7050a367708d1
96cd24e5af974904aed8e4ce8872e8696b0b7bca50e452cd7d30ea9a4adac0311d672c6bde849
6240b07431463708895cd9bafc31632d7397649388fdafcbf7d305a3de9a495eca7433a8f83ba
0f0b25c413c6e39c96eb7d691b34d37ce37f1eead1cf217e25ef34eecf3f7c60f84b8edfdde84
05d4f832576c61ef98e0a2f28da187700953924f686b94614705bcf53d33fedd4348edddbdf28
b5065e1f20775043e85cf931f829179363a1a7e7404a838ec00086b0976386fe637c98244757e
3f769ddd4467471bfad670f9a05f8246ee50a7b1eaf87fc4069c3ae2aa2033258117792f0bcd4
9e083fd1bc7496abff29cc94e4868b21214ed316525399a610fbdd4a80e7c80715f29578e2a84
bb40bdddbd9f47a11b6e7da118a1b658d359e8aef55eb46b5376b5b655979984a922beebfc59b
cd600d5309dccd72dbf0787db8ba757b537c1eafd5c0f50ea4bc9583549e2829a42c28cac248c
96d78124c47159b18aedd754aba17b19d430fb78f633ea9d26f54a9bd50f8d8f6b73594f82897
6e7ea09c53bbb9f11a56c9507fb89b9a5ebc037a37267a95f85b8d64ca97192b10a66f417b3f6
1fe9ca57130a48fd925eae2ab5502d571c8a51903c1d398f4c1f76a7e11743976afdbc697f230
94a3cd761ff9685de32e09fb3c28add453490300bc7c89dc01780096071722945775f264e1b06
23bcf4619c712c838761205d87691b75ef360196cbb9e9b92a0d4c4ed62326e5024d77510b8ee
2c7426cc22eae209dc9f13bde6bf08f5e7181bd3b459450b451a51539a715c21d67dd330eb597
0db00d9edbfb2822b036fa13bafeb86d8dc78866e3f8d43e53d78cca5595a6faf886b5dc112f1
cf4adcfa875800d90b48883af97316fe1506873fc157e570eacbfd222868d14234101966afb6b
f9940829253a953ada89fc756b6a849f70acb9838e69faa50bba75e3e89c2adb57e86d088ab9b
04a28e670709172243ec5e0008a5ceaf3f8722f487302596ffd755ad1b82a49c34b3469515b46
aa290cd86ee38ea7a9be3f103610335b531cca333ddfe32b14510f4b07ef95fc6684e8c454a92
c10dbb5d59c7a7c63fb305fe881967d99e669eb632840582560bb403431d40f75a49549084822
78292821f4ea91e42e78fa48caee3c836146dcfd738d117e92e9a15137d28e8e6a4b4622650cb
413504cb3a335d44beec5746c1c294b1e8cb99cb608d928f8ce3563632c521f23d13c61a8f61c
01df8c96c7360db4f3c68aa5d2fdd342a62ff3459c116389421ab43e8584c45882b50e6e4e96d
b6f0b8fde890d5dbfadcd88690b449e64240ddb2023747f308363e301aa77757169fc6150628d
5920b5aa1ab1c8cbf44cb00e025d7879d72b479e3af5311c785725590da9c89b9fc3b84507695
54eb44d203eba2bbaef9cad2237011c2ea44eff00f299a48ffe28ca93ddf85f76608242ef8d6c
c24610a1e2078fcac4f9385c314905ecaa82e553916d94d1a7c1ec652aa08897083daa2ebb177
5fbc471ae27777d7904ea9f1b92bcac3d8a3158426087b645b1108f0d65fec93789c053743ca1
4fd63d05e98b652df2b9c2ff9ce05f1940703ffb273f80e0e2732eca9960d981b4cfd3b7bb804
5b3c3830546b9dd8db0d215820000000000000000000000000000000000000000000000000000
0000000000000",
  "key_diag": "{2:
h'b8969ab4b37da9f0684e42647eb8a0be8b5b661ebf5d76f0583bf5b8d3a8059a', 1: 7,
3: -48, -1:
h'ba71f9f64e11baeb58fa9c6fbb6e14e61f18643dab495b47539a9166ca0198131c44f826bbd
56e34e55db5e5e2d733485e39ea260fc6000c5ea4ba80d3455cde53b46f34482aedfd5450fc2e
1ba4f25d15f9c144242fb39bb52287189030c50498e1717b7c758b190a6748ea9aa3f7acaaf2c
7cb526ed717c9f79aeb84214fa5cd8ded92a0c3fa1558810f12c7050a367708d196cd24e5af97
4904aed8e4ce8872e8696b0b7bca50e452cd7d30ea9a4adac0311d672c6bde8496240b0743146
3708895cd9bafc31632d7397649388fdafcbf7d305a3de9a495eca7433a8f83ba0f0b25c413c6
e39c96eb7d691b34d37ce37f1eead1cf217e25ef34eecf3f7c60f84b8edfde8405d4f832576c
61ef98e0a2f28da187700953924f686b94614705bcf53d33fedd4348edddbdf28b5065e1f2077
5043e85cf931f829179363a1a7e7404a838ec00086b0976386fe637c98244757e3f769ddd4467
471bfad670f9a05f8246ee50a7b1eaf87fc4069c3ae2aa2033258117792f0bcd49e083fd1bc74
96abff29cc94e4868b21214ed316525399a610fbdd4a80e7c80715f29578e2a84bb40bdddbd9f
47a11b6e7da118a1b658d359e8aef55eb46b5376b5b655979984a922beebfc59bcd600d5309dc
cd72dbf0787db8ba757b537c1eafd5c0f50ea4bc9583549e2829a42c28cac248c96d78124c471
```

```
59b18aedd754aba17b19d430fb78f633ea9d26f54a9bd50f8d8f6b73594f828976e7ea09c53bb
b9f11a56c9507fb89b9a5ebc037a37267a95f85b8d64ca97192b10a66f417b3f61fe9ca57130a
48fd925eae2ab5502d571c8a51903c1d398f4c1f76a7e11743976afdbc697f23094a3cd761ff9
685de32e09fb3c28add453490300bc7c89dc01780096071722945775f264e1b0623bcf4619c71
2c838761205d87691b75ef360196cbb9e9b92a0d4c4ed62326e5024d77510b8ee2c7426cc22ea
e209dc9f13bde6bf08f5e7181bd3b459450b451a51539a715c21d67dd330eb5970db00d9edbfb
2822b036fa13bafeb86d8dc78866e3f8d43e53d78cca5595a6faf886b5dc112f1cf4adcfa8758
00d90b48883af97316fe1506873fc157e570eacbfd222868d14234101966afb6bf9940829253a
953ada89fc756b6a849f70acb9838e69faa50bba75e3e89c2adb57e86d088ab9b04a28e670709
172243ec5e0008a5ceaf3f8722f487302596ffd755ad1b82a49c34b3469515b46aa290cd86ee3
8ea7a9be3f103610335b531cca333ddfe32b14510f4b07ef95fc6684e8c454a92c10dbb5d59c7
a7c63fb305fe881967d99e669eb632840582560bb403431d40f75a4954908482278292821f4ea
91e42e78fa48caee3c836146dcfd738d117e92e9a15137d28e8e6a4b4622650cb413504cb3a33
5d44beec5746c1c294b1e8cb99cb608d928f8ce3563632c521f23d13c61a8f61c01df8c96c736
0db4f3c68aa5d2fdd342a62ff3459c116389421ab43e8584c45882b50e6e4e96db6f0b8fde890
d5dbfadcd88690b449e64240ddb2023747f308363e301aa77757169fc6150628d5920b5aa1ab1
c8cbf44cb00e025d7879d72b479e3af5311c785725590da9c89b9fc3b8450769554eb44d203eb
a2bbaef9cad2237011c2ea44eff00f299a48ffe28ca93ddf85f76608242ef8d6cc24610a1e207
8fcac4f9385c314905ecaa82e553916d94d1a7c1ec652aa08897083daa2ebb1775fbc471ae277
77d7904ea9f1b92bcac3d8a3158426087b645b1108f0d65fec93789c053743ca14fd63d05e98b
652df2b9c2ff9ce05f1940703ffb273f80e0e2732eca9960d981b4cfd3b7bb8045b3c3830546b
9dd8db0d', -2:
h'00000000000000000000000000000000000000000000000000000000000000000000000000'}",
  "sign1":
"d2845827a201382f045820b8969ab4b37da9f0684e42647eb8a0be8b5b661ebf5d76f0583bf5
b8d3a8059aa0581d68656c6c6f20706f7374207175616e74756d207369676e617475726573590
9742657237b7520fd4cb8803f69a6e4ab613f4816420cd38e6474e548a370c6f0a18851ce8b7b
b1b43c658b795303d0f22d23aad9afc7077877ab77d7cc92947bcf800e09626d7ceb809f74d2d
c435200b272ecc92a993901087a42eaeaa6b9009df00f26055e6032ccca2995bf9c455e93c95a
db9dda970ba07d778a9b4950169b289a86ec272bb810f9506b960941fa4ac804de49cb80f9bd5
4f51adef76670c06f94bf948ad7675ab28aa3254944753aac0cdbd8594752a438552e846fb476
be3e31df0c91222db5e5d70bddb05b624a78103654d4e9ec514f6be91cfe8fa3b8529b2659a89
e70227f35d0059362ed51c7523bf4a8ca7ceb0da6216bea77576548cd98f5ad6f87326facc8b3
08debce4461f1f2c4b190bd4950eec52cb66da70c9913e8a476826a0ea05edd8f2d3ca53e485f
fcebc4e7ae33aeeb1d8dc3ee6b8d09cea138377ceeaed4fef57d868c16311e18c64b9df501791
a6142085083850b3ad2e74901298c09b7fc4d87a660031e955b39cf9e6fbbe3cae5b36360f6b6
1f904771d55d542fbc68be5468738f5b8c44eb624da535a112c0266f79b9ae7ac996feab2c587
4c65f59a72bf671b568d06e57b89f6fa168f48050f869e9fe0b95490487597e1746d7f54ef04e
ca32710bd4655a2269fd9afdfa0c7630c09ad59273d5d76f6bc026b623e5fee4fe3978efb4fdc
5f905d8a346259cad9cd8ad826cdea818fcca6804bd78ddddb70d46d723ec63980fe7bb2eb8da
b84692cb6f6a560eb80381dc0d5ded38d1de896772702f99637f6b9a9b207be86e2a401187bb2
50f68230f7840ecf9787bb6073e2e29f1287cd73bdf1dae8302fcf23f942305c4c9807aba037a
f66f8b278003c98a30084f9ad3f2e4c4b31eb1b3f20170c70f0310f71932a4e0065a2bd79eedc
70e59f9cc261aed96fd7ebec86be2490789ad0dffc76f4cccc28ed675a769edf9f8d6e9fd78d5
9393687fb19b641626f70bbed7c6496a3a1393be6751f533e7af8f20f9ef32c7b58b231feb423
1aa407ecf5e0be7921c449a537ab58871b4cef2f8b1212b189ddc9e207b0ebe8135be534b30f2
5ce0aa33371a94971da4b6b78bb2cb708035b539f3706348d1f6ef0e2ab9c741f1ffce5bd34c2
0c2ded6272c583188d2f48404cbd10f6aa759fecb1e5b87c755573db0d86ef17fecd7231179f4
7a19b0bcdafadad9a8b20dfe1d2792cc2d78d13c76722739d6c31563bc938fb07a0bc5d96d3a4
e852141815b526ac74fa210c48ce1e2ffa3faa682191aea55a476a6cd7e0ab42902180b1444a2
e08302c17608b5831daa4c4008dbb54f0b4ce566c069ed48d4a9c5b542816f3156cde0d7323bb
071cccc98ee35672248e873b5907d02a153a57e5777c6767fd75e833df46813c2abe44dc6492e
8de4487f4fa1d1377d4ae273d28869c6630ba4865e65676d9dc9ca0998a0082e95c78314d5430
68f6fd38a27bdbc98f8b5fefa21e704e4bc8ac7ed46ea5c03eb700cf0e549b8a1c50b5d051bd7
c2588938f7c9f5499e7b95430b1e567a2e36b4a55252829d7fb319c7edab4e19108fa2a784c96
ec1027f19f571448132b6c8c4441a7a7488ddda530b84ba0221120c95311eab37660b1329a703
65117eebbb7e0240cc5052ec723e0121c2a175053c762b88943ac7b965d10239c4b8f8d39a1a5
7ace097a1631c7e93c36abc8a085a21a18a14b621cff49369707891e06e508e41970b26490c8f
```

```
5c038bcb2e62a72d24591f563c42fed3dfa3539f75dacbc7918919642220a01da483a2c041336
0e424c6cc30dfc502858a57ffdc20d30bb57c1659a7d4beb6794c4675524e813a27e3807547d0
bc16e91242d7925b01f0a8cf03f5c6e867710373ad02e53816f82a21b2c9f359e7d586ec0590c
0a1780a6755e1723981ebd866d251e20a0a5b2dc08e05beb325797aa7c2746596c534964cc751
ff341d49e39c8b6f8a903549779189c5732b841abde352eddff9ffb67f20b9c27d30078994ac9
6c8250b3428c65a714c05c91c897a18ee58f908557062bd733444a9d73ed89a637c62143e46e1
cb3723c6a8fd2df0d90d03b6cdfb4e6c033f67c51a803b6eaea79e0ecfe4a3b22c5dc951d5168
3ea716149958c59ab43f1085d8e5896aa3c8d972d54998d3de2b27c2d67e0059b78dff6f804cd
491dfae0308b4c8983ea1c574b4414df8ca772fbb60dc49249f8dbab9c43357016893f7a4b2eb
28c0a8de635157b717e20ad60d5a52d37e2ebf5b87dcdcccddd1f40825d56b948e60015118e89
88f6000dd157ce92a0f0ec1d5459890317ee861a0d29f7305331047886e1918b8438d1df534e6
85c93f2f11317b000b0bd7da766e5f1d4a0816a7af878be4c8dc8fdd208abd5c7f98aa0e88277
2387ef5032f60e71a7c1c630a8eacdde2a7c5e86277b20e1317cd8b9892e8509647d55143dccc
a07ffdd678d5856eaab93f55df72ff4c909146de54393aeed095cbd9fc1a24b7f7950cb80eb42
3ed114cdc21e59593b2a5fcbbdf1613810fd63c8dd45e39bc5bd02d71328cfea87d2deadda750
89ca7d4529e0b5b64fb887fc38cb9531033386255c6a155af95447b2154354e6d163b752bef91
f248b5068f3e620365c8c497cfcbe61930d0cf08387308310f485bfa23c31bf2d01900e801352
a388c97212ef58b6a81f5082f08831433a7ca8c0df910cc462b36d61f532325eeee540547b6c0
7c738b010daf7384f8cf01975761101e556e8639848dfd049ee5360bb9b62bb38aef0fc84970d
ad3e78c0f3413573042abe52805b5aec545bcb43142f5d44a9c1d2b6cdf3ded20907f02ebc78e
78f598beadd0fc1faa676560edffbd7a83b61795bc29b6fbe4c7c6e9097139dbb85b54a8b446a
37f2fd6a7db528f1c5da5fe367823f8fa39adae0bd23196f689059e2de3cfcbaad6bec7104641
56cd72be70d5950075953286feb605f6898746586750e3aef767b0e80136453c1ab388ff5462b
fc0316ed78937ea235dd883e9fedbd66f9060b542272ac9747fe3109a27a89403fc1c2380ccb1
e3f199077582aa565fba4621092c5665f2f7803f5ecfdaf86878ec045a780ea3751bd32333cd0
2fef8b4eb9386f51fa7a5f3bb81c55fb0de38c905ba4002dadfcc5123bf561bef2d32c40577dc
487736162c69444279d917abd0d2320fb715299c1043defb582a20fec3190a6c0e48436091038
8889c122c4a13adc73031a0969e3c1a9008d8467c4c4d59c848d9ca2441ec57b02034fd5872b4
cf75185d5fb14e6af1aead0e1727db42db39877f01d674558f7b59b0e0f10363e3f505d82a7c0
c7cadd1618233541424f57596476777d80a6b8dfe6eefcfd0515196c8e99c3cfd2ebf2020b0c1
6202b3337484e525657a4b5bec3cad2d4d5d6dd00000000000000000000000e232e45",
  "sign1_diag":
"18([h'a201382f045820b8969ab4b37da9f0684e42647eb8a0be8b5b661ebf5d76f0583bf5b8
d3a8059a', {},
h'68656c6c6f20706f7374207175616e74756d207369676e617475726573',
h'2657237b7520fd4cb8803f69a6e4ab613f4816420cd38e6474e548a370c6f0a18851ce8b7bb
1b43c658b795303d0f22d23aad9afc7077877ab77d7cc92947bcf800e09626d7ceb809f74d2dc
435200b272ecc92a993901087a42eaeaa6b9009df00f26055e6032ccca2995bf9c455e93c95ad
b9dda970ba07d778a9b4950169b289a86ec272bb810f9506b960941fa4ac804de49cb80f9bd54
f51adef76670c06f94bf948ad7675ab28aa3254944753aac0cdbd8594752a438552e846fb476b
e3e31df0c91222db5e5d70bddb05b624a78103654d4e9ec514f6be91cfe8fa3b8529b2659a89e
70227f35d0059362ed51c7523bf4a8ca7ceb0da6216bea77576548cd98f5ad6f87326facc8b30
8debce4461f1f2c4b190bd4950eec52cb66da70c9913e8a476826a0ea05edd8f2d3ca53e485ff
cebc4e7ae33aeeb1d8dc3ee6b8d09cea138377ceeaed4fef57d868c16311e18c64b9df501791a
6142085083850b3ad2e74901298c09b7fc4d87a660031e955b39cf9e6fbbe3cae5b36360f6b61
f904771d55d542fbc68be5468738f5b8c44eb624da535a112c0266f79b9ae7ac996feab2c5874
c65f59a72bf671b568d06e57b89f6fa168f48050f869e9fe0b95490487597e1746d7f54ef04ec
a32710bd4655a2269fd9afdfa0c7630c09ad59273d5d76f6bc026b623e5fee4fe3978efb4fdc5
f905d8a346259cad9cd8ad826cdea818fcca6804bd78ddddb70d46d723ec63980fe7bb2eb8dab
84692cb6f6a560eb80381dc0d5ded38d1de896772702f99637f6b9a9b207be86e2a401187bb25
0f68230f7840ecf9787bb6073e2e29f1287cd73bdf1dae8302fcf23f942305c4c9807aba037af
66f8b278003c98a30084f9ad3f2e4c4b31eb1b3f20170c70f0310f71932a4e0065a2bd79eedc7
0e59f9cc261aed96fd7ebec86be2490789ad0dffc76f4cccc28ed675a769edf9f8d6e9fd78d59
393687fb19b641626f70bbed7c6496a3a1393be6751f533e7af8f20f9ef32c7b58b231feb4231
aa407ecf5e0be7921c449a537ab58871b4cef2f8b1212b189ddc9e207b0ebe8135be534b30f25
ce0aa33371a94971da4b6b78bb2cb708035b539f3706348d1f6ef0e2ab9c741f1ffce5bd34c20
c2ded6272c583188d2f48404cbd10f6aa759fecb1e5b87c755573db0d86ef17fecd7231179f47
a19b0bcdafadad9a8b20dfe1d2792cc2d78d13c76722739d6c31563bc938fb07a0bc5d96d3a4e
```

```
852141815b526ac74fa210c48ce1e2ffa3faa682191aea55a476a6cd7e0ab42902180b1444a2e
08302c17608b5831daa4c4008dbb54f0b4ce566c069ed48d4a9c5b542816f3156cde0d7323bb0
71cccc98ee35672248e873b5907d02a153a57e5777c6767fd75e833df46813c2abe44dc6492e8
de4487f4fa1d1377d4ae273d28869c6630ba4865e65676d9dc9ca0998a0082e95c78314d54306
8f6fd38a27bdbc98f8b5fefa21e704e4bc8ac7ed46ea5c03eb700cf0e549b8a1c50b5d051bd7c
2588938f7c9f5499e7b95430b1e567a2e36b4a55252829d7fb319c7edab4e19108fa2a784c96e
c1027f19f571448132b6c8c4441a7a7488ddda530b84ba0221120c95311eab37660b1329a7036
5117eebbb7e0240cc5052ec723e0121c2a175053c762b88943ac7b965d10239c4b8f8d39a1a57
ace097a1631c7e93c36abc8a085a21a18a14b621cff49369707891e06e508e41970b26490c8f5
c038bcb2e62a72d24591f563c42fed3dfa3539f75dacbc7918919642220a01da483a2c0413360
e424c6cc30dfc502858a57ffdc20d30bb57c1659a7d4beb6794c4675524e813a27e3807547d0b
c16e91242d7925b01f0a8cf03f5c6e867710373ad02e53816f82a21b2c9f359e7d586ec0590c0
a1780a6755e1723981ebd866d251e20a0a5b2dc08e05beb325797aa7c2746596c534964cc751f
f341d49e39c8b6f8a903549779189c5732b841abde352eddff9ffb67f20b9c27d30078994ac96
c8250b3428c65a714c05c91c897a18ee58f908557062bd733444a9d73ed89a637c62143e46e1c
b3723c6a8fd2df0d90d03b6cdfb4e6c033f67c51a803b6eaea79e0ecfe4a3b22c5dc951d51683
ea716149958c59ab43f1085d8e5896aa3c8d972d54998d3de2b27c2d67e0059b78dff6f804cd4
91dfae0308b4c8983ea1c574b4414df8ca772fbb60dc49249f8dbab9c43357016893f7a4b2eb2
8c0a8de635157b717e20ad60d5a52d37e2ebf5b87dcdcccddd1f40825d56b948e60015118e898
8f6000dd157ce92a0f0ec1d5459890317ee861a0d29f7305331047886e1918b8438d1df534e68
5c93f2f11317b000b0bd7da766e5f1d4a0816a7af878be4c8dc8fdd208abd5c7f98aa0e882772
387ef5032f60e71a7c1c630a8eacdde2a7c5e86277b20e1317cd8b9892e8509647d55143dccca
07ffdd678d5856eaab93f55df72ff4c909146de54393aeed095cbd9fc1a24b7f7950cb80eb423
ed114cdc21e59593b2a5fcbbdf1613810fd63c8dd45e39bc5bd02d71328cfea87d2deadda7508
9ca7d4529e0b5b64fb887fc38cb9531033386255c6a155af95447b2154354e6d163b752bef91f
248b5068f3e620365c8c497cfcbe61930d0cf08387308310f485bfa23c31bf2d01900e801352a
388c97212ef58b6a81f5082f08831433a7ca8c0df910cc462b36d61f532325eeee540547b6c07
c738b010daf7384f8cf01975761101e556e8639848dfd049ee5360bb9b62bb38aef0fc84970da
d3e78c0f3413573042abe52805b5aec545bcb43142f5d44a9c1d2b6cdf3ded20907f02ebc78e7
8f598beadd0fc1faa676560edffbd7a83b61795bc29b6fbe4c7c6e9097139dbb85b54a8b446a3
7f2fd6a7db528f1c5da5fe367823f8fa39adae0bd23196f689059e2de3cfcbaad6bec71046415
6cd72be70d5950075953286feb605f6898746586750e3aef767b0e80136453c1ab388ff5462bf
c0316ed78937ea235dd883e9fedbd66f9060b542272ac9747fe3109a27a89403fc1c2380ccb1e
3f199077582aa565fba4621092c5665f2f7803f5ecfdaf86878ec045a780ea3751bd32333cd02
fef8b4eb9386f51fa7a5f3bb81c55fb0de38c905ba4002dadfcc5123bf561bef2d32c40577dc4
87736162c69444279d917abd0d2320fb715299c1043defb582a20fec3190a6c0e484360910388
889c122c4a13adc73031a0969e3c1a9008d8467c4c4d59c848d9ca2441ec57b02034fd5872b4c
f75185d5fb14e6af1aead0e1727db42db39877f01d674558f7b59b0e0f10363e3f505d82a7c0c
7cadd1618233541424f57596476777d80a6b8dfe6eefcfd0515196c8e99c3cfd2ebf2020b0c16
202b3337484e525657a4b5bec3cad2d4d5d6dd00000000000000000000000e232e45'])",
  "raw_to_be_signed":
"846a5369676e6174757265315827a201382f045820b8969ab4b37da9f0684e42647eb8a0be8b
5b661ebf5d76f0583bf5b8d3a8059a40581d68656c6c6f20706f7374207175616e74756d20736
9676e617475726573",
  "raw_signature":
"2657237b7520fd4cb8803f69a6e4ab613f4816420cd38e6474e548a370c6f0a18851ce8b7bb1
b43c658b795303d0f22d23aad9afc7077877ab77d7cc92947bcf800e09626d7ceb809f74d2dc4
35200b272ecc92a993901087a42eaeaa6b9009df00f26055e6032ccca2995bf9c455e93c95adb
9dda970ba07d778a9b4950169b289a86ec272bb810f9506b960941fa4ac804de49cb80f9bd54f
51adef76670c06f94bf948ad7675ab28aa3254944753aac0cdbd8594752a438552e846fb476be
3e31df0c91222db5e5d70bddb05b624a78103654d4e9ec514f6be91cfe8fa3b8529b2659a89e7
0227f35d0059362ed51c7523bf4a8ca7ceb0da6216bea77576548cd98f5ad6f87326facc8b308
debce4461f1f2c4b190bd4950eec52cb66da70c9913e8a476826a0ea05edd8f2d3ca53e485ffc
ebc4e7ae33aeeb1d8dc3ee6b8d09cea138377ceeaed4fef57d868c16311e18c64b9df501791a6
142085083850b3ad2e74901298c09b7fc4d87a660031e955b39cf9e6fbbe3cae5b36360f6b61f
904771d55d542fbc68be5468738f5b8c44eb624da535a112c0266f79b9ae7ac996feab2c5874c
65f59a72bf671b568d06e57b89f6fa168f48050f869e9fe0b95490487597e1746d7f54ef04eca
32710bd4655a2269fd9afdfa0c7630c09ad59273d5d76f6bc026b623e5fee4fe3978efb4fdc5f
```

```
905d8a346259cad9cd8ad826cdea818fcca6804bd78ddddb70d46d723ec63980fe7bb2eb8dab8
4692cb6f6a560eb80381dc0d5ded38d1de896772702f99637f6b9a9b207be86e2a401187bb250
f68230f7840ecf9787bb6073e2e29f1287cd73bdf1dae8302fcf23f942305c4c9807aba037af6
6f8b278003c98a30084f9ad3f2e4c4b31eb1b3f20170c70f0310f71932a4e0065a2bd79eedc70
e59f9cc261aed96fd7ebec86be2490789ad0dffc76f4cccc28ed675a769edf9f8d6e9fd78d593
93687fb19b641626f70bbed7c6496a3a1393be6751f533e7af8f20f9ef32c7b58b231feb4231a
a407ecf5e0be7921c449a537ab58871b4cef2f8b1212b189ddc9e207b0ebe8135be534b30f25c
e0aa33371a94971da4b6b78bb2cb708035b539f3706348d1f6ef0e2ab9c741f1ffce5bd34c20c
2ded6272c583188d2f48404cbd10f6aa759fecb1e5b87c755573db0d86ef17fecd7231179f47a
19b0bcdafadad9a8b20dfe1d2792cc2d78d13c76722739d6c31563bc938fb07a0bc5d96d3a4e8
52141815b526ac74fa210c48ce1e2ffa3faa682191aea55a476a6cd7e0ab42902180b1444a2e0
8302c17608b5831daa4c4008dbb54f0b4ce566c069ed48d4a9c5b542816f3156cde0d7323bb07
1cccc98ee35672248e873b5907d02a153a57e5777c6767fd75e833df46813c2abe44dc6492e8d
e4487f4fa1d1377d4ae273d28869c6630ba4865e65676d9dc9ca0998a0082e95c78314d543068
f6fd38a27bdbc98f8b5fefa21e704e4bc8ac7ed46ea5c03eb700cf0e549b8a1c50b5d051bd7c2
588938f7c9f5499e7b95430b1e567a2e36b4a55252829d7fb319c7edab4e19108fa2a784c96ec
1027f19f571448132b6c8c4441a7a7488ddda530b84ba0221120c95311eab37660b1329a70365
117eebbb7e0240cc5052ec723e0121c2a175053c762b88943ac7b965d10239c4b8f8d39a1a57a
ce097a1631c7e93c36abc8a085a21a18a14b621cff49369707891e06e508e41970b26490c8f5c
038bcb2e62a72d24591f563c42fed3dfa3539f75dacbc7918919642220a01da483a2c0413360e
424c6cc30dfc502858a57ffdc20d30bb57c1659a7d4beb6794c4675524e813a27e3807547d0bc
16e91242d7925b01f0a8cf03f5c6e867710373ad02e53816f82a21b2c9f359e7d586ec0590c0a
1780a6755e1723981ebd866d251e20a0a5b2dc08e05beb325797aa7c2746596c534964cc751ff
341d49e39c8b6f8a903549779189c5732b841abde352eddff9ffb67f20b9c27d30078994ac96c
8250b3428c65a714c05c91c897a18ee58f908557062bd733444a9d73ed89a637c62143e46e1cb
3723c6a8fd2df0d90d03b6cdfb4e6c033f67c51a803b6eaea79e0ecfe4a3b22c5dc951d51683e
a716149958c59ab43f1085d8e5896aa3c8d972d54998d3de2b27c2d67e0059b78dff6f804cd49
1dfae0308b4c8983ea1c574b4414df8ca772fbb60dc49249f8dbab9c43357016893f7a4b2eb28
c0a8de635157b717e20ad60d5a52d37e2ebf5b87dcdcccddd1f40825d56b948e60015118e8988
f6000dd157ce92a0f0ec1d5459890317ee861a0d29f7305331047886e1918b8438d1df534e685
c93f2f11317b000b0bd7da766e5f1d4a0816a7af878be4c8dc8fdd208abd5c7f98aa0e8827723
87ef5032f60e71a7c1c630a8eacdde2a7c5e86277b20e1317cd8b9892e8509647d55143dccca0
7ffdd678d5856eaab93f55df72ff4c909146de54393aeed095cbd9fc1a24b7f7950cb80eb423e
d114cdc21e59593b2a5fcbbdf1613810fd63c8dd45e39bc5bd02d71328cfea87d2deadda75089
ca7d4529e0b5b64fb887fc38cb9531033386255c6a155af95447b2154354e6d163b752bef91f2
48b5068f3e620365c8c497cfcbe61930d0cf08387308310f485bfa23c31bf2d01900e801352a3
88c97212ef58b6a81f5082f08831433a7ca8c0df910cc462b36d61f532325eeee540547b6c07c
738b010daf7384f8cf01975761101e556e8639848dfd049ee5360bb9b62bb38aef0fc84970dad
3e78c0f3413573042abe52805b5aec545bcb43142f5d44a9c1d2b6cdf3ded20907f02ebc78e78
f598beadd0fc1faa676560edffbd7a83b61795bc29b6fbe4c7c6e9097139dbb85b54a8b446a37
f2fd6a7db528f1c5da5fe367823f8fa39adae0bd23196f689059e2de3cfcbaad6bec710464156
cd72be70d5950075953286feb605f6898746586750e3aef767b0e80136453c1ab388ff5462bfc
0316ed78937ea235dd883e9fedbd66f9060b542272ac9747fe3109a27a89403fc1c2380ccb1e3
f199077582aa565fba4621092c5665f2f7803f5ecfdaf86878ec045a780ea3751bd32333cd02f
ef8b4eb9386f51fa7a5f3bb81c55fb0de38c905ba4002dadfcc5123bf561bef2d32c40577dc48
7736162c69444279d917abd0d2320fb715299c1043defb582a20fec3190a6c0e4843609103888
89c122c4a13adc73031a0969e3c1a9008d8467c4c4d59c848d9ca2441ec57b02034fd5872b4cf
75185d5fb14e6af1aead0e1727db42db39877f01d674558f7b59b0e0f10363e3f505d82a7c0c7
cadd1618233541424f57596476777d80a6b8dfe6eefcfd0515196c8e99c3cfd2ebf2020b0c162
02b3337484e525657a4b5bec3cad2d4d5d6dd00000000000000000000000e232e45",
  "raw_public_key":
"ba71f9f64e11baeb58fa9c6fbb6e14e61f18643dab495b47539a9166ca0198131c44f826bbd5
6e34e55db5e5e2d733485e39ea260fc6000c5ea4ba80d3455cde53b46f34482aedfd5450fc2e1
ba4f25d15f9c144242fb39bb52287189030c50498e1717b7c758b190a6748ea9aa3f7acaaf2c7
cb526ed717c9f79aeb84214fa5cd8ded92a0c3fa1558810f12c7050a367708d196cd24e5af974
904aed8e4ce8872e8696b0b7bca50e452cd7d30ea9a4adac0311d672c6bde8496240b07431463
708895cd9bafc31632d7397649388fdafcbf7d305a3de9a495eca7433a8f83ba0f0b25c413c6e
39c96eb7d691b34d37ce37f1eead1cf217e25ef34eecf3f7c60f84b8edfdde8405d4f832576c6
```

```
1ef98e0a2f28da187700953924f686b94614705bcf53d33fedd4348edddbdf28b5065e1f20775
043e85cf931f829179363a1a7e7404a838ec00086b0976386fe637c98244757e3f769ddd44674
71bfad670f9a05f8246ee50a7b1eaf87fc4069c3ae2aa2033258117792f0bcd49e083fd1bc749
6abff29cc94e4868b21214ed316525399a610fbdd4a80e7c80715f29578e2a84bb40bdddbd9f4
7a11b6e7da118a1b658d359e8aef55eb46b5376b5b655979984a922beebfc59bcd600d5309dcc
d72dbf0787db8ba757b537c1eafd5c0f50ea4bc9583549e2829a42c28cac248c96d78124c4715
9b18aedd754aba17b19d430fb78f633ea9d26f54a9bd50f8d8f6b73594f828976e7ea09c53bbb
9f11a56c9507fb89b9a5ebc037a37267a95f85b8d64ca97192b10a66f417b3f61fe9ca57130a4
8fd925eae2ab5502d571c8a51903c1d398f4c1f76a7e11743976afdbc697f23094a3cd761ff96
85de32e09fb3c28add453490300bc7c89dc01780096071722945775f264e1b0623bcf4619c712
c838761205d87691b75ef360196cbb9e9b92a0d4c4ed62326e5024d77510b8ee2c7426cc22eae
209dc9f13bde6bf08f5e7181bd3b459450b451a51539a715c21d67dd330eb5970db00d9edbfb2
822b036fa13bafeb86d8dc78866e3f8d43e53d78cca5595a6faf886b5dc112f1cf4adcfa87580
0d90b48883af97316fe1506873fc157e570eacbfd222868d14234101966afb6bf9940829253a9
53ada89fc756b6a849f70acb9838e69faa50bba75e3e89c2adb57e86d088ab9b04a28e6707091
72243ec5e0008a5ceaf3f8722f487302596ffd755ad1b82a49c34b3469515b46aa290cd86ee38
ea7a9be3f103610335b531cca333ddfe32b14510f4b07ef95fc6684e8c454a92c10dbb5d59c7a
7c63fb305fe881967d99e669eb632840582560bb403431d40f75a4954908482278292821f4ea9
1e42e78fa48caee3c836146dcfd738d117e92e9a15137d28e8e6a4b4622650cb413504cb3a335
d44beec5746c1c294b1e8cb99cb608d928f8ce3563632c521f23d13c61a8f61c01df8c96c7360
db4f3c68aa5d2fdd342a62ff3459c116389421ab43e8584c45882b50e6e4e96db6f0b8fde890d
5dbfadcd88690b449e64240ddb2023747f308363e301aa77757169fc6150628d5920b5aa1ab1c
8cbf44cb00e025d7879d72b479e3af5311c785725590da9c89b9fc3b8450769554eb44d203eba
2bbaef9cad2237011c2ea44eff00f299a48ffe28ca93ddf85f76608242ef8d6cc24610a1e2078
fcac4f9385c314905ecaa82e553916d94d1a7c1ec652aa08897083daa2ebb1775fbc471ae2777
7d7904ea9f1b92bcac3d8a3158426087b645b1108f0d65fec93789c053743ca14fd63d05e98b6
52df2b9c2ff9ce05f1940703ffb273f80e0e2732eca9960d981b4cfd3b7bb8045b3c3830546b9
dd8db0d"
}
```

Figure 6: ML_DSA_44

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "key":
"a5025820b788acf242f1f1d6532926d816e76e1636874267f2a48c84c4e65789ab80cc020107
033830205907a0424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443
f0942ab8bdbad7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed8
0cd5fb2cbd3667e60d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd
4642a55ade693868a460cbec03f4fc99a4e30bccffa8a475e5395396674ebb81a94937587880f
6dbd27bf1c4f5a9ee43cdd8b0e53b3b7fb49c73adfbc2d4f8c54303520c29bf97e26ee57db342
d957c893936522d0942b41d82ee3772a00570adfb545c1143922b0496f826a0a970064b36ddf5
34b5f8e1c1cd0b5565ea846b45431f0618143ece89777bb3f61179ad20295fe0a6e062ae6eecb
c2ef38f2ac1a22dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb
8a999ad7a83e5e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727
f0b84c44b9b0a8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c
7045c22d33a083f6ae07a114746d1bfdccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2
de6a4aa3d99ddd88f48aaa4e88bfd1ea769d82c10779f2ded796db542971ca289b76863ede599
7b7e9ce183b43ccec278b10d92b87442ce0435bb1625171db5554b470239c50d2a0c3a41b2a38
807db070b47bfb3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d708844febaa8b6ddff0
1ab64d59358e6505c4ec1d7cbb14ed2212df458ecefc03fe03037b1505a4c9444322f5f98dfa9
1a4cb8c45860a2dadc7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891c90
78f62a8a9646a31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1
aa3a25bef06566cb34c79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4
b26d545365785ead8d63aef64a87c0b91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f1
7259ac45c9fa1c4bd3bf177d312ee52a6da023c05722a8738274dda8d1b04e99831cf57c87282
a256c565c296d0524a063a3a41a48a83009978d98d8abf61af68e8013b594fe151d9bec199902
c4c70b49584201743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c94d4c57c08
60b9d7b53d4cd261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43fd8aeebe5
e0ce2f54e3f0367eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247
de0e0894ad7cb7e1ae7ebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244
312158c2eb1b3e1117e194f0a1e4c783efbc62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b
055f4e7a2070fb096f56c415549cde74f3864e8b9fc27e3299724b4639986044b55928fd69727
85b280c25a3e21aab814ecbfb0c3cbec0914907ec907f25a1d88bce3d319ae8222a35945db62a
f7cc75cd29c1f5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a24d3e26c68e7bb10
e459f2577b90080359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346dad5
b55eddb4f977b326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a5117
7bcb089476b18cba09fa8b9b46d94a2946f358e1decb1998652c58a90852423e2c85e79d19724
461627e6390d1a81fb1a72f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589
df2e1b051783b8f718676b1defbae98ba496c2a935e92eeadea0a8393ef59f9e914f0743fe656
40ddf9981cea6dbdd957a534ad4e790efc974ee89938ad99d53c5b680775399326834729bb37b
082e795f8d87f52e6c8a8db68e515c277bbea82a7570d4280896c987a0608903e306c632a223c
55f0ea3682039c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f0487b2707b8
6286f8c4f55659b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153d87a7f
482d284b5b894ce1a78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32
430509b2fe4756303a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92
cdaa40f91a987e4a922ca81050e5bc3530ca85493bdf2a825374d0a8310a6860284ec3ec73232
6eeeffc42bbd42bc91b73e5e7c6b599d016490637629f3876c3e42f8db590e66a85a7838c818f
78fffb4853cbef09434989803545dca87657cf7c7e7e6afa71382bc10fa0bb6480f243eea1b86
1101006fa0cff3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8ffbdc11b0d0f9
61120e971015ad5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8b
425f1d73caf8496d742ed237f4c9fcd5a4e84fba7e27fb1a8ae12c4f0427ae24e910d951bd8c3
5d61f8a678db01caea8ef789a95b62ee1b8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f9
74c4c91cafc5bbf6b7ecfd57a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7
ac2393d93177f79ee5606c9df176f025ce49a6e5ff51a2a412ebf86ac0f40471c96ad4c119df2
30be6173df530ed656cbd8069214741ecdd0271c603fb6c4a8614ff878d33e726cac6693e938c
a3fba82c4995c14a2d4af9014fe4c4c50b794cac596b52189f66a7106fb325b526ea215820000
0000000000000000000000000000000000000000000000000000000000000000",
```

```
  "key_diag": "{2:
h'b788acf242f1f1d6532926d816e76e1636874267f2a48c84c4e65789ab80cc02', 1: 7,
3: -49, -1:
h'424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942ab8bdba
d7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd36
67e60d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade69
3868a460cbec03f4fc99a4e30bccffa8a475e5395396674ebb81a94937587880f6dbd27bf1c4f
5a9ee43cdd8b0e53b3b7fb49c73adfbc2d4f8c54303520c29bf97e26ee57db342d957c8939365
22d0942b41d82ee3772a00570adfb545c1143922b0496f826a0a970064b36ddf534b5f8e1c1cd
0b5565ea846b45431f0618143ece89777bb3f61179ad20295fe0a6e062ae6eecbc2ef38f2ac1a
22dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb8a999ad7a83e
5e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0b84c44b9b0
a8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a0
83f6ae07a114746d1bfdccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99d
dd88f48aaa4e88bfd1ea769d82c10779f2ded796db542971ca289b76863ede5997b7e9ce183b4
3ccec278b10d92b87442ce0435bb1625171db5554b470239c50d2a0c3a41b2a38807db070b47b
fb3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d708844febaa8b6ddff01ab64d59358e
6505c4ec1d7cbb14ed2212df458ecefc03fe03037b1505a4c9444322f5f98dfa91a4cb8c45860
a2dadc7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891c9078f62a8a9646
a31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef065
66cb34c79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d54536578
5ead8d63aef64a87c0b91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fa
1c4bd3bf177d312ee52a6da023c05722a8738274dda8d1b04e99831cf57c87282a256c565c296
d0524a063a3a41a48a83009978d98d8abf61af68e8013b594fe151d9bec199902c4c70b495842
01743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c94d4c57c0860b9d7b53d4c
d261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43fd8aeebe5e0ce2f54e3f0
367eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e0894ad7c
b7e1ae7ebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b
3e1117e194f0a1e4c783efbc62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b055f4e7a2070
fb096f56c415549cde74f3864e8b9fc27e3299724b4639986044b55928fd6972785b280c25a3e
21aab814ecbfb0c3cbec0914907ec907f25a1d88bce3d319ae8222a35945db62af7cc75cd29c1
f5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a24d3e26c68e7bb10e459f2577b90
080359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346dad5b55eddb4f977
b326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a51177bcb089476b1
8cba09fa8b9b46d94a2946f358e1decb1998652c58a90852423e2c85e79d19724461627e6390d
1a81fb1a72f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783
b8f718676b1defbae98ba496c2a935e92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea
6dbdd957a534ad4e790efc974ee89938ad99d53c5b68077539932683472 9bb37b082e795f8d87
f52e6c8a8db68e515c277bbea82a7570d4280896c987a0608903e306c632a223c55f0ea368203
9c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f0487b2707b86286f8c4f556
59b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153d87a7f482d284b5b89
4ce1a78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509b2fe47
56303a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdaa40f91a98
7e4a922ca81050e5bc3530ca85493bdf2a825374d0a8310a6860284ec3ec732326eeeffc42bbd
42bc91b73e5e7c6b599d016490637629f3876c3e42f8db590e66a85a7838c818f78fffb4853cb
ef09434989803545dca87657cf7c7e7e6afa71382bc10fa0bb6480f243eea1b861101006fa0cf
f3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8ffbdc11b0d0f961120e971015
ad5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8b425f1d73caf8
496d742ed237f4c9fcd5a4e84fba7e27fb1a8ae12c4f0427ae24e910d951bd8c35d61f8a678db
01caea8ef789a95b62ee1b8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5
bbf6b7ecfd57a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177
f79ee5606c9df176f025ce49a6e5ff51a2a412ebf86ac0f40471c96ad4c119df230be6173df53
0ed656cbd8069214741ecdd0271c603fb6c4a8614ff878d33e726cac6693e938ca3fba82c4995
c14a2d4af9014fe4c4c50b794cac596b52189f66a7106fb325b526ea', -2:
h'0000000000000000000000000000000000000000000000000000000000000000'}",
  "sign1":
"d2845827a2013830045820b788acf242f1f1d6532926d816e76e1636874267f2a48c84c4e657
89ab80cc02a0581d68656c6c6f20706f7374207175616e74756d207369676e617475726573590
```

```
cedd5bd2448903e4f81fb949158eefdeb93e2f40e58d3ffe5703d23954aeb547b2f490226b7e4
bc617a90156acd6afa662c0a5fe83be1f9e2d458436f9b9119c853c71fa7c7591b6471d9d6836
6d5bf12833c182ac927f7f0edd816e52ecea715c66e71e35029083fd26d0f16040e1da74b3789
50429fae8229af0495104549e2de909d6f8be09fcfc982e08425da663c181e862510b647f2f67
9ec16b7226fae6a9b90d8131c780a984b231c45811156470c143a5a9a611248532b574d40c0ef
9728264892ad97d523ca9146a8f965996dda13bc7eacde9040a7745a92790c2ec6672d8a66576
1495c873ddd4b9dc347db786ccfeabfb4f584bae9086f43639ade01f6c81a8f15d3c01ec9aaf0
b04699c38163de65967cc921acc66935cdbea43f393d9f65303a4640c081a6073f762fd78c532
911ecc60400688e329d7bca72d24fec7c8cd307130f0dfb37ce333470501d9e2ff16810ede1fc
811873fe8b38cf1c656d1927c190d240c0020514b9e71f6ad14fee3baac3444111c6a1a1676dc
92036e481c35b9db29a6282fa619a8b0110265b870f57c9b42d48b223c348b0621f55654fed73
5bae9344bae117deb583ab54e66a26f360468c47e3e40f553127164bb3eb803d17cb76d18d576
d942db7c18b5870fb26699b13e91f15c75b35d55eb2b10f6ffad617ee2c77b6bfaf2fc1b2a4cb
2703a528959f80d02e9325c88aff95cd51351cb6992e4e04ff124968d790056eef96664ed015c
4563ec71807022f6b92d8542a0feda0b8190ac2db5ea9c967836cda38839ce3bd5f46369bdb75
2fec8b047f4fb4608d6b21afc294564ac9d943566237f7a6dccebc1805cef60303f6058d43b7b
612cce12232e5a895f9e5237da5461b8ee17907b7caeb08d25488f80c786c849103d4c44c2c6b
ca1b57e9a3b55f307c9c299e322a9ec81abfcc5f38fe036fb17fa343748ef746f0e31350d05a4
7d0f37002b55624df95831c72ddce2dfd91382879b1673f5fcb1600c65d560034ee163eeb5c11
164ef88efed87f4e364fcd6e9d6cea384a62afbbaf34a6b4bdbd1b270a733a804d2f58703cc99
a91e8ce88d992f685b08d7ede6d36fc821e5094cc69085896f60b2a9d9cacb0c4d77bd44eab94
f11638b4798c3e462b8e020e4f22f0e14782051f16f2d7cb314dc24d4820549ff27ad458408d1
a663f5f5fc22a4e921ff26c97fa84c5f12d35ad9c89310d0c9c075ba373024a1dc208f5f17c59
2b5b5c3bdf4129bf304b2b731d383b844ffc48a234c0d07ff8ff550619f6b6eff3cad399c1a2b
61bd4aa68a7fd86cf661f73a309c3bafa512b6fc81f7702857d350744958be7050aac6d1f040b
fd866df38727df3bfd1ff3896f68550dfcb520c308fea4d1716790b1b6d51ef9c815e05d537c6
4460893beb9d82c350393ad15992e1c1ba16ff59a87c5d6fa19b4e88e2c433e0e96ffc6a8a7d4
9f84769ff9057bef8daf353e8516a852247e2f17ff13c81be266fff7c916c9b726a83058c66ac
0366335ee6e7b079095cf367bf79a3cc38da62d53e84a3b1a4ca97f40dd147e0d6c90dec5aa93
c178096884fc7718a675eee7900e4cb3ccc3601a08bf0003c3a029ca62a1924cc5bb83b29817f
892c5a5e7253abeb536d58d885008914a94bb2747f8a22478f35490d6f9693d0ff50073289add
a762b62823a9e4b134478642d9f1c44e20559bc5506df6baf76056c9cfbf15bb7134cd95f2952
7f006a0a49ebc4bb8e8ccfe3757a1f61c83a25ef44d2856f15d13272de73bfe726df6a775b181
57c85d419d20a7614dc18eb74dfb26af89fb2996ebcefe37dbdff37d3d2408411f9aad75f6d2c
ae122bf90e51ad6c4f6bbf85c50a50e78afaf86fa5e367d00c4fdade27148949fb8db485eb795
0d63c90013313db410ecf9b314a94c102dc8bf7e9e27ffdbedd64b9441bc687a534874739c527
59d1af213bf8ebd916e456561973f822e26aae6827b06ec4fcd45c146ac5c6637168e024c188f
93315dd57e7fb8a12879d1a83fbd2421368a1dbf54898b487951c24ad2535a0344d7f7380808d
44b207ac16b490c51155d275da3b863f775a13c8483f05c76aa6b64e8faf96fb2ff78672361d1
39183abe3957c6f431b342779e2fa96b07de7a530469d7096c01567c0c1ec7d3556d0ac636a94
82a84aef2087ad2c2bbb5fc49739c16d771203529b1134da0d0373a4e2305741711a21016a132
cd213fe2867b37465a103b68e16ce6ada0cbe1da2a0590f2a6d1afa8e06e29b4dc3c9ae21ef6c
a67e3c34a0e8f43dfaa0882d24e7fcc770ff28450efa19b88de83e8327e499b155529745473ce
9e1da81e9ce0fa1a816100c8d08741bfc8260fb0a6624c373b5823b587b34d16d1bddb6a03501
f6e8ccac59b877ee751cc841f2290eb8c37fbf119b93dbe6b0a700e3ee8e7a697b80d1a304a71
e3c1ebe734a412a8403c80d9ca3096c3a764bf8f6524427efd2648210a387fdcfbd05e4bbb6c3
53437750324b320458aaff555fe41765bb827c3c43d80bee1ef45dd3993d06ab1245e9c95aa79
76f54ba17aa031c8694e9b167a986cc289e534f1359f14ae335f7c41683dc85ccaf4ee2b4c1cd
d2116552f396ac8d6567e0f458c8cc0342086c31c0f8bffa3ac0d31677b10494c45e68e66432b
3f270a25cd389c126943b1d877ac6396d88a2df32c74eff79b9dbf1504b3cd55bcbbfa8ab2a16
979dfa53631a5d7d948bdc26c37eed9d2e2855338d029365b63b6b22abc211ed2ac1d3974550d
2d783be4c8b286fd8868a7c221ba15a527b1ccd14c50fc8590701693069 1f44f593a9c4ed3a1c
ec24f026735b719275fe27af036d234baeb812c5d60babae2f2b7032f0ad34a09cf98537a8b62
3f266eee28151acaa735af300ad6ce3e33c982b46db37479d5e3ad808b22b1453451dee5dbac2
6a03ae64990917b7060ee48281e1b8c486218a8c20d371f621fdd4466254c5d3cab08fc07dc96
b41c83d755377fe0363d11969802431cd4f2ff5cb92eb362591f12cf6f69fcd25727309235aa7
5acdd915c5a09403194a27b2f3b11cf51240ffeb0a457d383dd49503d3021ee19e83ef1b5d7f0
aa243c7a4b69978e1ef33911ecc320351a1e459ee1f672be88db2f0f5755758468a4509d067f5
```

```
edafb45334179d1317a4130e45320019cdc3113222c7933f0d12f3a71b23461cb9ebf072c3f70
01797c9124bb7f39778c7b393eeadeee2f6fd9ed76f39d16291722bf9bf68761e307438649ee7
e0042e7801e8c46d741fb216b13ab8d243c608d7d5cc6cc758d429c90b9ac1dc1275314bd506f
bd4e41767c8e8ec02282375b4f9e2d77b78c1c00dfd527c07506d0803dd2b9963535281cb9473
f03c37fc34b22aca3fea6630dc1f53e7ce938c9dbe3550076fd724675107f2cbdf186389f1894
92f6388da43baf6f9ea72982f665dcb1ec9f861021ee974abb8d0e36da8187dbb5dbe0c7100f0
c07fb6c0702e84e9591ee3c6cd9ca2482079556559ed691dbd97dc0bb1f052d64a938e2607951
92a876f97bf34097eb4380cb16e7415f58021fdf7dec9df8e521575b62d618bfc331b7efc3ea9
2394f73a0808df15e8794818649d9675edf3daaed3c5170a843d448bd1ec5d2e8e5dfd4254e33
4f4ad27d73b614fe0f8542a0a644f6f824422e8e1e10cd125b9363da6f015354baa244921f896
0ebc44f97ad1a29330ac6adbce3269922e9a1990feb9e4c89a7e34368a04b79f5db62cda84af2
ba028594de966674fa11ed21634922f8e5b4dbc0b9c9c899881dcaba8d6724d114b231b1dc308
8337a45070f5846c742f6184b0f0a1e55fe87bf37822cfc3ddb356c397ef85d9c1c0c65db191a
9d03469096c2ce42b919145708e3ee8b35e8d72db1c738d3a4389ae996f9604ea6903e61ac0bb
e56c8ba108cda00d1bdcc6904644705c9a858adc8cdc08f4449ef11f4d0e2855058647 8ac6c8a
8c8aed3927ca90e3b31fc8f5722aa68ad028642c14706b8ab0e413201305f9f1a899f2ddd5fb6
eff9985d0e57009956bc24f1d2c7b420eb3716a284df6408e38cedc4c7ec1c11c205c8567cda8
b12d4d8d97691015be532160a5a1731d8af5bd17a35f0d958ca423abfd1c6346f9472ba7d7aa7
0b845ff343acdf9153aa939bcd101f0578fafe84d4cc77c5b67eff3bdbc5bea27b703d4ca3cb5
c4f4943855ff512517b2c57535bcca7726e7c2cc739dc65cf805b018167ce1324ea5578f9af03
78eb281c2a3b28fdab5775a4249bbe587c06077eb20c1ddab672d4206cbcb0d48b461b92bdee4
249408f132e3a36e63e8ebd8dced63ef150da21c8264bdc65379a39f0331895e6d589444d9dbd
56f7626252d7145905dab7ed44ab0d14707fb1c19198196da8fc7388056a7a59fb0e19cc05d88
ce6a60802c73f9d785b48992318ae993397044f43c38709c319ef5a8e68a452bc5b79bd86ae50
981e58f7cbc58c7e17946804ab019c18a570c499e8b425a600201ef63a40f7d918b60ec9eeba6
68201cdab4624c35fdc014cdfaf2e7749e056f195f1eefc1949420e5569c461bc26f888b1aca0
418552ad2dc1c5b62e6c972b60ba643344d52cbdade3286497595a5adc1c40d0f10366cc9dbf9
fb0e22445d5e7ba14c759fbfd1d400000000000000000000000000000000000006080f181f25"
,
  "sign1_diag":
"18([h'a2013830045820b788acf242f1f1d6532926d816e76e1636874267f2a48c84c4e65789
ab80cc02', {},
h'68656c6c6f20706f7374207175616e74756d207369676e617475726573',
h'd5bd2448903e4f81fb949158eefdeb93e2f40e58d3ffe5703d23954aeb547b2f490226b7e4b
c617a90156acd6afa662c0a5fe83be1f9e2d458436f9b9119c853c71fa7c7591b6471d9d68366
d5bf12833c182ac927f7f0edd816e52ecea715c66e71e35029083fd26d0f16040e1da74b37895
0429fae8229af0495104549e2de909d6f8be09fcfc982e08425da663c181e862510b647f2f679
ec16b7226fae6a9b90d8131c780a984b231c45811156470c143a5a9a611248532b574d40c0ef9
728264892ad97d523ca9146a8f965996dda13bc7eacde9040a7745a92790c2ec6672d8a665761
495c873ddd4b9dc347db786ccfeabfb4f584bae9086f43639ade01f6c81a8f15d3c01ec9aaf0b
04699c38163de65967cc921acc66935cdbea43f393d9f65303a4640c081a6073f762fd78c5329
11ecc60400688e329d7bca72d24fec7c8cd307130f0dfb37ce333470501d9e2ff16810ede1fc8
11873fe8b38cf1c656d1927c190d240c0020514b9e71f6ad14fee3baac3444111c6a1a1676dc9
2036e481c35b9db29a6282fa619a8b0110265b870f57c9b42d48b223c348b0621f55654fed735
bae9344bae117deb583ab54e66a26f360468c47e3e40f553127164bb3eb803d17cb76d18d576d
942db7c18b5870fb26699b13e91f15c75b35d55eb2b10f6ffad617ee2c77b6bfaf2fc1b2a4cb2
703a528959f80d02e9325c88aff95cd51351cb6992e4e04ff124968d790056eef96664ed015c4
563ec71807022f6b92d8542a0feda0b8190ac2db5ea9c967836cda38839ce3bd5f46369bdb752
fec8b047f4fb4608d6b21afc294564ac9d943566237f7a6dccebc1805cef60303f6058d43b7b6
12cce12232e5a895f9e5237da5461b8ee17907b7caeb08d25488f80c786c849103d4c44c2c6bc
a1b57e9a3b55f307c9c299e322a9ec81abfcc5f38fe036fb17fa343748ef746f0e31350d05a47
d0f37002b55624df95831c72ddce2dfd91382879b1673f5fcb1600c65d560034ee163eeb5c111
64ef88efed87f4e364fcd6e9d6cea384a62afbbaf34a6b4bdbd1b270a733a804d2f58703cc99a
91e8ce88d992f685b08d7ede6d36fc821e5094cc69085896f60b2a9d9cacb0c4d77bd44eab94f
11638b4798c3e462b8e020e4f22f0e14782051f16f2d7cb314dc24d4820549ff27ad458408d1a
663f5f5fc22a4e921ff26c97fa84c5f12d35ad9c89310d0c9c075ba373024a1dc208f5f17c592
b5b5c3bdf4129bf304b2b731d383b844ffc48a234c0d07ff8ff550619f6b6eff3cad399c1a2b6
1bd4aa68a7fd86cf661f73a309c3bafa512b6fc81f7702857d350744958be7050aac6d1f040bf
```

```
d866df38727df3bfd1ff3896f68550dfcb520c308fea4d1716790b1b6d51ef9c815e05d537c64
460893beb9d82c350393ad15992e1c1ba16ff59a87c5d6fa19b4e88e2c433e0e96ffc6a8a7d49
f84769ff9057bef8daf353e8516a852247e2f17ff13c81be266fff7c916c9b726a83058c66ac0
366335ee6e7b079095cf367bf79a3cc38da62d53e84a3b1a4ca97f40dd147e0d6c90dec5aa93c
178096884fc7718a675eee7900e4cb3ccc3601a08bf0003c3a029ca62a1924cc5bb83b29817f8
92c5a5e7253abeb536d58d885008914a94bb2747f8a22478f35490d6f9693d0ff50073289adda
762b62823a9e4b134478642d9f1c44e20559bc5506df6baf76056c9cfbf15bb7134cd95f29527
f006a0a49ebc4bb8e8ccfe3757a1f61c83a25ef44d2856f15d13272de73bfe726df6a775b1815
7c85d419d20a7614dc18eb74dfb26af89fb2996ebcefe37dbdff37d3d2408411f9aad75f6d2ca
e122bf90e51ad6c4f6bbf85c50a50e78afaf86fa5e367d00c4fdade27148949fb8db485eb7950
d63c90013313db410ecf9b314a94c102dc8bf7e9e27ffdbedd64b9441bc687a534874739c5275
9d1af213bf8ebd916e456561973f822e26aae6827b06ec4fcd45c146ac5c6637168e024c188f9
3315dd57e7fb8a12879d1a83fbd2421368a1dbf54898b487951c24ad2535a0344d7f7380808d4
4b207ac16b490c51155d275da3b863f775a13c8483f05c76aa6b64e8faf96fb2ff78672361d13
9183abe3957c6f431b342779e2fa96b07de7a530469d7096c01567c0c1ec7d3556d0ac636a948
2a84aef2087ad2c2bbb5fc49739c16d771203529b1134da0d0373a4e2305741711a21016a132c
d213fe2867b37465a103b68e16ce6ada0cbe1da2a0590f2a6d1afa8e06e29b4dc3c9ae21ef6ca
67e3c34a0e8f43dfaa0882d24e7fcc770ff28450efa19b88de83e8327e499b155529745473ce9
e1da81e9ce0fa1a816100c8d08741bfc8260fb0a6624c373b5823b587b34d16d1bddb6a03501f
6e8ccac59b877ee751cc841f2290eb8c37fbf119b93dbe6b0a700e3ee8e7a697b80d1a304a71e
3c1ebe734a412a8403c80d9ca3096c3a764bf8f6524427efd2648210a387fdcfbd05e4bbb6c35
3437750324b320458aaff555fe41765bb827c3c43d80bee1ef45dd3993d06ab1245e9c95aa797
6f54ba17aa031c8694e9b167a986cc289e534f1359f14ae335f7c41683dc85ccaf4ee2b4c1cdd
2116552f396ac8d6567e0f458c8cc0342086c31c0f8bffa3ac0d31677b10494c45e68e66432b3
f270a25cd389c126943b1d877ac6396d88a2df32c74eff79b9dbf1504b3cd55bcbbfa8ab2a169
79dfa53631a5d7d948bdc26c37eed9d2e2855338d029365b63b6b22abc211ed2ac1d3974550d2
d783be4c8b286fd8868a7c221ba15a527b1ccd14c50fc8590701693069 1f44f593a9c4ed3a1ce
c24f026735b719275fe27af036d234baeb812c5d60babae2f2b7032f0ad34a09cf98537a8b623
f266eee28151acaa735af300ad6ce3e33c982b46db37479d5e3ad808b22b1453451dee5dbac26
a03ae64990917b7060ee48281e1b8c486218a8c20d371f621fdd4466254c5d3cab08fc07dc96b
41c83d755377fe0363d11969802431cd4f2ff5cb92eb362591f12cf6f69fcd25727309235aa75
acdd915c5a09403194a27b2f3b11cf51240ffeb0a457d383dd49503d3021ee19e83ef1b5d7f0a
a243c7a4b69978e1ef33911ecc320351a1e459ee1f672be88db2f0f5755758468a4509d067f5e
dafb45334179d1317a4130e45320019cdc3113222c7933f0d12f3a71b23461cb9ebf072c3f700
1797c9124bb7f39778c7b393eeadeee2f6fd9ed76f39d16291722bf9bf68761e307438649ee7e
0042e7801e8c46d741fb216b13ab8d243c608d7d5cc6cc758d429c90b9ac1dc1275314bd506fb
d4e41767c8e8ec02282375b4f9e2d77b78c1c00dfd527c07506d0803dd2b9963535281cb9473f
03c37fc34b22aca3fea6630dc1f53e7ce938c9dbe3550076fd724675107f2cbdf186389f18949
2f6388da43baf6f9ea72982f665dcb1ec9f861021ee974abb8d0e36da8187dbb5dbe0c7100f0c
07fb6c0702e84e9591ee3c6cd9ca2482079556559ed691dbd97dc0bb1f052d64a938e26079519
2a876f97bf34097eb4380cb16e7415f58021fdf7dec9df8e521575b62d618bfc331b7efc3ea92
394f73a0808df15e8794818649d9675edf3daaed3c5170a843d448bd1ec5d2e8e5dfd4254e334
f4ad27d73b614fe0f8542a0a644f6f824422e8e1e10cd125b9363da6f015354baa244921f8960
ebc44f97ad1a29330ac6adbce3269922e9a1990feb9e4c89a7e34368a04b79f5db62cda84af2b
a028594de966674fa11ed21634922f8e5b4dbc0b9c9c899881dcaba8d6724d114b231b1dc3088
337a45070f5846c742f6184b0f0a1e55fe87bf37822cfc3ddb356c397ef85d9c1c0c65db191a9
d03469096c2ce42b919145708e3ee8b35e8d72db1c738d3a4389ae996f9604ea6903e61ac0bbe
56c8ba108cda00d1bdcc6904644705c9a858adc8cdc08f4449ef11f4d0e28550586478ac6c8a8
c8aed3927ca90e3b31fc8f5722aa68ad028642c14706b8ab0e413201305f9f1a899f2ddd5fb6e
ff9985d0e57009956bc24f1d2c7b420eb3716a284df6408e38cedc4c7ec1c11c205c8567cda8b
12d4d8d97691015be532160a5a1731d8af5bd17a35f0d958ca423abfd1c6346f9472ba7d7aa70
b845ff343acdf9153aa939bcd101f0578fafe84d4cc77c5b67eff3bdbc5bea27b703d4ca3cb5c
4f4943855ff512517b2c57535bcca7726e7c2cc739dc65cf805b018167ce1324ea5578f9af037
8eb281c2a3b28fdab5775a4249bbe587c06077eb20c1ddab672d4206cbcb0d48b461b92bdee42
49408f132e3a36e63e8ebd8dced63ef150da21c8264bdc65379a39f0331895e6d589444d9dbd5
6f7626252d7145905dab7ed44ab0d14707fb1c19198196da8fc7388056a7a59fb0e19cc05d88c
e6a60802c73f9d785b48992318ae993397044f43c38709c319ef5a8e68a452bc5b79bd86ae509
81e58f7cbc58c7e17946804ab019c18a570c499e8b425a600201ef63a40f7d918b60ec9eeba66
```

```
8201cdab4624c35fdc014cdfaf2e7749e056f195f1eefc1949420e5569c461bc26f888b1aca04
18552ad2dc1c5b62e6c972b60ba643344d52cbdade3286497595a5adc1c40d0f10366cc9dbf9f
b0e22445d5e7ba14c759fbfd1d400000000000000000000000000000000000006080f181f25']
)",
  "raw_to_be_signed":
"846a5369676e6174757265315827a2013830045820b788acf242f1f1d6532926d816e76e1636
874267f2a48c84c4e65789ab80cc0240581d68656c6c6f20706f7374207175616e74756d20736
9676e617475726573",
  "raw_signature":
"d5bd2448903e4f81fb949158eefdeb93e2f40e58d3ffe5703d23954aeb547b2f490226b7e4bc
617a90156acd6afa662c0a5fe83be1f9e2d458436f9b9119c853c71fa7c7591b6471d9d68366d
5bf12833c182ac927f7f0edd816e52ecea715c66e71e35029083fd26d0f16040e1da74b378950
429fae8229af0495104549e2de909d6f8be09fcfc982e08425da663c181e862510b647f2f679e
c16b7226fae6a9b90d8131c780a984b231c45811156470c143a5a9a611248532b574d40c0ef97
28264892ad97d523ca9146a8f965996dda13bc7eacde9040a7745a92790c2ec6672d8a6657614
95c873ddd4b9dc347db786ccfeabfb4f584bae9086f43639ade01f6c81a8f15d3c01ec9aaf0b0
4699c38163de65967cc921acc66935cdbea43f393d9f65303a4640c081a6073f762fd78c53291
1ecc60400688e329d7bca72d24fec7c8cd307130f0dfb37ce333470501d9e2ff16810ede1fc81
1873fe8b38cf1c656d1927c190d240c0020514b9e71f6ad14fee3baac3444111c6a1a1676dc92
036e481c35b9db29a6282fa619a8b0110265b870f57c9b42d48b223c348b0621f55654fed735b
ae9344bae117deb583ab54e66a26f360468c47e3e40f553127164bb3eb803d17cb76d18d576d9
42db7c18b5870fb26699b13e91f15c75b35d55eb2b10f6ffad617ee2c77b6bfaf2fc1b2a4cb27
03a528959f80d02e9325c88aff95cd51351cb6992e4e04ff124968d790056eef96664ed015c45
63ec71807022f6b92d8542a0feda0b8190ac2db5ea9c967836cda38839ce3bd5f46369bdb752f
ec8b047f4fb4608d6b21afc294564ac9d943566237f7a6dccebc1805cef60303f6058d43b7b61
2cce12232e5a895f9e5237da5461b8ee17907b7caeb08d25488f80c786c849103d4c44c2c6bca
1b57e9a3b55f307c9c299e322a9ec81abfcc5f38fe036fb17fa343748ef746f0e31350d05a47d
0f37002b55624df95831c72ddce2dfd91382879b1673f5fcb1600c65d560034ee163eeb5c1116
4ef88efed87f4e364fcd6e9d6cea384a62afbbaf34a6b4bdbd1b270a733a804d2f58703cc99a9
1e8ce88d992f685b08d7ede6d36fc821e5094cc69085896f60b2a9d9cacb0c4d77bd44eab94f1
1638b4798c3e462b8e020e4f22f0e14782051f16f2d7cb314dc24d4820549ff27ad458408d1a6
63f5f5fc22a4e921ff26c97fa84c5f12d35ad9c89310d0c9c075ba373024a1dc208f5f17c592b
5b5c3bdf4129bf304b2b731d383b844ffc48a234c0d07ff8ff550619f6b6eff3cad399c1a2b61
bd4aa68a7fd86cf661f73a309c3bafa512b6fc81f7702857d350744958be7050aac6d1f040bfd
866df38727df3bfd1ff3896f68550dfcb520c308fea4d1716790b1b6d51ef9c815e05d537c644
60893beb9d82c350393ad15992e1c1ba16ff59a87c5d6fa19b4e88e2c433e0e96ffc6a8a7d49f
84769ff9057bef8daf353e8516a852247e2f17ff13c81be266fff7c916c9b726a83058c66ac03
66335ee6e7b079095cf367bf79a3cc38da62d53e84a3b1a4ca97f40dd147e0d6c90dec5aa93c1
78096884fc7718a675eee7900e4cb3ccc3601a08bf0003c3a029ca62a1924cc5bb83b29817f89
2c5a5e7253abeb536d58d885008914a94bb2747f8a22478f35490d6f9693d0ff50073289adda7
62b62823a9e4b134478642d9f1c44e20559bc5506df6baf76056c9cfbf15bb7134cd95f29527f
006a0a49ebc4bb8e8ccfe3757a1f61c83a25ef44d2856f15d13272de73bfe726df6a775b18157
c85d419d20a7614dc18eb74dfb26af89fb2996ebcefe37dbdff37d3d2408411f9aad75f6d2cae
122bf90e51ad6c4f6bbf85c50a50e78afaf86fa5e367d00c4fdade27148949fb8db485eb7950d
63c90013313db410ecf9b314a94c102dc8bf7e9e27ffdbedd64b9441bc687a534874739c52759
d1af213bf8ebd916e456561973f822e26aae6827b06ec4fcd45c146ac5c6637168e024c188f93
315dd57e7fb8a12879d1a83fbd2421368a1dbf54898b487951c24ad2535a0344d7f7380808d44
b207ac16b490c51155d275da3b863f775a13c8483f05c76aa6b64e8faf96fb2ff78672361d139
183abe3957c6f431b342779e2fa96b07de7a530469d7096c01567c0c1ec7d3556d0ac636a9482
a84aef2087ad2c2bbb5fc49739c16d771203529b1134da0d0373a4e2305741711a21016a132cd
213fe2867b37465a103b68e16ce6ada0cbe1da2a0590f2a6d1afa8e06e29b4dc3c9ae21ef6ca6
7e3c34a0e8f43dfaa0882d24e7fcc770ff28450efa19b88de83e8327e499b155529745473ce9e
1da81e9ce0fa1a816100c8d08741bfc8260fb0a6624c373b5823b587b34d16d1bddb6a03501f6
e8ccac59b877ee751cc841f2290eb8c37fbf119b93dbe6b0a700e3ee8e7a697b80d1a304a71e3
c1ebe734a412a8403c80d9ca3096c3a764bf8f6524427efd2648210a387fdcfbd05e4bbb6c353
437750324b320458aaff555fe41765bb827c3c43d80bee1ef45dd3993d06ab1245e9c95aa7976
f54ba17aa031c8694e9b167a986cc289e534f1359f14ae335f7c41683dc85ccaf4ee2b4c1cdd2
116552f396ac8d6567e0f458c8cc0342086c31c0f8bffa3ac0d31677b10494c45e68e66432b3f
```

```
270a25cd389c126943b1d877ac6396d88a2df32c74eff79b9dbf1504b3cd55bcbbfa8ab2a1697
9dfa53631a5d7d948bdc26c37eed9d2e2855338d029365b63b6b22abc211ed2ac1d3974550d2d
783be4c8b286fd8868a7c221ba15a527b1ccd14c50fc85907016930691f44f593a9c4ed3a1cec
24f026735b719275fe27af036d234baeb812c5d60babae2f2b7032f0ad34a09cf98537a8b623f
266eee28151acaa735af300ad6ce3e33c982b46db37479d5e3ad808b22b1453451dee5dbac26a
03ae64990917b7060ee48281e1b8c486218a8c20d371f621fdd4466254c5d3cab08fc07dc96b4
1c83d755377fe0363d11969802431cd4f2ff5cb92eb362591f12cf6f69fcd25727309235aa75a
cdd915c5a09403194a27b2f3b11cf51240ffeb0a457d383dd49503d3021ee19e83ef1b5d7f0aa
243c7a4b69978e1ef33911ecc320351a1e459ee1f672be88db2f0f5755758468a4509d067f5ed
afb45334179d1317a4130e45320019cdc3113222c7933f0d12f3a71b23461cb9ebf072c3f7001
797c9124bb7f39778c7b393eeadeee2f6fd9ed76f39d16291722bf9bf68761e307438649ee7e0
042e7801e8c46d741fb216b13ab8d243c608d7d5cc6cc758d429c90b9ac1dc1275314bd506fbd
4e41767c8e8ec02282375b4f9e2d77b78c1c00dfd527c07506d0803dd2b9963535281cb9473f0
3c37fc34b22aca3fea6630dc1f53e7ce938c9dbe3550076fd724675107f2cbdf186389f189492
f6388da43baf6f9ea72982f665dcb1ec9f861021ee974abb8d0e36da8187dbb5dbe0c7100f0c0
7fb6c0702e84e9591ee3c6cd9ca2482079556559ed691dbd97dc0bb1f052d64a938e260795192
a876f97bf34097eb4380cb16e7415f58021fdf7dec9df8e521575b62d618bfc331b7efc3ea923
94f73a0808df15e8794818649d9675edf3daaed3c5170a843d448bd1ec5d2e8e5dfd4254e334f
4ad27d73b614fe0f8542a0a644f6f824422e8e1e10cd125b9363da6f015354baa244921f8960e
bc44f97ad1a29330ac6adbce3269922e9a1990feb9e4c89a7e34368a04b79f5db62cda84af2ba
028594de966674fa11ed21634922f8e5b4dbc0b9c9c899881dcaba8d6724d114b231b1dc30883
37a45070f5846c742f6184b0f0a1e55fe87bf37822cfc3ddb356c397ef85d9c1c0c65db191a9d
03469096c2ce42b919145708e3ee8b35e8d72db1c738d3a4389ae996f9604ea6903e61ac0bbe5
6c8ba108cda00d1bdcc6904644705c9a858adc8cdc08f4449ef11f4d0e28550586478ac6c8a8c
8aed3927ca90e3b31fc8f5722aa68ad028642c14706b8ab0e413201305f9f1a899f2ddd5fb6ef
f9985d0e57009956bc24f1d2c7b420eb3716a284df6408e38cedc4c7ec1c11c205c8567cda8b1
2d4d8d97691015be532160a5a1731d8af5bd17a35f0d958ca423abfd1c6346f9472ba7d7aa70b
845ff343acdf9153aa939bcd101f0578fafe84d4cc77c5b67eff3bdbc5bea27b703d4ca3cb5c4
f4943855ff512517b2c57535bcca7726e7c2cc739dc65cf805b018167ce1324ea5578f9af0378
eb281c2a3b28fdab5775a4249bbe587c06077eb20c1ddab672d4206cbcb0d48b461b92bdee424
9408f132e3a36e63e8ebd8dced63ef150da21c8264bdc65379a39f0331895e6d589444d9dbd56
f7626252d7145905dab7ed44ab0d14707fb1c19198196da8fc7388056a7a59fb0e19cc05d88ce
6a60802c73f9d785b48992318ae993397044f43c38709c319ef5a8e68a452bc5b79bd86ae5098
1e58f7cbc58c7e17946804ab019c18a570c499e8b425a600201ef63a40f7d918b60ec9eeba668
201cdab4624c35fdc014cdfaf2e7749e056f195f1eefc1949420e5569c461bc26f888b1aca041
8552ad2dc1c5b62e6c972b60ba643344d52cbdade3286497595a5adc1c40d0f10366cc9dbf9fb
0e22445d5e7ba14c759fbfd1d400000000000000000000000000000000006080f181f25",
  "raw_public_key":
"424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942ab8bdbad
7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd366
7e60d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693
868a460cbec03f4fc99a4e30bccffa8a475e5395396674ebb81a94937587880f6dbd27bf1c4f5
a9ee43cdd8b0e53b3b7fb49c73adfbc2d4f8c54303520c29bf97e26ee57db342d957c89393652
2d0942b41d82ee3772a00570adfb545c1143922b0496f826a0a970064b36ddf534b5f8e1c1cd0
b5565ea846b45431f0618143ece89777bb3f61179ad20295fe0a6e062ae6eecbc2ef38f2ac1a2
2dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb8a999ad7a83e5
e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0b84c44b9b0a
8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a08
3f6ae07a114746d1bfdccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99dd
d88f48aaa4e88bfd1ea769d82c10779f2ded796db542971ca289b76863ede5997b7e9ce183b43
ccec278b10d92b87442ce0435bb1625171db5554b470239c50d2a0c3a41b2a38807db070b47bf
b3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d708844febaa8b6ddff01ab64d59358e6
505c4ec1d7cbb14ed2212df458ecefc03fe03037b1505a4c9444322f5f98dfa91a4cb8c45860a
2dadc7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891c9078f62a8a9646a
31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef0656
6cb34c79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d545365785
ead8d63aef64a87c0b91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fa1
c4bd3bf177d312ee52a6da023c05722a8738274dda8d1b04e99831cf57c87282a256c565c296d
```

```
0524a063a3a41a48a83009978d98d8abf61af68e8013b594fe151d9bec199902c4c70b4958420
1743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c94d4c57c0860b9d7b53d4cd
261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43fd8aeebe5e0ce2f54e3f03
67eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e0894ad7cb
7e1ae7ebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b3
e1117e194f0a1e4c783efbc62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b055f4e7a2070f
b096f56c415549cde74f3864e8b9fc27e3299724b4639986044b55928fd6972785b280c25a3e2
1aab814ecbfb0c3cbec0914907ec907f25a1d88bce3d319ae8222a35945db62af7cc75cd29c1f
5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a24d3e26c68e7bb10e459f2577b900
80359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346dad5b55eddb4f977b
326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a51177bcb089476b18
cba09fa8b9b46d94a2946f358e1decb1998652c58a90852423e2c85e79d19724461627e6390d1
a81fb1a72f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783b
8f718676b1defbae98ba496c2a935e92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea6
dbdd957a534ad4e790efc974ee89938ad99d53c5b6807753993268347 29bb37b082e795f8d87f
52e6c8a8db68e515c277bbea82a7570d4280896c987a0608903e306c632a223c55f0ea3682039
c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f0487b2707b86286f8c4f5565
9b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153d87a7f482d284b5b894
ce1a78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509b2fe475
6303a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdaa40f91a987
e4a922ca81050e5bc3530ca85493bdf2a825374d0a8310a6860284ec3ec732326eeeffc42bbd4
2bc91b73e5e7c6b599d016490637629f3876c3e42f8db590e66a85a7838c818f78fffb4853cbe
f09434989803545dca87657cf7c7e7e6afa71382bc10fa0bb6480f243eea1b861101006fa0cff
3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8ffbdc11b0d0f961120e971015a
d5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8b425f1d73caf84
96d742ed237f4c9fcd5a4e84fba7e27fb1a8ae12c4f0427ae24e910d951bd8c35d61f8a678db0
1caea8ef789a95b62ee1b8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5b
bf6b7ecfd57a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177f
79ee5606c9df176f025ce49a6e5ff51a2a412ebf86ac0f40471c96ad4c119df230be6173df530
ed656cbd8069214741ecdd0271c603fb6c4a8614ff878d33e726cac6693e938ca3fba82c4995c
14a2d4af9014fe4c4c50b794cac596b52189f66a7106fb325b526ea"
}
```

Figure 7: ML_DSA_65

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "key":
"a5025820d9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd565247a166cb4fa0107
03383120590a20e45ffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b
468cfc82bb929f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f1
24d5e60bd68b8c7e31fe01c7b0dc65ae470501cc565a6e1dfcfcfd12565433c4afedd511821e2
e9610c45275e2836dee35ced69d7efa672fd1e4318bef5eb6e897e8b451aa202ded042b2aaef7
7a7be3f699146da229a8bdb3ffa496445967e75217bfbc9048f9956443d8731f833eb30de10da
c96fffe7cf65ea0445c3e31e8601e133be6a100764fe3196e267726441f31751fbf9a6f588064
4f4e7275e57de2b0f105e4db055d50dd1c9c934fddf535b8de28b0c74c0449f222cd2ed0bb8fb
c775ccee8c940665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee758185
6ebd68f26845956e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab
932e69f778e2ceefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9
d5f98a3655098941993a1594860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98
e25a8583ac8dac1f861fd58e2afba5de5a52e020904f5b42bc0874e35befcf3e6119684768f36
e008f04712177cebe627607381e56eaaee161c1729b8de51dbde474d48cc68249ea27162b8799
3e60c84ed6cc6423cb3676d9eb50b2cab5a3a049ef131381d623fa6fbcbc9db1e7cc025ea0418
b9dad2cc6ccd4e95fa2cec24feeca70318a751716b7213f63edbf65a63338357f838f94ec0718
22c24851248885107b3d1c4e924678c7614ea1af038104619f2ae372940becfa69e29cbb5ff6c
3e20a47be4a4f74bac34c133c00a6a706accc6ffd3d8e4fbd69a99704e1283c850d8c58d1e575
3cd9587b83c4c346cb9a58137213ec10834c66adfe2bb5c501a8ef2ecadd1b677a3df1a6deb86
ebf0722c4f5030e20f9018dd5b6fc53eea24fd92b7b5b4025feae996d3e48fd4c650d82dbad7e
af936639698512f26253d2ef6847c8518e8565cc9a5495c6fff57cde7323882c54a7db470ab2d
af8ffd2bf794fa7c692d9e7fbd532eecc1d7880e2ca0b3216128be28b4a9f1d151fac97808b0b
d98b7b43a612a9ac865812bfeac6f47460277840b52a3b087f916ca7cedc0f768ea2bd19ea211
55f84b4a04c4000ad2ae0587154d560bc0a477a4f9329a8984dd31eb1f2a05e3d918701d630cf
ca9af61ef088d2c5581acb463e439902e5d425719e956b8d6df7305b28e0ff27d3ad0de2085d2
92499b19a3390d4396fb3bac9a8d8cbead2a7a4290fc9ac6fca045f98a614a45a39cbe24360f8
4d14f8e472712aceb74dbf45b53d49a0e4737e476ffc4d5b2f7cd247aa186d3b764ad9e9cfeee
456a73c291d8de3912414ac43911c372173ad7b472af35c6853ced2fe7b5fe0a89565ab33baa6
f65cdd928319d7065e040e7a5e84f9aa903f7648094bad07136b16927b8ec6dbc2bef0cc2856d
e1e795923e1412c49f24deeb6c21f6c8a9765c9c7986e0da4b4c67d8e0d0c8d466824fb923d85
73148990cd2ef133c78ceecab72ed9dd285c5a3766852d54534207ffd34027f6c76ede8fd1a32
d72c30048bbaa797d5df6fde27d087de5721ad7b7fa3e8d3f70d6bfc3ab2e252335368bbfa15a
cb5cb37d4694e8b23cebe25de9c925a221a183b904d3f85df9929a919c54d6f87457373a0d6ec
c1403e4cbbe620999435e80696634cd1a8e4747e9825bfa336e5bbad14f73640f1b9febe800db
aefe1630c61fae635b074c564eaa9db189c9e7302873fc64e6d497bc5c29080987a07a21d4af2
10703a4fa07f2fd816f12fd1e29b4c0f44afe9bd4a1eaa8a7ae6f02a5b4258f52caf6127f6263
2a67cf4e8310be56a7c28c86b2e277600c3e92c8d23d42586244c571e90568df202f2f6d81f86
0a565f9eb91a3c78372e2a8b1be61c5418cf49bf2d6c8955d4a482a9919b7660b3f9a4404ffc4
54ea073e1e4b2689ab2cca4e46bd7004a6c491fa26ee7a57d60f35edb2b821e6266442c8f335d
452d524c772e0353724c23c7dd15b7aa155e91442022140c5fcb0153147edcf3e8952f6f0399a
3c88066a72756c9409915de63f64fa797841c57c796c6fc550ef745dfe9f179457f94755ae5a2
506a764f327e550be3dc14dd41f3b04b147d454938c63a8d69b2ea4c5710ec0b36e3a6c72571f
a5d59dde036c42033df35af056966ff0cd1204008971aa6ba9fb97b685ab9ffa2a9d1778104cd
2c3b326de1fcbc242e94d0311c3275b12850ed30ceead3a2ee6d060508411d4396f5421d8b6d0
67cf7cb5e826785fbe119e05e21bd879b64f57cb0cd1972c2815f20abe7ce6ab34d0f471af44b
aad179e90644122f5f33288e689ddddc5ce833e9755df1e73c65c5a201c4ede2ffa6b19274927
719d2d38fdb7a65aa43708b7fa9a94aa7d3210253d78d3b181e1020d0000bd0a1dc05d447f9f5
8ebeb84c65b36c8afcb83727a1508994e826957a663b0b9b8a003325ab6d6d6462ee4e106019c
0dffe10323b7bde7d82a38f85fd08786e860ba66c161b64b0708c363de5c6af62d8db3c243d1e
1b712cb1d59e942b9b6b4295a5a500b182cbd5fd1bc6ce9376d91b47a2284f1fbe0ad1c048cc2
cfbb4afa3a9eb9697503b69feca990eba7e9441af9ca44cb3ac6b5ed66e591c201fe30efa8a7c
471dc613d6254c263a8e132104bec47f1aacb3b2fcd4051b69b5e3fcb1c147a65c2f90c4b5188
bafc521cab03c12a309da50b5a7517727ed41228ed123fe1b152f6a6319cd623bf34ad7b8e064
```

```
ab993260bcbd405f5b7fff9b2fa40ba5ed5630242539e5d96823e89dc818a13d16675ee3079d9
76f694f5acc9760ae789e9b3391b289e0e22a7ef17cc6a4577157b6d95c09baa4fd532e3ee0a2
90810ed35e56bb19d9b61fb98a97c617425b06093d98a5cf0ee2dd127f0eea600b9a0c67fbe76
1db9b77e5d5bba9701da1b883e521a0cfe88451f57bd36085b67e56f061f84a2e6a152a71bce6
e522daab6a0a33ce22e537fa9793d28b617e6c0a4176a83aa3be578afac0f2f5547c5516d2189
84755b7445c7143afa4e551fce0071bdb873b34e6b9e2b9e79ed0c69d288ed6421f237e860a0c
6492ebbdd2a44c2c4f368dbe99941b1e8561d859d3859f496cee3d741f252973f8fcc539c409e
35cc80a5ed6df23cc3a65601313f5d681fd9540c5291a9e30a72e38c96413c47c61ff84fde78d
011b01b4154d1b920af003f7abb1e1999dea6a766cf9fd2702b3ce0ee57af931b62124b0861b1
63a3b91aa4bea28076c3432df3b29b6c4e1ba588def420071fc157de90eb2722ecc9ab00df3c6
69383a61a91bb67bd287ce349b4745ee7a479dbceef166b9acc412eb579fcd6437307edda253d
606b7be7599c38092bc52a8598480edab8b82b1d21c565d2137ceae0b6642619b16133d91205d
6355029e9cdfeb9a28b373d95916b6b707d4c712c09cf36daf1a511b2bedb1aa70ee58d46a066
6bb287784b0a3840c589a7a04d5d6f2216be90aa4a512d5632f5c9bfe7b8b13382f999b95d367
c7c46b968074ce315197a5ff3545c7b77a804ade56a95b5c24cdece5937b5c0366d93ad03da9b
c5db1b551dfb91e9b343d2b57b763439686d4a32158200000000000000000000000000000000
0000000000000000000000000000000000",
  "key_diag": "{2:
h'd9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd565247a166cb4fa', 1: 7,
3: -50, -1:
h'e45ffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b468cfc82bb92
9f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f124d5e60bd68b
8c7e31fe01c7b0dc65ae470501cc565a6e1dfcfcfd12565433c4afedd511821e2e9610c45275e
2836dee35ced69d7efa672fd1e4318bef5eb6e897e8b451aa202ded042b2aaef77a7be3f69914
6da229a8bdb3ffa496445967e75217bfbc9048f9956443d8731f833eb30de10dac96fffe7cf65
ea0445c3e31e8601e133be6a100764fe3196e267726441f31751fbf9a6f5880644f4e7275e57d
e2b0f105e4db055d50dd1c9c934fddf535b8de28b0c74c0449f222cd2ed0bb8fbc775ccee8c94
0665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee7581856ebd68f26845
956e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab932e69f778e2
ceefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a365509
8941993a1594860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8d
ac1f861fd58e2afba5de5a52e020904f5b42bc0874e35befcf3e6119684768f36e008f0471217
7cebe627607381e56eaaee161c1729b8de51dbde474d48cc68249ea27162b87993e60c84ed6cc
6423cb3676d9eb50b2cab5a3a049ef131381d623fa6fbcbc9db1e7cc025ea0418b9dad2cc6ccd
4e95fa2cec24feeca70318a751716b7213f63edbf65a63338357f838f94ec071822c248512488
85107b3d1c4e924678c7614ea1af038104619f2ae372940becfa69e29cbb5ff6c3e20a47be4a4
f74bac34c133c00a6a706accc6ffd3d8e4fbd69a99704e1283c850d8c58d1e5753cd9587b83c4
c346cb9a58137213ec10834c66adfe2bb5c501a8ef2ecadd1b677a3df1a6deb86ebf0722c4f50
30e20f9018dd5b6fc53eea24fd92b7b5b4025feae996d3e48fd4c650d82dbad7eaf9366396985
12f26253d2ef6847c8518e8565cc9a5495c6fff57cde7323882c54a7db470ab2daf8ffd2bf794
fa7c692d9e7fbd532eecc1d7880e2ca0b3216128be28b4a9f1d151fac97808b0bd98b7b43a612
a9ac865812bfeac6f47460277840b52a3b087f916ca7cedc0f768ea2bd19ea21155f84b4a04c4
000ad2ae0587154d560bc0a477a4f9329a8984dd31eb1f2a05e3d918701d630cfca9af61ef088
d2c5581acb463e439902e5d425719e956b8d6df7305b28e0ff27d3ad0de2085d292499b19a339
0d4396fb3bac9a8d8cbead2a7a4290fc9ac6fca045f98a614a45a39cbe24360f84d14f8e47271
2aceb74dbf45b53d49a0e4737e476ffc4d5b2f7cd247aa186d3b764ad9e9cfeee456a73c291d8
de3912414ac43911c372173ad7b472af35c6853ced2fe7b5fe0a89565ab33baa6f65cdd928319
d7065e040e7a5e84f9aa903f7648094bad07136b16927b8ec6dbc2bef0cc2856de1e795923e14
12c49f24deeb6c21f6c8a9765c9c7986e0da4b4c67d8e0d0c8d466824fb923d8573148990cd2e
f133c78ceecab72ed9dd285c5a3766852d54534207ffd34027f6c76ede8fd1a32d72c30048bba
a797d5df6fde27d087de5721ad7b7fa3e8d3f70d6bfc3ab2e252335368bbfa15acb5cb37d4694
e8b23cebe25de9c925a221a183b904d3f85df9929a919c54d6f87457373a0d6ecc1403e4cbbe6
20999435e80696634cd1a8e4747e9825bfa336e5bbad14f73640f1b9febe800dbaefe1630c61f
ae635b074c564eaa9db189c9e7302873fc64e6d497bc5c29080987a07a21d4af210703a4fa07f
2fd816f12fd1e29b4c0f44afe9bd4a1eaa8a7ae6f02a5b4258f52caf6127f62632a67cf4e8310
be56a7c28c86b2e277600c3e92c8d23d42586244c571e90568df202f2f6d81f860a565f9eb91a
3c78372e2a8b1be61c5418cf49bf2d6c8955d4a482a9919b7660b3f9a4404ffc454ea073e1e4b
2689ab2cca4e46bd7004a6c491fa26ee7a57d60f35edb2b821e6266442c8f335d452d524c772e
```

```
0353724c23c7dd15b7aa155e91442022140c5fcb0153147edcf3e8952f6f0399a3c88066a7275
6c9409915de63f64fa797841c57c796c6fc550ef745dfe9f179457f94755ae5a2506a764f327e
550be3dc14dd41f3b04b147d454938c63a8d69b2ea4c5710ec0b36e3a6c72571fa5d59dde036c
42033df35af056966ff0cd1204008971aa6ba9fb97b685ab9ffa2a9d1778104cd2c3b326de1fc
bc242e94d0311c3275b12850ed30ceead3a2ee6d060508411d4396f5421d8b6d067cf7cb5e826
785fbe119e05e21bd879b64f57cb0cd1972c2815f20abe7ce6ab34d0f471af44baad179e90644
122f5f33288e689ddddc5ce833e9755df1e73c65c5a201c4ede2ffa6b19274927719d2d38fdb7
a65aa43708b7fa9a94aa7d3210253d78d3b181e1020d0000bd0a1dc05d447f9f58ebeb84c65b3
6c8afcb83727a1508994e826957a663b0b9b8a003325ab6d6d6462ee4e106019c0dffe10323b7
bde7d82a38f85fd08786e860ba66c161b64b0708c363de5c6af62d8db3c243d1e1b712cb1d59e
942b9b6b4295a5a500b182cbd5fd1bc6ce9376d91b47a2284f1fbe0ad1c048cc2cfbb4afa3a9e
b9697503b69feca990eba7e9441af9ca44cb3ac6b5ed66e591c201fe30efa8a7c471dc613d625
4c263a8e132104bec47f1aacb3b2fcd4051b69b5e3fcb1c147a65c2f90c4b5188bafc521cab03
c12a309da50b5a7517727ed41228ed123fe1b152f6a6319cd623bf34ad7b8e064ab993260bcbd
405f5b7fff9b2fa40ba5ed5630242539e5d96823e89dc818a13d16675ee3079d976f694f5acc9
760ae789e9b3391b289e0e22a7ef17cc6a4577157b6d95c09baa4fd532e3ee0a290810ed35e56
bb19d9b61fb98a97c617425b06093d98a5cf0ee2dd127f0eea600b9a0c67fbe761db9b77e5d5b
ba9701da1b883e521a0cfe88451f57bd36085b67e56f061f84a2e6a152a71bce6e522daab6a0a
33ce22e537fa9793d28b617e6c0a4176a83aa3be578afac0f2f5547c5516d218984755b7445c7
143afa4e551fce0071bdb873b34e6b9e2b9e79ed0c69d288ed6421f237e860a0c6492ebbdd2a4
4c2c4f368dbe99941b1e8561d859d3859f496cee3d741f252973f8fcc539c409e35cc80a5ed6d
f23cc3a65601313f5d681fd9540c5291a9e30a72e38c96413c47c61ff84fde78d011b01b4154d
1b920af003f7abb1e1999dea6a766cf9fd2702b3ce0ee57af931b62124b0861b163a3b91aa4be
a28076c3432df3b29b6c4e1ba588def420071fc157de90eb2722ecc9ab00df3c669383a61a91b
b67bd287ce349b4745ee7a479dbceef166b9acc412eb579fcd6437307edda253d606b7be7599c
38092bc52a8598480edab8b82b1d21c565d2137ceae0b6642619b16133d91205d6355029e9cdf
eb9a28b373d95916b6b707d4c712c09cf36daf1a511b2bedb1aa70ee58d46a0666bb287784b0a
3840c589a7a04d5d6f2216be90aa4a512d5632f5c9bfe7b8b13382f999b95d367c7c46b968074
ce315197a5ff3545c7b77a804ade56a95b5c24cdece5937b5c0366d93ad03da9bc5db1b551dfb
91e9b343d2b57b763439686d4a3', -2:
h'0000000000000000000000000000000000000000000000000000000000000000'}",
  "sign1":
"d2845827a201383104582 0d9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd56524
7a166cb4faa0581d68656c6c6f20706f7374207175616e74756d207369676e617475726573591
213e132b492fc022d5fd1d2205f52dbf1ad1aaef3ece4622b4e3875696d64d66dccc74df743c1
b85552a0f3c1bdaaa8f789a15fdb3ce6329021f5815316cda1da5b012f1ccea4a47ef7e93eff3
19048ac9e3b6ed46cd58c6557af1b340da3bd7966f1588f8bd88e05383aee12a7248db3aec96b
a5d9afd1d79d62865eee04cac9cc2176ae585ae914d614805d916c142b4969be7ad95a44bf9c1
54d19bd41d8a3882ad6f0b0802d1e037c7579453a0606bbbb31db164fc607646477572c63b717
20f8d47bbb7615dd264f5829f726e22740cb3a1e1b5e381c4f692f7ecaa0979ae17aea3139d73
3491fe213eeddcd5f68e06ee71b80f14ed693f407ce6e199cb3edb048d3e2905ce75b31bd6837
a1d4b5eefa35431d0ca407200e60768b2dc5b0370e91a6c03c3d0e5c47225616034f55fb0a30a
66fd2074847be3c1230b93650d119492efc20338af0c4cb6a176191d7c5bbc7427f6f0c9bb49a
0d73e7f026cf3855547fc7ca9369733313963ffe4647e155a93cfa5403edebfc7842e75dad9ae
2accba720487e476ffe3bc0a60cf32271429242023d0d0a8f6e4e77a874afd2074a11ff20bae2
8d00fd5d990f839ca99c6db28a55da94a785290a6b536893a237224639717ba5cf833d57db2cc
a0a7aeeed874597c6ee71e0dc35e06851e9d2bd022c37b5fbcd2a4d5e8daea98a44cb9c97df43
a0aa512005358c8d5d5db88fba610e47d5a863f53f9ec7a8f3cb0b0ec2f02b1dfe9867a1437e8
4e941392b149275e868b959c58b9e814fb618c61208cb683881247bb0dcab96e84a77e0195b4e
93f693c1e98dcb99e495632f6cd5839d3bcccdfa2bf6b26921759d0a293595a96e6ddd42c83d8
d9a7b10a001b34f47c20fd46d1e09100e532e5b1900b89f14400bbcdd5ee0cf61a1ca353398a4
98da488b0f117effcf999f5aafe4a587deaa3ff78cc431637adcbb4e40ec385fac23e8176b74e
0e750460f7d2002bf7465944caa2708835d3849199732090b7c514575311ef9999c9bfcf737a4
d906af914d0507f5a7c2e61ff12359999d173f88db9ef85a6d71ac2e3a8074bed9472e00aedac
26c48ab9c2d1ad96eeffe6e200686efa17086317a541ffad5c8b5707279aecb12ca48f7e7d755
e8cdc2bc990c6391abf9351c2f5305bda2c57bf54e419dce477947a64de07eb0432e5f1cc8723
4ed673fa810d562095d0d0eed260bef5fc3daed8506756acb9059257b025471d8df2d4e697a3e
7c74c47081b569519e1de636a971668a376b4d84d95c30a554894475be8f01bda7c6d78989572
```

```
aea4c4e976a408b4a04b406e79e176163dcc1ffa7a7e9bd6ef6f854128097aa760ed3d6ad279f
7ea4ad6003f43cfb75de79c0bf8113a6f788e35e92f30185695f4abb18e924b29abf218e70897
7cb2776a7abf46a41e46afe24863eed4fe890916f95d5b1fbe6cea096ceb4ad478fc994214f59
c5e68c8b9695c27f8fada32c90ed324925540912da750451f033359177579e4e4a04e5d5b9bfa
72616df63df20f17038e7d4bbe61562583046c35e3a71a0f596f119ef183786ed76e1da6d3be9
8277db1583c8f2c8784c08f5c098abfd31baa9fc6abdc0cc441b6f93961b6630c45b9e7dda60d
88be7c9577b6fbc5edf65de4ed0b53f4377ce83b1e55c4d62015569b96ea094644e0f9cbe89cf
f4c539f77c629a5101c259c56cb9d31e20160dfe28386b37e610c2db9ecf6a000bfb2a85756e5
85ae6b97915e5113970946df068e6da7f0af0a48802b9e0464bfac7e0c6b7dee953665061ac74
86d9eee3bf21137383e97eb393a708e91a94f5012fa1d072c04f5c5ca2bbf894e7b275805fe5d
81341d75b9f7fcb89b3ff7da2b623c35d717d0da7180e258384ff39a914c2f30f893af4e1520d
64a15bb0997b852f3ec6ca398d245361fc2297c83867f388c8aa35e704d3f7081a961c528751f
aa64fd7efbcc03bed69e99ae1517d499117227cb08254d7b8aa079530af39fb19b246d45a4d41
a9955095636c786dcc3c30c817ee3c8e60689fd9a494c9e774463df7b884a78dfe80f1e247b3f
122401b0834e54fdeb57d7835f0409126983e40d8922bbd54981e2b651cc3fdee9193468c0412
01c2c4727493002506282250 52f935d37ab9dd8e466b6a3acb63ee93023013443ddeb91347b84
eb6ecf37423996d682967a5aab7ccaaa73a690a9cbd45b15ee38f2ae698aac3cb2117ecc91608
70993a3e50ea7647b0c03cb5f6daa290492dd693a0b8a9a9759d0d977b662d45c4af5dce95084
062f7a0f39d0bc3bdabaa31d8f815047244303e6a6e5d977ec757a56797f0630ef1d4f02f7a0e
7680c0865c4404c97bbf7014bfa64d0f89b02a2b981f616c0e16090c4b7fe9998a0232469b0c0
59d3daff58af6148cee567e52f1a41730b28d6af79358ad3679cf4c3dec0df780eccc91d004a4
ec0a4d20cc6771dbb3f42da69dc2140994c228a60adc0e97438a2332db657e91e5b7f5029541d
13ce8456d93bb4933522c94e16ee4766af28b5754b5a74c71efb6ff445dc1aed5f3e21cfe512c
f9862489582925c763251376279f69e633a43aaadcf4c104744cfca747f477c1af8c18f65109b
06680cd392d14e3e0ed0ba117643c8794bc8d036e85222d543063a01f91cb9bceb80d884b1305
d0065ef3555d6f64be4893816e0e9be111c65c9cb1840774ddd4ed5906ae2a73c7ca6103ecd3b
b506747681e192dd6c259b66dc63c39dbdc33dac1d564b54db4d8de935370abca642e05c6e95e
e827fb71d6086691bc6d1be2a0c7e491ce22163d3e8d48541cd7aca76eecc93f4e02ac0179cf7
073d5000b3ff338d096bc87eada3f4019fdf1a5d12470a33f65c2990c217680710069de75e033
8d1e26c179b1cf9ef853edaaab2c0519026b3d9f574b82b5bd316686b26c9e9e87870041fdfa1
a5c538cb98cb39200856b4c9bdacaa1c7717a22b883c06ca0f78229cd59362614361cc5ec76d8
36d2dafc1ed51066afa7297db869508cc80543b1efcddc62eb7c4ffabe3fafbc02f4802b4992f
f0be194ae123880ceee6187e08c7db96b22438ac4bdabadd8aba7af68b8e2ac0c60c0f9aad5e4
e1bf886db18212e9cb46d8bc201e4a1a6fb231d91a309dbca30b6b1269ec31bda1bb6b6d8ff41
d84baf7db7ac30de5ad5d9259398bbfb5ffbb89cce88a15f0f7413c9c71487b56eea23573697a
583fa57d3537588ba5558363d8abd679f2968dbca3ff00b141d68d5baed53fa66480029f46f6b
195e3dc99a0e09f990841c62735db8e4b6b867ee416cd946b65fae48acd2c580c5ee461fdc78c
2d671abb657f9296f976cb74c0249676a111e7608785ede2acde6f8af297f88ce9ad0e6b4cfda
c1c586519042ac700a4178f5c23add6634c26588f47bfb7ec9e244ae8c71382042c24606410ef
598ccfcaa459923e748d608caf3c82dd141c8eb32a500a03bb7fbd5d628b625fecd3d9399254d
7c569ab1418c6af0db64009f09d457e287b0e8b83bf40d529379464df999d7519a454bb3fa968
4f398c965c4f980061d33fd8883c5ad2964806f27fdfb09458b1bb2daaced0fbc0c68d46d6222
4f63725932b58ae0a694ec7fa0d4e5fcdc75840b467e12514f1cd006befcf3410cf7a5c81adf3
d29cd93ef5680c1a953daa0645273d0f5fdc8e6e0f8c632b67a674fb4f390c392720ec6d8e3f1
234e84f8420b91217ad71f406b1a4c7f2c438fff7844a097cdfb00a2f1a94ee6bdd597756a754
681111d66040c13a661b978440b05ba8c16e2a4255ebff56e5adada6fb92292d501d30e351f4f
b5b907d9f1510e9801489da0a3cf4997eed6df4fb06b86f81af3735781513c6654e030a03e358
970fa129fdb8cb49365a86f1cdd1a9b5f966794c8bca163c3af148406c24f0e149da338e6a1fb
5f365b1a6bf0fe426ec424823588dce11dfe7de3b3aa740d27fac9b6d9c60909b4afe2f88dde8
58069e330e6f9a7ecc779022d3925ea0bd73e67041945e04691152683453f3126cb3699b607dd
598af05fd441c157bb3b8d69243705cd1e71442b502b7ea987c8837a3bd896e5bf2796052a23d
302c70b23a62383278e1f3c878c2bdcb68524c078fc73148f227951566c19248240d972d55473
50909c63d6f505ad889884fe9710154d2ec05aa15a4f734e5b88480916ec73e1518fbd2605954
580ec2b0a8f9c4bd4d075461b6b3015c344e83382c36b161e57a6c3933e98209ce308190531f8
5f5d5fd9451d37f40f6f36af830b376ed2d48ab20b2b58b7c6e5956b7d4142b19ccb19a88db70
e5829047751950e2975bb4d0e9991fc3bbc4fa5adf2d9d1e25e4ded5396731bd2808b8227a302
33cc7a1ab7759623357547e46060a4c6c54a8d2416680186ca97291afd2be4ffdc9bea1c4b81
ad80a3e7be17fb5585eeb72dfc030655040993fe12f58d21d3ea499c1ecac70725f2e133450e9
```

```
c1e75ce657300f85ae0f44e470336dbd5df32fbc0a8ffbe3c66058e45ac5fb0ea3889313214b6
b2ec98a91e6414b3dda04d9c41857707bbdcf4763ee3846c7f4df034e1dc8fefc8a2a5dcda9f9
1940cdcd1f7b98b93c08bc9f1c198e80fcde8a5effe4ea4363a56cae57de4a7248fd8bde5767f
1ae699b5bd998d9f613306346472e96954dc32baccd31c3f44b0f11b8e6810bb3f27af7de6a57
550288f56015b1b76f1c1e492d5b998493b72a38ba4f2619b891aeccfd96c27fe80b958e08728
581ca4d6e7da5f2760b48734a049e8fb29aa6ff373911d712091ef6bbed204da3b1237c119565
4c7f66aa6776e950e7a27aed6c9a4ffebe76671ff1dea7b1ee5d0434c976d2d23bb481b6d80d2
42a2c942329dbe051396d0a9add08068634f6c7f8aadfd55e4109cde60f693229f605d71f896f
5e1c9d3b94fb9a497a9b955960307811296f2ed263ad57780c6f2f96b42eb71e817bbed065400
0c6bc20d3087f7971b8d517c00cdf9732294285c6faa24b405e3b31e6fb856b57aabae81e72a8
876f06cc0fbda5ca4479a5cecdee7b5bd0fff8f8c788e2d803dad28ca110f6013672323540b94
eb5a7638116cfec790f2d899d7f6bc075cbb78ad925845bc75b8086078356b0c6dc722283e774
cb7a5ee24a6b976ca6dcc40fef3ea10e77cc50a0523ab4df32971a19c9c6e889edb99ea9d863e
7f9922d02303b80a29899397f4abacc5ecf6da98574e2ee2afcd18077063d7419e4ee36189108
5217c905f6cefb2041ee6f49df051511152f45609a0d06d951b0351431651bde5b5434c06b146
509727cd5b76f182c1353ee94e6ef98901cdba4b6cfc1dda01628ff86b21e2be53da4a8c2c9fc
1b50b28ada2836959ed1398c70018b5f3c35d9f3c8768af0966a0e8ee6b16dd17455acecd377f
d259379e7e22f187876db740c3c09a0307891484f9b12da66916d9d4018ac34b9d70a094a655e
ce0282839a9e60b8cea041316803b262a4928d375889017f3da58b9721ac9d7a4e69b06fb26d4
6a904b062728286ee2e44c18354be39252482e5135fbfd1ea4f85dfc96b63e0fc8815a3a0f1be
7476e60712a566911663159e74838f27a0068b2131aec8653b5f697ede4dd8c769234ba5d018e
de320aeace49e263844b93d3c2410af9c5df83c0e7eb617930eea8a272e16a6d58e6ce1ce9a3b
42ad94436abe73e01b95839038d5430676ef6a7a3c77cd541fe860d40bd9414133a8983280e13
9161d85dc0c395eac1ffc6fe52d637fd5f327d112f8ed15172925b0a21334d8b5dbeaea1bdbfc
f9bcb8c9bd72b58aa6745f07fae50343191f90983e4d138a278f46433a8c404565c4d15a55c4d
61f396444b639bf7191515c558155bf2a09576e7b3376236a23baeb2f7826e1b5e95e100bae7d
0b9226864839d04f2145cf0a0c0dbb0194f2224aa63cb144a0038cd63ac6b42bd9c74e7d1eff9
cc1419043a8bbec602e5665d45ddfa09c1831c0c04fa116ff8ad7fd93a0d005dedb329407c84b
809d4552c6e31174ca01f7fe336dd1759b3d4bafdcf5df63f5bca512caf29a4e645e5315c0777
478f1640afa2d30f2e8f5293571d3b94f65be0cc98f24261633ae9b0a44e6048c35ce44eca75d
6362ce6b5698806addecf26d1928a2ac14939923ca63d54afa103e7a1c8f23fa9880e381d17ee
89b4e65922ebe81d58b3dfe637f554f0dbb499073cb4ca9c2ee30a6bd0c5fc56675e0215a8b45
77dd6c1490087bf4b2039b5b52ad49c08212a8171d0cb6fb4f84855cf426d36147f5e46fd3f77
22481ce26b0511d6603087fbb9d1382a69011de7aedadd0d29b7c0ffeae5640c8079acf8818de
222664728df79967e54962537fa06bde323de630bf63ae92e57e33f242fd508e767da3f2dfa14
c0726b12bce09c4310502807ef00b88afbe76ff01a941ce512504c25d552e8863afa3c89bdb53
d757d09161a5e65b4c1d6f4fe00879d1e247d8a93f30b252d5d6d7308676a76c4d9ee11131b2c
2f7f8092b0d2e417225f6d7c82a4eff0f7204765a4bcd2dafd0000000000000000000000000000
00a0d1319202b353d",
  "sign1_diag":
"18([h'a2013831045820d9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd565247a
166cb4fa', {},
h'68656c6c6f20706f7374207175616e74756d207369676e617475726573',
h'e132b492fc022d5fd1d2205f52dbf1ad1aaef3ece4622b4e3875696d64d66dccc74df743c1b
85552a0f3c1bdaaa8f789a15fdb3ce6329021f5815316cda1da5b012f1ccea4a47ef7e93eff31
9048ac9e3b6ed46cd58c6557af1b340da3bd7966f1588f8bd88e05383aee12a7248db3aec96ba
5d9afd1d79d62865eee04cac9cc2176ae585ae914d614805d916c142b4969be7ad95a44bf9c15
4d19bd41d8a3882ad6f0b0802d1e037c7579453a0606bbbb31db164fc607646477572c63b7172
0f8d47bbb7615dd264f5829f726e22740cb3a1e1b5e381c4f692f7ecaa0979ae17aea3139d733
491fe213eeddcd5f68e06ee71b80f14ed693f407ce6e199cb3edb048d3e2905ce75b31bd6837a
1d4b5eefa35431d0ca407200e60768b2dc5b0370e91a6c03c3d0e5c47225616034f55fb0a30a6
6fd2074847be3c1230b93650d119492efc20338af0c4cb6a176191d7c5bbc7427f6f0c9bb49a0
d73e7f026cf3855547fc7ca9369733313963ffe4647e155a93cfa5403edebfc7842e75dad9ae2
accba720487e476ffe3bc0a60cf32271429242023d0d0a8f6e4e77a874afd2074a11ff20bae28
d00fd5d990f839ca99c6db28a55da94a785290a6b536893a237224639717ba5cf833d57db2cca
0a7aeeed874597c6ee71e0dc35e06851e9d2bd022c37b5fbcd2a4d5e8daea98a44cb9c97df43a
0aa512005358c8d5d5db88fba610e47d5a863f53f9ec7a8f3cb0b0ec2f02b1dfe9867a1437e84
e941392b149275e868b959c58b9e814fb618c61208cb683881247bb0dcab96e84a77e0195b4e9
```

```
3f693c1e98dcb99e495632f6cd5839d3bcccdfa2bf6b26921759d0a293595a96e6ddd42c83d8d
9a7b10a001b34f47c20fd46d1e09100e532e5b1900b89f14400bbcdd5ee0cf61a1ca353398a49
8da488b0f117effcf999f5aafe4a587deaa3ff78cc431637adcbb4e40ec385fac23e8176b74e0
e750460f7d2002bf7465944caa2708835d3849199732090b7c514575311ef9999c9bfcf737a4d
906af914d0507f5a7c2e61ff12359999d173f88db9ef85a6d71ac2e3a8074bed9472e00aedac2
6c48ab9c2d1ad96eeffe6e200686efa17086317a541ffad5c8b5707279aecb12ca48f7e7d755e
8cdc2bc990c6391abf9351c2f5305bda2c57bf54e419dce477947a64de07eb0432e5f1cc87234
ed673fa810d562095d0d0eed260bef5fc3daed8506756acb9059257b025471d8df2d4e697a3e7
c74c47081b569519e1de636a971668a376b4d84d95c30a554894475be8f01bda7c6d78989572a
ea4c4e976a408b4a04b406e79e176163dcc1ffa7a7e9bd6ef6f854128097aa760ed3d6ad279f7
ea4ad6003f43cfb75de79c0bf8113a6f788e35e92f30185695f4abb18e924b29abf218e708977
cb2776a7abf46a41e46afe24863eed4fe890916f95d5b1fbe6cea096ceb4ad478fc994214f59c
5e68c8b9695c27f8fada32c90ed324925540912da750451f033359177579e4e4a04e5d5b9bfa7
2616df63df20f17038e7d4bbe61562583046c35e3a71a0f596f119ef183786ed76e1da6d3be98
277db1583c8f2c8784c08f5c098abfd31baa9fc6abdc0cc441b6f93961b6630c45b9e7dda60d8
8be7c9577b6fbc5edf65de4ed0b53f4377ce83b1e55c4d62015569b96ea094644e0f9cbe89cff
4c539f77c629a5101c259c56cb9d31e20160dfe28386b37e610c2db9ecf6a000bfb2a85756e58
5ae6b97915e5113970946df068e6da7f0af0a48802b9e0464bfac7e0c6b7dee953665061ac748
6d9eee3bf21137383e97eb393a708e91a94f5012fa1d072c04f5c5ca2bbf894e7b275805fe5d8
1341d75b9f7fcb89b3ff7da2b623c35d717d0da7180e258384ff39a914c2f30f893af4e1520d6
4a15bb0997b852f3ec6ca398d245361fc2297c83867f388c8aa35e704d3f7081a961c528751fa
a64fd7efbcc03bed69e99ae1517d499117227cb08254d7b8aa079530af39fb19b246d45a4d41a
9955095636c786dcc3c30c817ee3c8e60689fd9a494c9e774463df7b884a78dfe80f1e247b3f1
22401b0834e54fdeb57d7835f0409126983e40d8922bbd54981e2b651cc3fdee9193468c04120
1c2c4727493002506282250 52f935d37ab9dd8e466b6a3acb63ee93023013443ddeb91347b84e
b6ecf37423996d682967a5aab7ccaaa73a690a9cbd45b15ee38f2ae698aac3cb2117ecc916087
0993a3e50ea7647b0c03cb5f6daa290492dd693a0b8a9a9759d0d977b662d45c4af5dce950840
62f7a0f39d0bc3bdabaa31d8f815047244303e6a6e5d977ec757a56797f0630ef1d4f02f7a0e7
680c0865c4404c97bbf7014bfa64d0f89b02a2b981f616c0e16090c4b7fe9998a0232469b0c05
9d3daff58af6148cee567e52f1a41730b28d6af79358ad3679cf4c3dec0df780eccc91d004a4e
c0a4d20cc6771dbb3f42da69dc2140994c228a60adc0e97438a2332db657e91e5b7f5029541d1
3ce8456d93bb4933522c94e16ee4766af28b5754b5a74c71efb6ff445dc1aed5f3e21cfe512cf
9862489582925c763251376279f69e633a43aaadcf4c104744cfca747f477c1af8c18f65109b0
6680cd392d14e3e0ed0ba117643c8794bc8d036e85222d543063a01f91cb9bceb80d884b1305d
0065ef3555d6f64be4893816e0e9be111c65c9cb1840774ddd4ed5906ae2a73c7ca6103ecd3bb
506747681e192dd6c259b66dc63c39dbdc33dac1d564b54db4d8de935370abca642e05c6e95ee
827fb71d6086691bc6d1be2a0c7e491ce22163d3e8d48541cd7aca76eecc93f4e02ac0179cf70
73d5000b3ff338d096bc87eada3f4019fdf1a5d12470a33f65c2990c217680710069de75e0338
d1e26c179b1cf9ef853edaaab2c0519026b3d9f574b82b5bd316686b26c9e9e87870041fdfa1a
5c538cb98cb39200856b4c9bdacaa1c7717a22b883c06ca0f78229cd59362614361cc5ec76d83
6d2dafc1ed51066afa7297db869508cc80543b1efcddc62eb7c4ffabe3fafbc02f4802b4992ff
0be194ae123880ceee6187e08c7db96b22438ac4bdabadd8aba7af68b8e2ac0c60c0f9aad5e4e
1bf886db18212e9cb46d8bc201e4a1a6fb231d91a309dbca30b6b1269ec31bda1bb6b6d8ff41d
84baf7db7ac30de5ad5d9259398bbfb5ffbb89cce88a15f0f7413c9c71487b56eea23573697a5
83fa57d3537588ba5558363d8abd679f2968dbca3ff00b141d68d5baed53fa66480029f46f6b1
95e3dc99a0e09f990841c62735db8e4b6b867ee416cd946b65fae48acd2c580c5ee461fdc78c2
d671abb657f9296f976cb74c0249676a111e7608785ede2acde6f8af297f88ce9ad0e6b4cfdac
1c586519042ac700a4178f5c23add6634c26588f47bfb7ec9e244ae8c71382042c24606410ef5
98ccfcaa459923e748d608caf3c82dd141c8eb32a500a03bb7fbd5d628b625fecd3d9399254d7
c569ab1418c6af0db64009f09d457e287b0e8b83bf40d529379464df999d7519a454bb3fa9684
f398c965c4f980061d33fd8883c5ad2964806f27fdfb09458b1bb2daaced0fbc0c68d46d62224
f63725932b58ae0a694ec7fa0d4e5fcdc75840b467e12514f1cd006befcf3410cf7a5c81adf3d
29cd93ef5680c1a953daa0645273d0f5fdc8e6e0f8c632b67a674fb4f390c392720ec6d8e3f12
34e84f8420b91217ad71f406b1a4c7f2c438fff7844a097cdfb00a2f1a94ee6bdd597756a7546
81111d66040c13a661b978440b05ba8c16e2a4255ebff56e5adada6fb92292d501d30e351f4fb
5b907d9f1510e9801489da0a3cf4997eed6df4fb06b86f81af3735781513c6654e030a03e3589
70fa129fdb8cb49365a86f1cdd1a9b5f966794c8bca163c3af148406c24f0e149da338e6a1fb5
f365b1a6bf0fe426ec424823588dce11dfe7de3b3aa740d27fac9b6d9c60909b4afe2f88dde85
```

```
8069e330e6f9a7ecc779022d3925ea0bd73e67041945e04691152683453f3126cb3699b607dd5
98af05fd441c157bb3b8d69243705cd1e71442b502b7ea987c8837a3bd896e5bf2796052a23d3
02c70b23a62383278e1f3c878c2bdcb68524c078fc73148f227951566c19248240d972d554735
0909c63d6f505ad889884fe9710154d2ec05aa15a4f734e5b88480916ec73e1518fbd26059545
80ec2b0a8f9c4bd4d075461b6b3015c344e83382c36b161e57a6c3933e98209ce308190531f85
f5d5fd9451d37f40f6f36af830b376ed2d48ab20b2b58b7c6e5956b7d4142b19ccb19a88db70e
5829047751950e2975bb4d0e9991fc3bbc4fa5adf2d9d1e25e4ded5396731bd2808b8227a3023
3cc7a1ab7759623357547e46060a4c6c54a8d2411680186ca97291afd2be4ffdc9bea1c4b81a
d80a3e7be17fb5585eeb72dfc030655040993fe12f58d21d3ea499c1ecac70725f2e133450e9c
1e75ce657300f85ae0f44e470336dbd5df32fbc0a8ffbe3c66058e45ac5fb0ea3889313214b6b
2ec98a91e6414b3dda04d9c41857707bbdcf4763ee3846c7f4df034e1dc8fefc8a2a5dcda9f91
940cdcd1f7b98b93c08bc9f1c198e80fcde8a5effe4ea4363a56cae57de4a7248fd8bde5767f1
ae699b5bd998d9f613306346472e96954dc32baccd31c3f44b0f11b8e6810bb3f27af7de6a575
50288f56015b1b76f1c1e492d5b998493b72a38ba4f2619b891aeccfd96c27fe80b958e087285
81ca4d6e7da5f2760b48734a049e8fb29aa6ff373911d712091ef6bbed204da3b1237c1195654
c7f66aa6776e950e7a27aed6c9a4ffebe76671ff1dea7b1ee5d0434c976d2d23bb481b6d80d24
2a2c942329dbe051396d0a9add08068634f6c7f8aadfd55e4109cde60f693229f605d71f896f5
e1c9d3b94fb9a497a9b955960307811296f2ed263ad57780c6f2f96b42eb71e817bbed0654000
c6bc20d3087f7971b8d517c00cdf9732294285c6faa24b405e3b31e6fb856b57aabae81e72a88
76f06cc0fbda5ca4479a5cecdee7b5bd0fff8f8c788e2d803dad28ca110f6013672323540b94e
b5a7638116cfec790f2d899d7f6bc075cbb78ad925845bc75b8086078356b0c6dc722283e774c
b7a5ee24a6b976ca6dcc40fef3ea10e77cc50a0523ab4df32971a19c9c6e889edb99ea9d863e7
f9922d02303b80a29899397f4abacc5ecf6da98574e2ee2afcd18077063d7419e4ee361891085
217c905f6cefb2041ee6f49df051511152f45609a0d06d951b0351431651bde5b5434c06b1465
09727cd5b76f182c1353ee94e6ef98901cdba4b6cfc1dda01628ff86b21e2be53da4a8c2c9fc1
b50b28ada2836959ed1398c70018b5f3c35d9f3c8768af0966a0e8ee6b16dd17455acecd377fd
259379e7e22f187876db740c3c09a0307891484f9b12da66916d9d4018ac34b9d70a094a655ec
e0282839a9e60b8cea041316803b262a4928d375889017f3da58b9721ac9d7a4e69b06fb26d46
a904b062728286ee2e44c18354be39252482e5135fbfd1ea4f85dfc96b63e0fc8815a3a0f1be7
476e60712a566911663159e74838f27a0068b2131aec8653b5f697ede4dd8c769234ba5d018ed
e320aeace49e263844b93d3c2410af9c5df83c0e7eb617930eea8a272e16a6d58e6ce1ce9a3b4
2ad94436abe73e01b95839038d5430676ef6a7a3c77cd541fe860d40bd9414133a8983280e139
161d85dc0c395eac1ffc6fe52d637fd5f327d112f8ed15172925b0a21334d8b5dbeaea1bdbfcf
9bcb8c9bd72b58aa6745f07fae50343191f90983e4d138a278f46433a8c404565c4d15a55c4d6
1f396444b639bf7191515c558155bf2a09576e7b3376236a23baeb2f7826e1b5e95e100bae7d0
b9226864839d04f2145cf0a0c0dbb0194f2224aa63cb144a0038cd63ac6b42bd9c74e7d1eff9c
c1419043a8bbec602e5665d45ddfa09c1831c0c04fa116ff8ad7fd93a0d005dedb329407c84b8
09d4552c6e31174ca01f7fe336dd1759b3d4bafdcf5df63f5bca512caf29a4e645e5315c07774
78f1640afa2d30f2e8f5293571d3b94f65be0cc98f24261633ae9b0a44e6048c35ce44eca75d6
362ce6b5698806addecf26d1928a2ac14939923ca63d54afa103e7a1c8f23fa9880e381d17ee8
9b4e65922ebe81d58b3dfe637f554f0dbb499073cb4ca9c2ee30a6bd0c5fc56675e0215a8b457
7dd6c1490087bf4b2039b5b52ad49c08212a8171d0cb6fb4f84855cf426d36147f5e46fd3f772
2481ce26b0511d6603087fbb9d1382a69011de7aedadd0d29b7c0ffeae5640c8079acf8818de2
22664728df79967e54962537fa06bde323de630bf63ae92e57e33f242fd508e767da3f2dfa14c
0726b12bce09c4310502807ef00b88afbe76ff01a941ce512504c25d552e8863afa3c89bdb53d
757d09161a5e65b4c1d6f4fe00879d1e247d8a93f30b252d5d6d7308676a76c4d9ee11131b2c2
f7f8092b0d2e417225f6d7c82a4eff0f7204765a4bcd2dafd00000000000000000000000000000
0a0d1319202b353d'])",
  "raw_to_be_signed":
"846a5369676e6174757265315827a2013831045820d9bc439f97bd6d4093e68f0f3fcf09c9a9
7adf888ed7308dd565247a166cb4fa40581d68656c6c6f20706f7374207175616e74756d20736
9676e617475726573",
  "raw_signature":
"e132b492fc022d5fd1d2205f52dbf1ad1aaef3ece4622b4e3875696d64d66dccc74df743c1b8
5552a0f3c1bdaaa8f789a15fdb3ce6329021f5815316cda1da5b012f1ccea4a47ef7e93eff319
048ac9e3b6ed46cd58c6557af1b340da3bd7966f1588f8bd88e05383aee12a7248db3aec96ba5
d9afd1d79d62865eee04cac9cc2176ae585ae914d614805d916c142b4969be7ad95a44bf9c154
d19bd41d8a3882ad6f0b0802d1e037c7579453a0606bbbb31db164fc607646477572c63b71720
```

```
f8d47bbb7615dd264f5829f726e22740cb3a1e1b5e381c4f692f7ecaa0979ae17aea3139d7334
91fe213eeddcd5f68e06ee71b80f14ed693f407ce6e199cb3edb048d3e2905ce75b31bd6837a1
d4b5eefa35431d0ca407200e60768b2dc5b0370e91a6c03c3d0e5c47225616034f55fb0a30a66
fd2074847be3c1230b93650d119492efc20338af0c4cb6a176191d7c5bbc7427f6f0c9bb49a0d
73e7f026cf3855547fc7ca9369733313963ffe4647e155a93cfa5403edebfc7842e75dad9ae2a
ccba720487e476ffe3bc0a60cf32271429242023d0d0a8f6e4e77a874afd2074a11ff20bae28d
00fd5d990f839ca99c6db28a55da94a785290a6b536893a237224639717ba5cf833d57db2cca0
a7aeeed874597c6ee71e0dc35e06851e9d2bd022c37b5fbcd2a4d5e8daea98a44cb9c97df43a0
aa512005358c8d5d5db88fba610e47d5a863f53f9ec7a8f3cb0b0ec2f02b1dfe9867a1437e84e
941392b149275e868b959c58b9e814fb618c61208cb683881247bb0dcab96e84a77e0195b4e93
f693c1e98dcb99e495632f6cd5839d3bcccdfa2bf6b26921759d0a293595a96e6ddd42c83d8d9
a7b10a001b34f47c20fd46d1e09100e532e5b1900b89f14400bbcdd5ee0cf61a1ca353398a498
da488b0f117effcf999f5aafe4a587deaa3ff78cc431637adcbb4e40ec385fac23e8176b74e0e
750460f7d2002bf7465944caa2708835d3849199732090b7c514575311ef9999c9bfcf737a4d9
06af914d0507f5a7c2e61ff12359999d173f88db9ef85a6d71ac2e3a8074bed9472e00aedac26
c48ab9c2d1ad96eeffe6e200686efa17086317a541ffad5c8b5707279aecb12ca48f7e7d755e8
cdc2bc990c6391abf9351c2f5305bda2c57bf54e419dce477947a64de07eb0432e5f1cc87234e
d673fa810d562095d0d0eed260bef5fc3daed8506756acb9059257b025471d8df2d4e697a3e7c
74c47081b569519e1de636a971668a376b4d84d95c30a554894475be8f01bda7c6d78989572ae
a4c4e976a408b4a04b406e79e176163dcc1ffa7a7e9bd6ef6f854128097aa760ed3d6ad279f7e
a4ad6003f43cfb75de79c0bf8113a6f788e35e92f30185695f4abb18e924b29abf218e708977c
b2776a7abf46a41e46afe24863eed4fe890916f95d5b1fbe6cea096ceb4ad478fc994214f59c5
e68c8b9695c27f8fada32c90ed324925540912da750451f033359177579e4e4a04e5d5b9bfa72
616df63df20f17038e7d4bbe61562583046c35e3a71a0f596f119ef183786ed76e1da6d3be982
77db1583c8f2c8784c08f5c098abfd31baa9fc6abdc0cc441b6f93961b6630c45b9e7dda60d88
be7c9577b6fbc5edf65de4ed0b53f4377ce83b1e55c4d62015569b96ea094644e0f9cbe89cff4
c539f77c629a5101c259c56cb9d31e20160dfe28386b37e610c2db9ecf6a000bfb2a85756e585
ae6b97915e5113970946df068e6da7f0af0a48802b9e0464bfac7e0c6b7dee953665061ac7486
d9eee3bf21137383e97eb393a708e91a94f5012fa1d072c04f5c5ca2bbf894e7b275805fe5d81
341d75b9f7fcb89b3ff7da2b623c35d717d0da7180e258384ff39a914c2f30f893af4e1520d64
a15bb0997b852f3ec6ca398d245361fc2297c83867f388c8aa35e704d3f7081a961c528751faa
64fd7efbcc03bed69e99ae1517d499117227cb08254d7b8aa079530af39fb19b246d45a4d41a9
955095636c786dcc3c30c817ee3c8e60689fd9a494c9e774463df7b884a78dfe80f1e247b3f12
2401b0834e54fdeb57d7835f0409126983e40d8922bbd54981e2b651cc3fdee9193468c041201
c2c4727493002506282250 52f935d37ab9dd8e466b6a3acb63ee93023013443ddeb91347b84eb
6ecf37423996d682967a5aab7ccaaa73a690a9cbd45b15ee38f2ae698aac3cb2117ecc9160870
993a3e50ea7647b0c03cb5f6daa290492dd693a0b8a9a9759d0d977b662d45c4af5dce9508406
2f7a0f39d0bc3bdabaa31d8f815047244303e6a6e5d977ec757a56797f0630ef1d4f02f7a0e76
80c0865c4404c97bbf7014bfa64d0f89b02a2b981f616c0e16090c4b7fe9998a0232469b0c059
d3daff58af6148cee567e52f1a41730b28d6af79358ad3679cf4c3dec0df780eccc91d004a4ec
0a4d20cc6771dbb3f42da69dc2140994c228a60adc0e97438a2332db657e91e5b7f5029541d13
ce8456d93bb4933522c94e16ee4766af28b5754b5a74c71efb6ff445dc1aed5f3e21cfe512cf9
862489582925c763251376279f69e633a43aaadcf4c104744cfca747f477c1af8c18f65109b06
680cd392d14e3e0ed0ba117643c8794bc8d036e85222d543063a01f91cb9bceb80d884b1305d0
065ef3555d6f64be4893816e0e9be111c65c9cb1840774ddd4ed5906ae2a73c7ca6103ecd3bb5
06747681e192dd6c259b66dc63c39dbdc33dac1d564b54db4d8de935370abca642e05c6e95ee8
27fb71d6086691bc6d1be2a0c7e491ce22163d3e8d48541cd7aca76eecc93f4e02ac0179cf707
3d5000b3ff338d096bc87eada3f4019fdf1a5d12470a33f65c2990c217680710069de75e0338d
1e26c179b1cf9ef853edaaab2c0519026b3d9f574b82b5bd316686b26c9e9e87870041fdfa1a5
c538cb98cb39200856b4c9bdacaa1c7717a22b883c06ca0f78229cd59362614361cc5ec76d836
d2dafc1ed51066afa7297db869508cc80543b1efcddc62eb7c4ffabe3fafbc02f4802b4992ff0
be194ae123880ceee6187e08c7db96b22438ac4bdabadd8aba7af68b8e2ac0c60c0f9aad5e4e1
bf886db18212e9cb46d8bc201e4a1a6fb231d91a309dbca30b6b1269ec31bda1bb6b6d8ff41d8
4baf7db7ac30de5ad5d9259398bbfb5ffbb89cce88a15f0f7413c9c71487b56eea23573697a58
3fa57d3537588ba5558363d8abd679f2968dbca3ff00b141d68d5baed53fa66480029f46f6b19
5e3dc99a0e09f990841c62735db8e4b6b867ee416cd946b65fae48acd2c580c5ee461fdc78c2d
671abb657f9296f976cb74c0249676a111e7608785ede2acde6f8af297f88ce9ad0e6b4cfdac1
c586519042ac700a4178f5c23add6634c26588f47bfb7ec9e244ae8c71382042c24606410ef59
```

```
8ccfcaa459923e748d608caf3c82dd141c8eb32a500a03bb7fbd5d628b625fecd3d9399254d7c
569ab1418c6af0db64009f09d457e287b0e8b83bf40d529379464df999d7519a454bb3fa9684f
398c965c4f980061d33fd8883c5ad2964806f27fdfb09458b1bb2daaced0fbc0c68d46d62224f
63725932b58ae0a694ec7fa0d4e5fcdc75840b467e12514f1cd006befcf3410cf7a5c81adf3d2
9cd93ef5680c1a953daa0645273d0f5fdc8e6e0f8c632b67a674fb4f390c392720ec6d8e3f123
4e84f8420b91217ad71f406b1a4c7f2c438fff7844a097cdfb00a2f1a94ee6bdd597756a75468
1111d66040c13a661b978440b05ba8c16e2a4255ebff56e5adada6fb92292d501d30e351f4fb5
b907d9f1510e9801489da0a3cf4997eed6df4fb06b86f81af3735781513c6654e030a03e35897
0fa129fdb8cb49365a86f1cdd1a9b5f966794c8bca163c3af148406c24f0e149da338e6a1fb5f
365b1a6bf0fe426ec424823588dce11dfe7de3b3aa740d27fac9b6d9c60909b4afe2f88dde858
069e330e6f9a7ecc779022d3925ea0bd73e67041945e04691152683453f3126cb3699b607dd59
8af05fd441c157bb3b8d69243705cd1e71442b502b7ea987c8837a3bd896e5bf2796052a23d30
2c70b23a62383278e1f3c878c2bdcb68524c078fc73148f227951566c19248240d972d5547350
909c63d6f505ad889884fe9710154d2ec05aa15a4f734e5b88480916ec73e1518fbd260595458
0ec2b0a8f9c4bd4d075461b6b3015c344e83382c36b161e57a6c3933e98209ce308190531f85f
5d5fd9451d37f40f6f36af830b376ed2d48ab20b2b58b7c6e5956b7d4142b19ccb19a88db70e5
829047751950e2975bb4d0e9991fc3bbc4fa5adf2d9d1e25e4ded5396731bd2808b8227a30233
cc7a1ab7759623357547e46060a4c6c54a8d2411668018 6ca97291afd2be4ffdc9bea1c4b81ad
80a3e7be17fb5585eeb72dfc030655040993fe12f58d21d3ea499c1ecac70725f2e133450e9c1
e75ce657300f85ae0f44e470336dbd5df32fbc0a8ffbe3c66058e45ac5fb0ea3889313214b6b2
ec98a91e6414b3dda04d9c41857707bbdcf4763ee3846c7f4df034e1dc8fefc8a2a5dcda9f919
40cdcd1f7b98b93c08bc9f1c198e80fcde8a5effe4ea4363a56cae57de4a7248fd8bde5767f1a
e699b5bd998d9f613306346472e96954dc32baccd31c3f44b0f11b8e6810bb3f27af7de6a5755
0288f56015b1b76f1c1e492d5b998493b72a38ba4f2619b891aeccfd96c27fe80b958e0872858
1ca4d6e7da5f2760b48734a049e8fb29aa6ff373911d712091ef6bbed204da3b1237c1195654c
7f66aa6776e950e7a27aed6c9a4ffebe76671ff1dea7b1ee5d0434c976d2d23bb481b6d80d242
a2c942329dbe051396d0a9add08068634f6c7f8aadfd55e4109cde60f693229f605d71f896f5e
1c9d3b94fb9a497a9b955960307811296f2ed263ad57780c6f2f96b42eb71e817bbed0654000c
6bc20d3087f7971b8d517c00cdf9732294285c6faa24b405e3b31e6fb856b57aabae81e72a887
6f06cc0fbda5ca4479a5cecdee7b5bd0fff8f8c788e2d803dad28ca110f6013672323540b94eb
5a7638116cfec790f2d899d7f6bc075cbb78ad925845bc75b8086078356b0c6dc722283e774cb
7a5ee24a6b976ca6dcc40fef3ea10e77cc50a0523ab4df32971a19c9c6e889edb99ea9d863e7f
9922d02303b80a29899397f4abacc5ecf6da98574e2ee2afcd18077063d7419e4ee3618910852
17c905f6cefb2041ee6f49df051511152f45609a0d06d951b0351431651bde5b5434c06b14650
9727cd5b76f182c1353ee94e6ef98901cdba4b6cfc1dda01628ff86b21e2be53da4a8c2c9fc1b
50b28ada2836959ed1398c70018b5f3c35d9f3c8768af0966a0e8ee6b16dd17455acecd377fd2
59379e7e22f187876db740c3c09a0307891484f9b12da66916d9d4018ac34b9d70a094a655ece
0282839a9e60b8cea041316803b262a4928d375889017f3da58b9721ac9d7a4e69b06fb26d46a
904b062728286ee2e44c18354be39252482e5135fbfd1ea4f85dfc96b63e0fc8815a3a0f1be74
76e60712a566911663159e74838f27a0068b2131aec8653b5f697ede4dd8c769234ba5d018ede
320aeace49e263844b93d3c2410af9c5df83c0e7eb617930eea8a272e16a6d58e6ce1ce9a3b42
ad94436abe73e01b95839038d5430676ef6a7a3c77cd541fe860d40bd9414133a8983280e1391
61d85dc0c395eac1ffc6fe52d637fd5f327d112f8ed15172925b0a21334d8b5dbeaea1bdbfcf9
bcb8c9bd72b58aa6745f07fae50343191f90983e4d138a278f46433a8c404565c4d15a55c4d61
f396444b639bf7191515c558155bf2a09576e7b3376236a23baeb2f7826e1b5e95e100bae7d0b
9226864839d04f2145cf0a0c0dbb0194f2224aa63cb144a0038cd63ac6b42bd9c74e7d1eff9cc
1419043a8bbec602e5665d45ddfa09c1831c0c04fa116ff8ad7fd93a0d005dedb329407c84b80
9d4552c6e31174ca01f7fe336dd1759b3d4bafdcf5df63f5bca512caf29a4e645e5315c077747
8f1640afa2d30f2e8f5293571d3b94f65be0cc98f24261633ae9b0a44e6048c35ce44eca75d63
62ce6b5698806addecf26d1928a2ac14939923ca63d54afa103e7a1c8f23fa9880e381d17ee89
b4e65922ebe81d58b3dfe637f554f0dbb499073cb4ca9c2ee30a6bd0c5fc56675e0215a8b4577
dd6c1490087bf4b2039b5b52ad49c08212a8171d0cb6fb4f84855cf426d36147f5e46fd3f7722
481ce26b0511d6603087fbb9d1382a69011de7aedadd0d29b7c0ffeae5640c8079acf8818de22
2664728df79967e54962537fa06bde323de630bf63ae92e57e33f242fd508e767da3f2dfa14c0
726b12bce09c4310502807ef00b88afbe76ff01a941ce512504c25d552e8863afa3c89bdb53d7
57d09161a5e65b4c1d6f4fe00879d1e247d8a93f30b252d5d6d7308676a76c4d9ee11131b2c2f
7f8092b0d2e417225f6d7c82a4eff0f7204765a4bcd2dafd0000000000000000000000000000
a0d1319202b353d",
```

```
  "raw_public_key":
"e45ffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b468cfc82bb929
f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f124d5e60bd68b8
c7e31fe01c7b0dc65ae470501cc565a6e1dfcfcfd12565433c4afedd511821e2e9610c45275e2
836dee35ced69d7efa672fd1e4318bef5eb6e897e8b451aa202ded042b2aaef77a7be3f699146
da229a8bdb3ffa496445967e75217bfbc9048f9956443d8731f833eb30de10dac96fffe7cf65e
a0445c3e31e8601e133be6a100764fe3196e267726441f31751fbf9a6f5880644f4e7275e57de
2b0f105e4db055d50dd1c9c934fddf535b8de28b0c74c0449f222cd2ed0bb8fbc775ccee8c940
665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee7581856ebd68f268459
56e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab932e69f778e2c
eefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a3655098
941993a1594860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8da
c1f861fd58e2afba5de5a52e020904f5b42bc0874e35befcf3e6119684768f36e008f04712177
cebe627607381e56eaaee161c1729b8de51dbde474d48cc68249ea27162b87993e60c84ed6cc6
423cb3676d9eb50b2cab5a3a049ef131381d623fa6fbcbc9db1e7cc025ea0418b9dad2cc6ccd4
e95fa2cec24feeca70318a751716b7213f63edbf65a63338357f838f94ec071822c2485124888
5107b3d1c4e924678c7614ea1af038104619f2ae372940becfa69e29cbb5ff6c3e20a47be4a4f
74bac34c133c00a6a706accc6ffd3d8e4fbd69a99704e1283c850d8c58d1e5753cd9587b83c4c
346cb9a58137213ec10834c66adfe2bb5c501a8ef2ecadd1b677a3df1a6deb86ebf0722c4f503
0e20f9018dd5b6fc53eea24fd92b7b5b4025feae996d3e48fd4c650d82dbad7eaf93663969851
2f26253d2ef6847c8518e8565cc9a5495c6fff57cde7323882c54a7db470ab2daf8ffd2bf794f
a7c692d9e7fbd532eecc1d7880e2ca0b3216128be28b4a9f1d151fac97808b0bd98b7b43a612a
9ac865812bfeac6f47460277840b52a3b087f916ca7cedc0f768ea2bd19ea21155f84b4a04c40
00ad2ae0587154d560bc0a477a4f9329a8984dd31eb1f2a05e3d918701d630cfca9af61ef088d
2c5581acb463e439902e5d425719e956b8d6df7305b28e0ff27d3ad0de2085d292499b19a3390
d4396fb3bac9a8d8cbead2a7a4290fc9ac6fca045f98a614a45a39cbe24360f84d14f8e472712
aceb74dbf45b53d49a0e4737e476ffc4d5b2f7cd247aa186d3b764ad9e9cfeee456a73c291d8d
e3912414ac43911c372173ad7b472af35c6853ced2fe7b5fe0a89565ab33baa6f65cdd928319d
7065e040e7a5e84f9aa903f7648094bad07136b16927b8ec6dbc2bef0cc2856de1e795923e141
2c49f24deeb6c21f6c8a9765c9c7986e0da4b4c67d8e0d0c8d466824fb923d8573148990cd2ef
133c78ceecab72ed9dd285c5a3766852d54534207ffd34027f6c76ede8fd1a32d72c30048bbaa
797d5df6fde27d087de5721ad7b7fa3e8d3f70d6bfc3ab2e252335368bbfa15acb5cb37d4694e
8b23cebe25de9c925a221a183b904d3f85df9929a919c54d6f87457373a0d6ecc1403e4cbbe62
0999435e80696634cd1a8e4747e9825bfa336e5bbad14f73640f1b9febe800dbaefe1630c61fa
e635b074c564eaa9db189c9e7302873fc64e6d497bc5c29080987a07a21d4af210703a4fa07f2
fd816f12fd1e29b4c0f44afe9bd4a1eaa8a7ae6f02a5b4258f52caf6127f62632a67cf4e8310b
e56a7c28c86b2e277600c3e92c8d23d42586244c571e90568df202f2f6d81f860a565f9eb91a3
c78372e2a8b1be61c5418cf49bf2d6c8955d4a482a9919b7660b3f9a4404ffc454ea073e1e4b2
689ab2cca4e46bd7004a6c491fa26ee7a57d60f35edb2b821e6266442c8f335d452d524c772e0
353724c23c7dd15b7aa155e91442022140c5fcb0153147edcf3e8952f6f0399a3c88066a72756
c9409915de63f64fa797841c57c796c6fc550ef745dfe9f179457f94755ae5a2506a764f327e5
50be3dc14dd41f3b04b147d454938c63a8d69b2ea4c5710ec0b36e3a6c72571fa5d59dde036c4
2033df35af056966ff0cd1204008971aa6ba9fb97b685ab9ffa2a9d1778104cd2c3b326de1fcb
c242e94d0311c3275b12850ed30ceead3a2ee6d060508411d4396f5421d8b6d067cf7cb5e8267
85fbe119e05e21bd879b64f57cb0cd1972c2815f20abe7ce6ab34d0f471af44baad179e906441
22f5f33288e689ddddc5ce833e9755df1e73c65c5a201c4ede2ffa6b19274927719d2d38fdb7a
65aa43708b7fa9a94aa7d3210253d78d3b181e1020d0000bd0a1dc05d447f9f58ebeb84c65b36
c8afcb83727a1508994e826957a663b0b9b8a003325ab6d6d6462ee4e106019c0dffe10323b7b
de7d82a38f85fd08786e860ba66c161b64b0708c363de5c6af62d8db3c243d1e1b712cb1d59e9
42b9b6b4295a5a500b182cbd5fd1bc6ce9376d91b47a2284f1fbe0ad1c048cc2cfbb4afa3a9eb
9697503b69feca990eba7e9441af9ca44cb3ac6b5ed66e591c201fe30efa8a7c471dc613d6254
c263a8e132104bec47f1aacb3b2fcd4051b69b5e3fcb1c147a65c2f90c4b5188bafc521cab03c
12a309da50b5a7517727ed41228ed123fe1b152f6a6319cd623bf34ad7b8e064ab993260bcbd4
05f5b7fff9b2fa40ba5ed5630242539e5d96823e89dc818a13d16675ee3079d976f694f5acc97
60ae789e9b3391b289e0e22a7ef17cc6a4577157b6d95c09baa4fd532e3ee0a290810ed35e56b
b19d9b61fb98a97c617425b06093d98a5cf0ee2dd127f0eea600b9a0c67fbe761db9b77e5d5bb
a9701da1b883e521a0cfe88451f57bd36085b67e56f061f84a2e6a152a71bce6e522daab6a0a3
3ce22e537fa9793d28b617e6c0a4176a83aa3be578afac0f2f5547c5516d218984755b7445c71
```

```
43afa4e551fce0071bdb873b34e6b9e2b9e79ed0c69d288ed6421f237e860a0c6492ebbdd2a44
c2c4f368dbe99941b1e8561d859d3859f496cee3d741f252973f8fcc539c409e35cc80a5ed6df
23cc3a65601313f5d681fd9540c5291a9e30a72e38c96413c47c61ff84fde78d011b01b4154d1
b920af003f7abb1e1999dea6a766cf9fd2702b3ce0ee57af931b62124b0861b163a3b91aa4bea
28076c3432df3b29b6c4e1ba588def420071fc157de90eb2722ecc9ab00df3c669383a61a91bb
67bd287ce349b4745ee7a479dbceef166b9acc412eb579fcd6437307edda253d606b7be7599c3
8092bc52a8598480edab8b82b1d21c565d2137ceae0b6642619b16133d91205d6355029e9cdfe
b9a28b373d95916b6b707d4c712c09cf36daf1a511b2bedb1aa70ee58d46a0666bb287784b0a3
840c589a7a04d5d6f2216be90aa4a512d5632f5c9bfe7b8b13382f999b95d367c7c46b968074c
e315197a5ff3545c7b77a804ade56a95b5c24cdece5937b5c0366d93ad03da9bc5db1b551dfb9
1e9b343d2b57b763439686d4a3"
}
```

Figure 8: ML_DSA_87

Acknowledgments

We would like to thank Simo Sorce, Ilari Liusvaara, Neil Madden, Anders Rundgren, David Waite, Russ Housley, Filip Skokan, Peter Yee, and Lucas Prabel for their comments and reviews of this document.

Contributors

Rafael Misoczki
Google
Email: rafaelmisoczki@google.com

Michael Osborne
IBM
Email: osb@zurich.ibm.com

Christine Cloostermans
NXP
Email: christine.cloostermans@nxp.com

Authors' Addresses

Michael Prorock
Tradeverifyd
Email: mprorock@mesur.io

Orie Steele
Tradeverifyd
Email: orie@or13.io