

CBOR Object Signing and Encryption  
Internet-Draft  
Intended status: Standards Track  
Expires: 17 April 2026

M. Prorock  
O. Steele  
Tradeverifyd  
14 October 2025

ML-DSA for JOSE and COSE  
draft-ietf-cose-dilithium-10

## Abstract

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

## About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://cose-wg.github.io/draft-ietf-cose-dilithium/draft-ietf-cose-dilithium.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/>.

Discussion of this document takes place on the CBOR Object Signing and Encryption Working Group mailing list (<mailto:cose@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/cose/>. Subscribe at <https://www.ietf.org/mailman/listinfo/cose/>.

Source for this draft and an issue tracker can be found at <https://github.com/cose-wg/draft-ietf-cose-dilithium>.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 17 April 2026.

## Copyright Notice

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

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

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
3. Algorithm Key Pair Type . . . . .	3
4. ML-DSA Private Keys . . . . .	4
5. ML-DSA Algorithms . . . . .	5
6. AKP Thumbprints . . . . .	6
7. Security Considerations . . . . .	7
7.1. Private key compromise . . . . .	7
7.2. Rationale for not supporting HashML-DSA . . . . .	7
7.3. Validation of keys . . . . .	7
7.4. Mismatched AKP parameters . . . . .	8
8. IANA Considerations . . . . .	8
8.1. Additions to Existing Registries . . . . .	8
8.1.1. New COSE Algorithms . . . . .	8
8.1.2. New COSE Key Types . . . . .	9
8.1.3. New COSE Key Type Parameters . . . . .	10
8.1.4. New JOSE Algorithms . . . . .	10
8.1.5. New JOSE Key Types . . . . .	12
8.1.6. New JSON Web Key Parameters . . . . .	12
9. References . . . . .	13
9.1. Normative References . . . . .	13
9.2. Informative References . . . . .	14
Appendix A. Examples . . . . .	14
A.1. JOSE . . . . .	14
A.2. COSE . . . . .	15
Acknowledgments . . . . .	16
Contributors . . . . .	16
Authors' Addresses . . . . .	17

## 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. Algorithm Key Pair 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 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 JSON Web Keys (JWK), 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": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
}
```

Figure 1: The all-zeros ML-DSA-44 JSON Web Key

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'000000000000000...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 [I-D.draft-ietf-lamps-dilithium-certificates], 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 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 Algorithm Key Pair Type section 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, 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 bytestrings using the algorithms defined in Section 7.2 of US NIST [FIPS-204].

When producing JSON Web Signatures, the signature bytestrings 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 algorithm key pairs 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 algorithm key pairs 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 JSON Web Key and COSE Key examples in the appendix 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 [I-D.draft-ietf-lamps-dilithium-certificates] 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 [I-D.draft-ietf-lamps-dilithium-certificates] 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 is requested to add the following entries to 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: TBD (requested assignment -48)
- \* Description: CBOR Object Signing Algorithm for ML-DSA-44
- \* Capabilities: [kty]
- \* Change Controller: IETF
- \* Reference: RFC XXXX
- \* Recommended: Yes



## 8.1.1.2. ML-DSA-65

- \* Name: ML-DSA-65
- \* Value: TBD (requested assignment -49)
- \* Description: CBOR Object Signing Algorithm for ML-DSA-65
- \* Capabilities: [kty]
- \* Change Controller: IETF
- \* Reference: RFC XXXX
- \* Recommended: Yes

## 8.1.1.3. ML-DSA-87

- \* Name: ML-DSA-87
- \* Value: TBD (requested assignment -50)
- \* Description: CBOR Object Signing Algorithm for ML-DSA-87
- \* Capabilities: [kty]
- \* Change Controller: IETF
- \* Reference: RFC XXXX
- \* Recommended: Yes

## 8.1.2. New COSE Key Types

IANA is requested to add the following entries to the COSE Key Types Registry. The following completed registration templates are provided as described in RFC 9053.

## 8.1.2.1. AKP

- \* Name: AKP
- \* Value: TBD (requested assignment 7)
- \* Description: COSE Key Type for Algorithm Key Pairs
- \* Capabilities: [kty(7)]

- \* Change Controller: IETF
- \* Reference: RFC XXXX

#### 8.1.3. New COSE Key Type Parameters

IANA is requested to add the following entries to the COSE Key Type Parameters. The following completed registration templates are provided as described in RFC 9053.

##### 8.1.3.1. AKP Public Key

- \* Key Type: TBD (requested assignment 7)
- \* Name: pub
- \* Label: -1
- \* CBOR Type: bstr
- \* Description: Public key
- \* Reference: RFC XXXX

##### 8.1.3.2. AKP Private Key

- \* Key Type: TBD (requested assignment 7)
- \* Name: priv
- \* Label: -2
- \* CBOR Type: bstr
- \* Description: Private key
- \* Reference: RFC XXXX

#### 8.1.4. New JOSE Algorithms

IANA is requested to add the following entries to 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 XXXX
- \* 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 XXXX
- \* 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 XXXX
- \* Algorithm Analysis Documents(s): [FIPS-204]

#### 8.1.5. New JOSE Key Types

IANA is requested to add the following entries to the JSON Web Key Types Registry. The following completed registrations are 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 XXXX

#### 8.1.6. New JSON Web Key Parameters

IANA is requested to add the following entries to 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 XXXX

##### 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 XXXX

## 9. References

### 9.1. Normative References

- [FIPS-204] "Module-Lattice-Based Digital Signature Standard", n.d., <<https://doi.org/10.6028/NIST.FIPS.204>>.
- [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/rfc/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/rfc/rfc7515>>.
- [RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <<https://www.rfc-editor.org/rfc/rfc7517>>.
- [RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <<https://www.rfc-editor.org/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/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/rfc/rfc9679>>.

## 9.2. Informative References

[I-D.draft-ietf-lamps-dilithium-certificates]  
Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-13, 30 September 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-13>>.

[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>>.

## Appendix A. Examples

### A.1. JOSE

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "T4xl70S7MT6Zeq6r9V9fPJGVn76wfnXJ21-gyo0Gu6o",
    "kty": "AKP",
    "alg": "ML-DSA-44",
    "pub": "unH59k4RuutY-pxvu24U5h8YZD2rSVtHU5qRZsoBmBMcRPgmu9VuNOVdteXilzNIXjnnqJg_GAAxep
LqA00Vc3l00bzRIKu39VFD8Lhuk8l0V-cFEJC-zm7UihxiQMMUEmOFxe3xlixkKZ0jqmqP3rKryx8tSbtCxyfea64
QhT6XNje2SoMP6FViBDxLHBQo2dwjRls0k5a-XSQSu2OTOiHLoaWsLe8pQ5FLNfTDqmkrawDEdZyxr3oSWJAsHQxR
jcIiVzZuvwxYylzl2STiP2vy_fTBaPemkleynQzqPg7oPCyXEE8bjnJbrfWkbNNN8438e6tHPIX4l7zTuzz98YPhL
jt_d6EBdT4MldsYe-Y4KLyjaGHcAlTtk9oa5RhRwW89T0z_t1DSO3dvfKLUGXh8gd1BD6Fz5MfgpF5NjoafnQEqDj
sAAhrCXy4b-Y3yYJEdX4_dp3dRGdHG_rWcPmgX4JG7lCnser4f8QGnDriqiAzJYEXeS8LzUngg_0bx0lqv_KcyU5I
aLISFO0xZSU5mmEPvdSoDnyAcV8pV44qhLtAvd29n0ehG259oRihtlJtWeiU9V60a1N2tbZV15mEqSK-6_xZvNYA1
TCdzNctvweH24unV7U3wer9XA9Q6kvJWDVJ4oKaQsKMRCSmlteBJMRxWbGK7ddUq6F7GdQw-3j2M-qdJvVKm9UPjY
9rc1lPgol25-oJxTu7nxGlbJUH-4m5pevAN6NyZ6lfhbJWTKlxkrEKZvQXs_Yf6cpXEWpI_ZJeriq1UC1XHIpRkDw
dOY9MH3an4RdDl2r9vG1_IwlKPNdh_5aF3jLgn7PCitlFNJAwc8fIncAXgAlgcXIPRXdfJk4bBi089GGccSyDh2Eg
XYdpG3XvNgGWy7npusONTE7WIyblAk13UQu04sdCbMIuricdyfE73mvwj15xgb07RZRQQtFGLFTmnFcIdz90zDrWXD
bANntv7KCKwNvoTuv64bY3HiGbj-NQ-U9eMylWVpvr4hrXcES8c9K3PqHwADZC0iIOvlzFv4VBoc_wVflcOrL_Sio
aNFCNBAZZq-2v5lAgpJTqVotqJ_HVraoSfcKy5g45p-qULunXj6Jwq21fobQiKubBKKOZwcJFYJD7F4ACKXOrz-HI
vSHMCWW_9dVrRuCPJw0s0aVfBRqopDNhu446nqb4_EDYQmltTHMozPd_jKxRRD0sH75X8ZoToxFSpLBDbtDwCenxj
-zBf6IGwfZnmaetjKEBYJWC7QDQxlA9lpJVJCEgieCkoIfTqkeQuePpIyu48g2FG3PlzjRF-kumhUTfsJo5qS0YiZ
Qy0E1BMS6M1lEvuxXRSHCLHoy5nLYI2Sj4zjVjYyxSHYPRPGGo9hwB34yWxzYnTPPGiqXS_dNCpi_zRZwRY4lCGr
Q-hYTEWIKlDm50lttvC4_eiQldv63NiGkLRJ5kJA3bICN0fzCDY-MBqndlcWn8YVBijVkgtaoascjL9EywDgJdeHn
XK0eeOvUxHHhXJVkNqciBn804RQdpVU60TSA-uuu675ytIjcbHC6kTv8A8pmkj_4oypPd-F92YIJC74lswkYQoeIH
j8rE-ThcMUkF7KqC5VORbZTRp8HsZSggiJcIPaouxdl-8Rxxrid3fXkE6p8bkrySPYoxWEJgh7ZFsRCPDWX-yTeJw
FN0PKFP1j0F6YtlLfk5wv-c4F8ZQHA_-yc_gODicy7KmWDZgbTP07e7gEWzw4MFRrndjbdQ",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws": "eyJhbGciOiJIJNTClEU0EtNDQlLCJraWQiOiJUNHhsNzBTN01UNlplcTZyOVY5ZlBKR1ZuNzZ3Zm5YSjI
xLWd5bzBHdTZvIn0.SXTigJlZIGegZGFuZ2VyY3ZzIGJlc2luZXNzLCBGcm9kbWVzZ29pbmcb3V0IHlvdXIGZG9v
ci4.knIlQ_9CIzLH5Xy94Kkc7WVKqZcAgtJ3mNf0GUjluLA6YXAWFJfXkh-zQxUtEl3UIC7zPCiUwKTDR6ZsuUmFj
8Ctb_6aH64hElN7weS_lm5okCy8GqHNL2lsfclCH3Y2f4QNP-DLVS1XsuboDA7Dw3ir2IdYKIfWJyIU7ROHgd24nu
unlZJbxcLJC2EKt2M8R0wZudcIE9nm5OpZYXq0z-hPsKoXp9leVYkqgMm09Lo8SP_1YYIEth3B8v-GuP249KDTFRK
PjISmK4aPcKnjtjihHsQVv2XePXkEXatHl4qhsiiW-y-EJXa1KfW4WYpLA7B4_5Ids--cIJmIx7f6xxAWKh5qoBW
```

q1QIOaaFuzsAraRW3NOEuzThew1En85gI3GcRTZGp-VDGyxHm0A104cyWo2bxAVOF0fbDc265iP2mCNw6Qg10jiJe  
AhGB4OAMyCBuWJAG011MN1U\_koEmGh5dXKnQTRL461ea\_Cq3DLKcA2Dj2woWUFyDTmQ8oO\_yheASfJacyRm7\_suj8  
8z5XFNo8F53P8OxTG9xUPlrwH-TAq7AH3NU4SNXApYVKtU3zhx1tJ34nlTILcTuJxVJVo\_f0DZfUxr6JSCYqvy4z  
1K10wDQzd55aopyFtQxvOPhcCHbAN34g2Ug750Jm835f17N0xcqoMbuTcgH68kr37M-Pdh2K9WazXUJgCupgdIWW8  
WjfoJmTiF59CrVtFvK2qDzF400ENCfqtNPQ1Ze5cN5p0P8arj4USB8HCPh7NdqQBAEWrW0wsYhdiM39lrSkA8mLR  
YMHZnqKGCTPCrHXDDejRKYRNaqIUT441aY15c27K0v-ozjKpu6tzEhkYSC4XZ3LehEFTmAzOE0mHbhKMGXqjoPJJO  
rGIPibX3jwK8\_Q5RmMOXtXo8R3vXfBaUdQoLeeyyWNYE0nIcsl4z5a8\_utwEFiVf0VK2pdviyiOPVSi3zOMAmqz6g  
FhVy8aMMQOWZAEAuTyDw7ZWG6diwptmrgSXZotW63I19S2ZH7keCXRIq\_pFLuYhOuG6dD4MkouILRdC9bXZMLrNDq  
7COpU0086aQVlYd0pR935WpUw-V6obSRnHlRFZSmUSIB7h1Q0ImciRzojN93Xhw7qpzGzdzDEO300TayXaSG\_0YHQ  
yy-eH4hBbmgT\_LBx120gleY4XHeHFRfTfetHkL5ZZusX1jQ\_nk9ez4XBG\_6hRtTNSuVBsYlH8-KUuR5-qTP8dkvRf  
8Wk2hHoUr2sz5YO\_xDFCMMTrt8ahiMyfjJo5ih5Fwo3riFbFUGKibniTLXspFd4spcNK\_wchlZLRgkPK4jh6Z\_X8JJ  
kHxvQhpyouHQFYGxgBr124x-\_EB1zbWMhJthmm8DiKt-nzKaJz8Cjul-HwCpg76CRqRsEz2hyKEpbb4M5KQSj3AsE  
NCroVmQ5Qiv3K2XNRkve4vjBmP6sV2b6GSY\_UeRvPELA7SUGBGTKbn-c0aYhBuB8plPhRTBa55\_cFqAmNmavF1-fd  
MktJuIah2f-K0zCzbHw54998T7kIWgyMsyGCAvynEB\_khOqwT7tCjg5HQ8SIjdnRYW0kjjZfjt5LJbGA-PnRo8gPV  
QVGeYDP2vsSXhNJY94AitKCYlsrcSsuYDrhNBKrnOJluEsMPVHsgFw\_ZHMyAEaVQughSNW4fm8q6\_lNv4zLutDITz  
mAL6a6i6-WS6QRIs\_4Vutwr5cXXIFDDeHVWGeGcNivQ6W9urEUP4crguiq7z\_DTiYaGfUksub-T7mw0zU8ZoOSd5pU  
TpJLv-IYIUAl6CscHvunnRLEKqpW1SaldcFZs5VP4Afr3mg7wX4Vlq1AHnpFxE2L1LZiKoTc9jDEOvTDkxr86gMkw  
Mm6RdyPF\_q48AVJlbr8Qp88-4B84X52zZ5cw-IJYe-HiVJ29LpeYm340\_rWivpy-UB5i9TKlMrxf94ylokzZTPbP3  
\_v1\_XX0nE7RTLz98EA96euJ7l3EpbeQks7mh6ilFJNnvvlM\_u29sYobJ6PUT-ilVlQnF\_JBARKEz74pBXm1l5Y5Lo  
l5rsIlaQHInUBCO8fHCHI59LafKusN4JmodDqLYwkWijEL\_sfrC6LtrbXqpMlpw09zSrs\_tS1RQ-LnWHuPrU5KLCz  
v53JKrh8lU\_cdBowe\_F-Ib\_Ui4bQ2FME-0mnyG0XiJHUsrGMZ9dfowvIkr83JpqwlFOZAwMmSGPNPEJRw9kDshjot  
ndUB5S1UCfv\_U4IoVn7WgvxeCS-BBxqyWfh7YTdf73EnmGwVYxVj1XaHCeeTZmUacnT4MQUAcBFjTq6BBlboAQGWP  
2FZWpd6HNnruv744VeWmfGkL9z5567wFhwuXMkme2xvDo4wP80xutjUfsePx5YkLxhY1XsWqTZr19tInxJWWq8RLZ  
sWPmtq5wZ5ucBMasCLpOABenYZdSACQNhC73wLS0Z2s1HQhBoil7lrlp372LzS\_Seulu\_8Fo7DoJqRpKaNoC2\_JUM  
mn7TUZS8zLyzzxgeq8R8iNbRP20DwDBNXocsTDBKaQrtB-QiEPySQtJa4H661XeNZyh5aGzfowZ9OmjZG9pbbhecgwI  
rt-ESjPyeT6sfSrvOfTzr7fBXwpUs2rS4Br1Nse5g\_h8CQik8aa0TOEPkXiyg4s5DewRlgDZHS-3g-YXPUIBNO62  
\_HxknkMpkJvKW-tkvDbgtxvy4nG80ul6W\_KerSoEKDTRYNKZWxXjZITNa0h6agnwNCJKEbFg3Qhre394c0i60mfP9  
YIgKTXrCX3Yt2eX-6mPzYmLbSbv5jH69v6WZqYV2WAj-9DU0diR4hofYQaJnBZhTtKb-SQsYiFuNlBDJ3v9eM9K8h  
q91NBdCHVa-Thk9Dov-JkctZnZGRRyW5yXHUV4NOElTBXh8GkjJdvs5Yo3u-2rPCXjK1aGPSi1W8BaUJLQY5sbfAV  
CAuUHBv-Vlh5Qamt-lgeKguhqTSuy-tjabOb5kiBOG7xGQt3z-XYXtnWFDcIi-5h1lXfZsQ-xQxy8gSfdMz4hDK9N  
w\_VQt6fzWiQY0Th\_dHzVki0MUfVfsDUjgblhd6j0wgsb3zdj-GM3rtt8oit0wXx1lb1OaOKgf07tP0wimVXMRqRWe  
7LCUAKTE5PkRKUlX\_h4iusrzi5uwKDhc4SmRwm6KssNrmCAkiNDZCREVKd3yMnrja4PAGDzdKWVplcHJ6jKmrSbrE  
ztHd9QAAAAAAAAAAAAAAAAABIfMEQ",

"raw\_to\_be\_signed": "65794a68624763694f694a4e54433145553045744e4451694c434a72615751694f  
694a554e4868734e7a42544e3031554e6c706c63545a794f5659355a6c424b52315a754e7a5a335a6d3559536  
a49784c576435627a424864545a76496e302e53585469674a6c7a494745675a4746755a3256796233567a4947  
4a3163326c755a584e7a4c434247636d396b627977675a323970626d63676233563049486c76645849675a473  
976636934",

"raw\_signature": "92723543fff422332c7e57cbde0a91ced654aa9970082d27798d7f41948f5b8b03a617  
0161497d7921fb343152d125dd4202ef33c2894c0a4c347a66cb949858fc0ad6ffe9a1fae2112537bc1e4bfd6  
6e68902cbc1aa1cd2f696c7dc9421f76367f840d3fe0cb552d57b2e6e80c0ec3c378abd887582887d6272214e  
d138781ddb89eeba7d7325bc5c2c90b610ab7633c474c19b9d70813d9e6e683f3617ab4cfe84fb0aa17a7d95e  
55892a80c98ef4ba3c48ffff5618204b61dc1f2fff86b8fdb8f4a0d315128f8c84a62b868f0a49e3b638a11ec41  
5bf65de3d7c4a1316ad1e5e2a86c8a25becbe1095dad4a7f0e166292c0ec1e3fe4876cfbe708266231edfeb1c  
4058a879aa8056ab540839a685bb3b00ada456dcd384bb34e17b0d449fcee6023719c453646a7e5431b2c479b4  
025d387325a8d9bc4054e1747db0dcdbae623f6982370e90835d232097808460783803187015162401b497530  
dd5446e4a049868797572a7413465e3ad5e6bf0aad32e4700d838f6c285941720d3990f283bfc178049f25a7  
32466effb28efc33e5714da3c179dcff0ec531bdc543e5af0bc7f9302aec017f7354e12357029c9529357ce1  
c75b49df89e54c82dc4ee8d7549568fddf0365f531afa2520f8aafcb8cf52a5d300d0cdd6796a8a7216d431bc  
e3e17021db00ddf8836520ef9d099bcd9f97e5ecd3b172aa0c6ee4dc807ebc92bdfb33e3dd8762bd59acd75098  
02ba981d2165bc5a37ce8e64e2179f42ad5b5f56d2b6a83cc5e343843427eab4d3d09597b970de69d0ff1aae3  
e14481f0708f87b35da90040796af0d30b1885d88cdfd96b4a403c98b458321667a8a1824cf0abld70dd12344  
a61135aa88513e3895a625e5cddb2b4bfea338ca3eeeadcc48646120b85d9dcb7a1105b66033384d261db84a3  
205ea8e83c98ceac620f89b5f78f02bcfd0e5198c397b57a3c477bd77c1694750a0b79ecb2c0d604d2721cb25  
e33e5af3fbadc0416255fd152b6a5dbe2ca238f5528b7cce3009aacfa805855cbc68c310396640100b93c83c3  
b6561ba762c29b66ae0497668b56eb7235f52d991fb91e097448abfa452ee6213aelba743e0c928b882d1742f  
5b5d930bacd0eaec23a950e3bce9a415958774a51f77e56a54c3e57aa1b4919c79511594a6512201eel5d0d08  
99c891ce88cdf775elc3baa9cc6cddcc310edce3936b25da486ff4607432cbe787e2105b9a0b7f2c1c75db483  
5798e171delc545f4df7ad1e42f9659bac5f58d0fe793d7b3e17046ffa851b53352b9506c6251fcf8a52e479f  
aa4cff1d92f45ff16936847a14af6b33e583bfc4314230c4ebb7c6a188cc9f8e3862879170a37ae215b15418a  
89b9e24cb5eca45778b2970d2bf59c86564b46090f2b88e1e99fd7f092641f1bd0869ca8b87405c86c6006b97  
6e31fbf101d736d632126d8669bc0e22adfa7cca689cfc0a3bb5f87c02a60efa091a91b04cf6872284a5b6f83  
392904a3dc0b04342ae8566439408bf72b65cd464bdee2f8c198feac5766fa19263f51e46f3c4940ed2520046  
4ca6e7f9cd1a62106e07ca653e145305ae79fdc16a0263666af175f9f74c92d26e21a1f67fe2b4cd90b36c7c3  
9e3df7c4fb9085a0c8cb3218202fca7101fe484eab04fbb428e0e4743c4888dd9d1616d248d97e3b792c96c60  
3e3e7468f203d541519e6033f6bec49784d258f78022b4a098d6cad4acb980eb84d04aae7a09d6e12c30f547







```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "Suiu29qbfuaBaR4Ats-c6XQBePB_OpAxAwcTR_0KXVM",
    "kty": "AKP",
    "alg": "ML-DSA-65",
    "pub": "QksvJn5Y1b00TXGs_Gpla7JpUNV8YdsiAvPof6rRD8JQquL2619cIq7wlYHj22ZolInH-YsdAkeu
Ur7m5JkxQqIjg3-2AzV-yy9NmfmDVOevkSTAhNNT67RXbs0VaJkgCufSbzkLudVD-_9lGQqVa3mk4aKRgy-wD9PyZ
pOMLzP-opHXlOVOWZ067galJNlh4gPbb0nvxxPWp7kPN2LDlOzt_tJxzrfvC1PjFQwNSDCm_1-Ju5X2zQt1XyJOTZ
S5lQ1CtB2C7jdyoAVwrftUXBFDkisElvgmoKlwbKs23fU0tfjhwc0LVWXqhGtFQx8GBBQ-zol3e7P2EXmtIClf4Kbg
Yq5U7Lwu848qwaItYtT7EmM2IjxVth64wHlVQruy3GXnIurcaGb_qWg764qZmteoP15uAWwuTDX292Sa071S7Gfsh
Fxue5lydxIYvpVUu6dyfwuExEubCovYmfz_LJd5zNTKMMatdbBJg-Qd6JPuXznqc1UYC3CccEXCLTOgg_auB6EUdG
0b_cy-5bkEOHm7Wi4SDipGNig_ShzUkkot5qSqPZnd2I9IqqToi_0ep2nYLBb3ny3teW2lQpccoom3aGpt5Zl7fpz
hg7Q8zsJ4sQ2SuHRCzgQluxYlFx21VUthAjnFDSOMokGyo4gH2wcLR7-z59EPPN15lpljyNefgCnMSkjrBPyzlwie
T-uqi23f8Bq2TVk1jmUFxOwdfLsU7SIS30WOzvwd_gMDexUFpMlEQyL1-Y36kaTLjEWGCI2txlFTULttQx5JpryPW
6lW5oKw5RMyGpfrliYCiRyQePYqipZGoxOHpvCWhCZIN4meDY7H0RxWWQEpIyCzRQgWkOtMViwao6Jb7wZWbLNMeb
wLJeQJXWunk-gTEEaMykVJJobwDuiX-E_E7fSybVRTZXherY1jrvZKh8C5Gi5VADg5Vs3l9uN8-dVILRyOolvjxc
lmsRcn6HEvTvxd9MS7lKm2gi8BXIqhzgnTdqNGwTpmDHPV8hyggJWxWXClTBSSgY6OkGkioMAmXjZjYq_Ya9o6AE7
WU_hUdm-wZmQLExwtJWEIBdDxrUxA9L9JL3weNyQtaGiTpjXcheZiNBbBJTUxXwIYLnXtTlM0mHzMqGFFWXVKS_N_A
IdHyv4yDzY9m-tuQRfbQ_2K7r5eDOL1Tj8DZ-s8yXG74MMBqOUvlg1JNgNcbuPKLRPbSDON0E3BYkfeDgiUrXy34a
5-vU-PkAWCsgAh539wJUUBxqw90VlDu7eTHFKDJEMSFYwusBPhEX4ZTtwoeTHg--8Ysn4HCFWLQ00pfBCteqvMvMfl
cWwVfTnogcPsJblbEFVSc3nTzhk6Ln8J-MplyS0Y5mGBETVko_WlyeFsoDCWj4hqrGU7L-ww8vsCRSQfshK8lodil
zj0xmugiKjWUXbYq98xlzSnB9dmPy5P3UNwwMQdebtR38N9I-jup4Bzok0-JsaOe7EORZ8ld7kAgDWa4K7BAXjc2
eD540Apwxs-VLGFVkXbQgYYeDNG2tWlXt20-XezJqZVU16-IZXsqc7DiJwNin03ft5o8ZAcLKUulzSlEXe8sIlHax
jLoJ-oubRtlKKUzbWOHeyxmYZSxYqQhSQj4sheedGXJEYWJ-Y5DRqB-xpy-cftxLl0fdXIUhelhwFBAoQU3b5xRY8
KCytYnflhsFFF4049xhnax3vuumLpJbCqTXpLureoKg5PvWfnPFPB0P-ZWQN35mBzqbb3ZV6U0rU55DvyXTuiZOK2Z
1TxbaAdlOZMmg0cpuzewgueV-Nh_UubIqNto5RXCd7vqqgdXDUKAIWyYegYIkD4wbGMqIjxV8Oo2ggOcSj9UQPSlr
D5u0rLckAzsxyty9Q5JsmKa0w8Eh7Jwe4Yob4xPVWWbJf9m16avRgzDxXo5gmY7txdGFYHhlo1JKdhBU9h6f0gtKE
tbiUzhp4IWsqAR8riHQs7lLVEZ6P537a4kLlr5FjfdF_yjJDBQmy_kdWMDqaNln-MlKK8eENjuO-qZGy0Ql4bMztN
bHXjfJJuSzapA-RqYfkqSLKgQUOW8NTDKhUk73yqCU3TQqDEKaGaOTsPscyMm7u_8QrvUK8kbc-XnxrWZ0BZJBjdi
nzh2w-QvjbWQ5mqFp40MgY94_tIU8vvCUNJiYAlRdyodlfpFH5-avpxOCvBD6C7ZIDyQ-6huGEQEAb6DP8ydwIZQ
8xY603DoEKKXkJwCP6CJo3nHfEdj_vcEbDQ-WESDpcQFalfrIiGuAlj-sEWcjGdSHyE8QATOCuWl4TLVzRPKaf4tC
XxlzyvhJbXQu0jf0yFzVpOhPun4n-xqK4SxPBCeuJOkQ2VG9jDXWH4pnjbAcrqjveJqvti7huMXTLGuqU2uoihBw6
mGqu_WSlOP2-XTEyRyvxbv2t-z9V6GPT1V9ceBuka0oGwtJqgD-q7NXFK8zhw7desIPZMXf3nuVgbJ3xdvAlzkmm
5f9RoqQx6m_hqwPQEccllMEZ3YML5hc99TdtZWY9gGkhR0Hs3QJxxgP7bEqGFP-HjTPnJsrGaT6TjKp7qCxCJlcfKL
Ur5AU_ksMULEyUsWwTSGJ9m3xBvsyWlJuo",
  "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
  },
  "jws": "eyJhbGciOiJIJNTClEU0EtNjUiLCJraWQiOiJpdDw1MjlxYmZlYUJhUjRbDHMtYzZYU0U1UEJfT3BBEF
3YlRSXzBLWFZNI0.SXTigJlZIGegZGFuZ2VyY3VzIGJlc2luZXNzLCBGcm9kbywgZ29pbmcgb3V0IHlvdXIgZG9v
ci4.ZmO9_0bLgJAegoVNymfRo4nGPK5lvtSFGnDbzfzYAD5mUEXpaBUg4itvZ8rAUzi4HLb59QqDQSBSPMXC0axaj
XOMV_YttfmwGgC6FMyaMRZkx-A92bGiNLutqX9jcwRLJqXjMkUGhz2YpHe_mv9QpxokRCH9K6jkyFZp4hZiWfXhRt
1z0OGIa5rOoHKSxOCAUZhTXKiASb3vk9lUASW0-Y58WKT4rVmst7_dvk7FVbe9A9I21IH-Tq1glzSMoI8ozh1aBSG
92uPursBd5KRcOlJwhNUYJDgHScIHXM6Hzk6u98W5orKPHulrDIK7rHJI4Zrui4WbjmQLsPE01LcZHRx4zexDCTMC
GSobjbLlFiT9CU3oUep4oWOytTEAf2eCi3qDD0iSrp5IslCueoNjtGOFSSnUKlsnCeizF-tNqTy1KpJ3ErTanPcCzCv
sEalhJwFa7NOWyQOEJUzcLaPY_VEFwcCXlGk4bEI-1rLDiyZqkXgny-U2oRnll0d3u-e2S_Rg-_eLlH_XEBPs_km-
822GJY9li4muZ5GVVvfQf_5hza1V4GweqvmeWuZLlGbuZ2HPS7x1tWL798AlOWOk1rMnxsvBOPiSLxAEdPoIuw0_qmLK
jTavJcDFaihgcGMUK5SjJ651IWQS9t4rgxv9Idu0OCsozo9iCBqrVcna0wUpkMhV6KeiXA7kQNcegVaMio40cjSyM
iEkHGIOEOf8L6eohOh_bPPRys-8NrZ-VOBJCa0ubJcDUlctUGNCA7nWWXaqfVjcmYNDx9XHBYSnSocFNfMP7S9nvq
w3KC50U_t2PH5Sfws9w4DLvcgrlEP_gwSgOXuf-i0tRGLQly3IMB7O8QOnkofyFaCUDZeurFkGTpoBfT6lzbJznQA
MIDPNcWUsRlNTXsH7atClnxl4xDJLmmPLCxiErxfxbCW5gMWox0kLDwfsFj57hsXG75cZ4jiBbq9b0Vjd7Vkf8xlC
6ExdzBhGXz8oJiat5WHDsuzGtrFmh6diNlC04Cxjr6KdNE8IlyxsfxXQ4AI-0ke3gMyi0DOGEgHuNc-JHD7oZ6nj
UMSTBkRlaUMNT7n_2nfFTDCdqWlHaMsMwIHfLok6dayKXE1oMqY5Op8S5k_SAaknR0vNxmhlTA5h3bZJ28NZxm6R7
D00_eBEYrH20rmRP7G7kXKzLvmWeaKAh4oQHiqjVhgauePDRiMmjx0OhdQnMctO8Pwbx06SiviRn_5hswdV08B4
8MVHqbm2AxCLLJYinc2Ep0302Uo0DI-rTNZ1Znn58km7VCskcxDLsH9AYvPz-HQr3H7Xg0ElwjYn-jJXgZ_cdnLft
4_TuKQdpw_qhvyrNjOx0Mdc-1PrwoWqpA9sSv_pS5lwI2qNVHI2Vj2mZHBdyodlQUeOQExf3SBjP_FHEAUzUulOK8M
-1SQZGzJT2su3a6ZnMnp0U5qdXyMONFoI2jJ2hdjt7QEQLx-rvaLxZJMjtc2z0MHdwJGAC_kug7Xjh3SWQZzBu7zz
reIaSwr2A2oobeZiAydwb8LX2QsY9Jr_NphGAMAqzrpkuamYbD_pFTKmp9s0GYxwyG1ZD9uRuPI9imA4CS7bt-08Y
vbwg6eQ-qa9OqDlxNt3Xc32TniQFVxVxN6PDY33XXU-Rpvd1w47NZ48nkyJzjD8Xlrvk9p2ynxWHR-Sto5HXZdru4
j8ETUW7ri3mEGlM_dXaAbE2kVbsBp2I1vPqpugbmRexuMRLdYFIkqNm0qpQWotr_k2t5KHnWolrSbFH7Usm8Pwyi4
sNhh4_yRHADO2q2o19zCCx2pLDsMEYI74CQPRGLlK_GLM455Bzfny3E2eaE5_gQBTSGNHpQtJB0ipPwDjqsJDCXqX
upCkRtalvxnxg4coi2-vWYvKu6mq9HhdovHAAwrZRyvuPPI4ZDN_NkmfOR8HoqR6NLVhLlRplcwMARSSDA3f8Qlnjd
```

baeutxRXvFnCCjBk79ws8VGdWAuRmIWgoEFeVAVxkJjJ07zOW8I3kNfB6pnxsZmJwWAGqWc1UlPmkNBstmSXinAzb  
dl-W-knlXRDUhzTafHnkCbKS5XgJKsWD2FrhcncCaxRxuxIGxi jofjD4ihmJoYDFh1FYs9IcC-szEfMSeKanWOIZC  
HdlfVzTSbLr5bNaOXR2sOlmuFX7w22m8pBVD3fyOHK2JnK4FBCnEBrruMIDaqq8Z4xesAHKfxY67w-25eUuvVCGL  
3xpXSyp90684ICkG4STztPlshLVsxKDA-37sKKplqemERlMPY4vDM1Np8JlVawbSGIuom20g6p2KV\_zpIPwx9vdln  
AiaeZbryf3N5gtL-dOq-c6uZhTCx9OLBtLGE3BcAmn5JfjMGQFxyTL07BlNu24Kf-lttGj9jzbwPZYrok-SnMilX  
GFEqB3D3cKCOlWjsgg\_3cUWluMp4KlWQvkmV9Pd7cY70w607jcYBJ3MlFZ8EeWeYPZ9qu6xwidA8XlLHxXxfLIJO  
gfpU8MTppfxdnMhqNSvH\_Hx57oDphbUks5KlZ8-O4dSnNqQ-ZWbhaAydYQFDKuUF6HYTAvaWhJmACxhTkTp2t6-P3  
bev-FcdFIIdszJC9LxWtJ96LY\_GV4Qvp0hiIdyPlBukWNHtsXK2Rxxres3\_4Cndg2BOGxVcKZ9YpQDCUy76GRbTCenq  
jD-SG5sVUEVha5yxbKArPr2-Xpgk8cuZBRsAdmPNRdxCGUtlldfCLeL7xhJvryMouxqF75PMBaImHcsMd95075ePt\_  
VkClUaUj55Y9E81FbOEchPfud2w3TtSvRPvB8-RgY8sLJUaClxcUGE4PnKSZJ7TIBUtHD6uyZ0-nC5KGxbXZsBEzU  
eHns4ix0Wmo6-6vAM4PGK3qRALVAhtKXyvNcAfVccVi8KJMK9Mz2eIOXPATvyRy34Ltrcg8tcgK0ftYqEWYpAZ2fV  
pZBXcYfTIinuLN0-qLra388EZuu59jvmRD7mUv1msMWVMGveBoNP3lJaJGGWK8iYyu4q7Grq-6WXR5qCz\_7kwAtVJ  
db-zW8U3jLJ3tRSYlyjlpzeVAGjDQ6Yni5y9x4BF-5QUqcoGMLLglyx2WOCeLT8IW7nsV2lQnqqAbtCzZ76UtEdmU  
uEOYqiKQZ0lrjMRm3YrCvJKxtR5thhTRka708NzBvwSRs-JxGG\_EWjHfT-aB4VL3IL\_oz3mt3iQoszfa-SzHcKU  
1laZMBuUCyxks6KiJgQGZRPXyaxxDtqZdaRP8Ic5CmuPeyu3kafi0L6LFiJsUxnSGxTpgu7hfvcmowQijfe9\_ylvg  
8k\_EbI2miG11giODVCYb7k9Yjyriwc9dSUUZ7Xois24hWYUX6BGGQNN3wVHPkDkOVSDBYTjt099ulquryx4K\_UMCu  
9sQVNxBfMh8tLN709-MXlnJbHfKfQFHiPGdIYOBPwuqJdAJiyiuSG3gJxMG\_wuwNkBW0--i0m6PIarCyyL8\_P-tu  
Uft4zIgjJJ3o6YJhbo-q2K82ZFmHuILyzfDSGtHDZpZIR7XnRQWet90cJEHL5k653kvyEHJg0iUiE0iwnA5d\_4gBq  
3vmwlJ74hWAHx0Z\_iYECPS6hDGow8M8D7UJTZDkUV\_86zj2YqGm\_QC\_aAed\_NP6sa61bI9-gTOzvYc0JiExKTDjO  
K9fIvHaV-HN4xr2vWner8o6jPyETvGM8D7aEezlUVOEFwALmhJPSMAq\_Fk9JlcIUuC-ITJZNTNz9Awfiru3wkPja1  
bXN76WAURHjia0x5ptgMCy2py\_vSHZybfIS85ZjsOQ-i\_e\_niBzhyzXwzBaLEyEitbF4ZQx5c88lXKDMpe9tirAI6  
XAcqLf4UZkd8Wm2YV7hhVfxLQlAWLekWE9DZlJctE-SbS1EWNGR8faXKCvaZznRyoqdWz8IN3w7KvaA\_ZrEKKIXkk  
reztG6pI06DlDHCl\_sU6rCOoyQf6y1AY77Ob4SdksROBHGGR6Uv-LrxHpyJ6trzcuc0kqxbHrkW2yHcqe6enVf43  
zYwWkUeJJZ10bt3a92ziSne-3aj6v3guiKoJoLnV\_9h8rUF6zorTWE-Tq58tYfb5SmGf4iCJ5cy9LTY0COIfwJtPk  
UmyBCZwUHWJnV24P5pOZPe\_CckQ28xv5J7Zf4Bvqrq\_rhubFEHTJ5Jvdmfz8Whc56WSHX7GRKEMqXvp3pHohBvOyT  
9BmotzIlibVklJy4gzKzUcJJJold-BOaM\_cnMiHpyKXSJAXTNwXngzEpbvDP2Y0fnrgqDpO3RR3gINaZLRmeGOWI  
4wWBMMfw8PHjpyVl7C\_lhmfRI-darbZcX7PD3N4Rw4lBACyk\_wnOHBCAS-5cLZEzNmFmhc4i04msz\_seQlN0drbB0  
NoUVWBmcY3pGC9TiY6f6Pn-FBUnQkuBhIyPtgAAAAAAAAAABgVHCUv",

"raw\_to\_be\_signed": "65794a68624763694f694a4e54433145553045744e6a55694c434a72615751694f  
694a5464576c314d6a6c78596d5a3159554a68556a524264484d74597a5a5955554a6c55454a6654334242654  
5463359315253587a424c57465a4e496e302e53585469674a6c7a494745675a4746755a3256796233567a4947  
4a3163326c755a584e7a4c434247636d396b627977675a323970626d63676233563049486c76645849675a473  
976636934",

"raw\_signature": "ce63bdf46cb80901e82854dca67d1a389c63cae6556d4851a70dbcdfcd8003e66504  
5e96815e02e22b6f67cac05198b81cb6f9f50a83412052a4c5c2d1ac5a8d738c57f62db5f9b01a00ba14cc9a31  
1664c7e03dd9b1a234bbada97f6373044b26a5e3324506873d98a477bf995f50a71a244421fd2ba8e4c85669e  
21648c055e146dd73d0e1886b9acea072acc4e0805198535ca8049bdef93d9540125b4f98e7c58a4f8ad59ac  
b7bfddbe4ec555b7bd03d236d481fe4ea960d7348ca08f28ce1d5a0521bddae3eeac05de4a45c3a527084d51  
824380749c2075cce87ce4eaf7c5b9a2b28f1eed6b0c82bbac7248e19aee8b8c018e640bb0f134d4b7191d1c  
78cdec43093302192a236cbd45893f42537a147a9e2858ecad4c401fd9e0a2dea0c3d224aba7922c942b9ea0d  
8ed18e1529d42a5b2709e89917eb4da93cb52a927712b4da34f702cc2bec11a96127015aecd396c90384254cd  
c2da3d8fd5105c1c097d469386c423ed6b2c38b266a917827cbe536a119e5974777bbe7b64bf460fbf78bd47f  
d711b3ecfe49bef36d86ec963d962e26b99e4a56f7d07ffe61cdad55e06cleaaf99e5ae64bd60054d873d2ef1  
d6d58befdf002ce935acc9f1b2f04e3e248bc4011d3e822ec34fea3252a34dabc970315a8a18028063149394a  
353ae485904bdb78ae0c6ff4876ed0e0aca33a3d88206aad572768ec14a6432157a29e89703b91035c7a055a3  
22a38d1c8d2c8c88492118838439ff0be9ea213a1fdb3cf458b3ef0dad9f953812426b4b9b25c0d4d5c4ee18d  
09ae7596c40a9fe56370cc8d0f1f571c16019d239c14d70c3fb4bd9efab0dca0b9d14fedebf1f949f1c12f70e0  
32ef720a5510ffe0f1c1280e5ee7fe8b4b5118b425cb720c73bc409e4a1fc8568250365edbab164193ca6805f4  
fa9736c9ce74003080cf35c594b1194d4d7b07edab42d67c65e310c92e698f2c2c6212b7f16c25b980c5a8c74  
90b0f07ec163e7b86c5c6ef9719e238816eaf5bd158c3ed591ff3195cd3a131773061197cfca0989a4f95870e  
cbb31adac59a1e9d88dd5c3b80b18ebe8a74d13c225cb1b1f5f1438008fb491ede03328b40ce19e1e0lee35cf  
891c3ee867a9e350c49306447569430d4fb9ffda77c54c309da96d4768cb0cc081df2ce93a75ac8a5c4d6832a  
6393a9f12e64fd201a927474bcd668654c0e61ddb649dbc359c4ce91ec3d34fde04462b1f6d2b9913fblbb91  
72b32ef99679a280878a101e2aa356181aba278f0d188c9a3c743a17509cc0ad3bc3d66f1d3a4a2be2467ff98  
6cc1d555d3c078f0c547a9b33603108b2c96229c2d84a74df4d94a340c8fab4cd6756679f9f2433b542b24731  
0cbb07f4062f3f3f8742bdc7ed7834125c23627fa3257819fdc7672c5b78fd3b8a41da70fea86fcab3633b1d0  
c75cfb53ebc285aaa40f6c4affe94b9970236a8d547236563da6647072a1dd5051e3901317f74818cfff51c40  
14cd4bb538af0cfb5490646cc94f6b2eddae999cc9e9d14e6a757c8c38d1682368c9da10e3b7b40442c2f1fab  
bda2f164c26d736cf4307770246002fe4ba0ed78c7dd2590677306eef3ceb788692c2bd80da8a1b799880c9dc1  
bf0b5f642c63d26bfcda61180300ab3ae992e68cc8177fa454ca329f6cd06631c321b5643f6e46c38f62980e  
024bb6edf8ef18bdb5a0e9e43ea9af4ea8397136ddd7737d939e240557157137a3c3637dd75d4f91a6f775c38  
ecd678f279322738c3f1795bbe4f69db29f1587afe4ada391d765daeee23f044d45bbae2de6106d66fddc406c  
07b69156ec069d88d6f429a6e81b9917b1b8c44b7581482aa366d2aa50a164ebfe4dade4a1e75a896b49b147e  
d4b26f0fc328b8b0d861e3fc911c00cedaada8d7dcc20b1da994348c79823be0240f4462e52bf18b338139073  
7e7cb713679a139fe04014d218d1e942d241d22a4fc038eab230c25ea5eea42911b5ad6fc678387288b6faf59  
8bcabba9aaf4785da2f1c0696ad9472bee3cf23864337f36499f411f07a2047a34b5612e5469d5cc0c02b4920

c0ddff109678dd6da7aeb71457bc59c20a3064efdc2cf1519d580b919885a0a0415e5405719098c9d3bcce5bc  
23790d7c1ea99f1b19989c16006a967355253e690d06cb664978a70336dd97e5be927d57443ba1cd369f1e790  
26ca4b95e024ab160f616b85c9c26b1c51c6ec481b18a3a1f8c3e22866268603161d4562cf48702facc47cc4  
9e91a9d63886421ddd5f5734d26cbaf96cd68e5d1dac3b59ae157ef0db69bca41543ddfc8e1cad899cae05042  
9c406baee3080daaaabbc678c5eb001ca7f163aef0fb6e5e52ebd50862f7c695d2ca9f74ebce080a41b8493ce  
d3f5b212d5b3128303edfbb0a2a996a7a611194c3d8e2f0ccd4da7c26555ac1b48622ea26db483aa76295ff3a  
483f0c7dbddd6702269e65baf27f737982d2fe74eabe73ab998530b1f4e2c1b4b184dc17009a7e49163306405  
c724cbd3b065b8dbb6e0a7fe96db468fd8f36f03d962ba24f929cc8a55c6144a81dc3ddc2823a55a3b2083fdd  
c516d6e329e0a95642f922995f4f77b718ef4c3ad3b8dc601277325159f047967983d9f6abbac7089d03c5e52  
c7c57c5f2c824e81fa54f0c4e9a5fc5d9cc86a352bc7fc7c79ee80e985b524b392b567cf8ee1d4a736a43e656  
6e1680c9d6101432ae505e8761302f6968499800b1853913a76b7af8fddb7aff8571d14876ccc90bd2f15ad27  
de8b63f195e10be9d218887723f506e916347b6c5cad91c6b7acdf029dd83604e1b155c299f58a500c2532e  
fa1916d309e9a8c3f921b9b155045616b9cb16ca02b3ebdbe5e9824f1cb990514807663cd45dc42814b6575f  
08b78bef1849bebc8ca2ec5f43be4f30168898f772c31df79d3be5e3edfd59029546948f9e58f44f3515b38472  
13dfb9ddb0dd3b52bd13ef07cf91818f2c2c9500725c5c5061383e7292649ed320152d1c3eaec99d3e9c2e4a1  
b16d766c044cd47879ece22c745a6a3afbababc03383c62b7a9103554086d297caf35c01f55c7158bc28930af4c  
cf67883973c04efc91cb7e0bb6b720f2d7202b47ed62a116629019d9f5696415dc61f4c88a7b8b374faa2eb6b  
7f3c119baee7d8ef9910fb994bf59ac31654c195781a0d3f794968918658af22632bb8abblababee965ebe6a0  
b3fffb93002d54975bfb35bc5378cb277b514989728e5a737950068c343a6278b9cbdc78045fb9414a9ca0630b  
2e0972c7658e0842d3f085bb9ec576d509eaa806ed0b367be94b4476652e10e4f2aa229067496b8cc466dd8ac  
2bc92b1b51e6d8614d191aef4f0dcc1bf0491b3e271186fff1168c7853f9a07854bdc82ffa33de6b77890a2cc  
df03e4b31dc294d65699301b940b2c64b3a2a22604066513d7c9ac710eda9975a44ff087390a6b8f7b2bb791a  
7e2d0be8b1628ec5319d21b14e982eee17ef726a304228df13dff296f83c93f11b2369a21b5d6088e0d50986f  
b93d623cab8b073d75251467b5e8892db88566145fa04619034ddf05473e40e43954830584e3b68f7dba5aaea  
f2c782bf50c0aef6c41537105f321f2d2cdecef7e31796725b1df29fa851e23c674860e069c2ea89740262ca2  
b921b7809c4c1bfc2ec0d9015a83befa23a6e8f21aac2caf2fcfcffadb947d3e332208c9277a3a60985ba3eab  
62bcd991661ee20bcb37c3486b470d9a59211ed79d14167adf747091072f993ae7792fc841c9834894884d22c  
0d03977fe2006adef9b0d49ef8870007c7467f89811c3d2ea10c6a30f0cf03ed425364391457ff3ace3d98a86  
9bf402fda01e0fffc3fablaeb56c8f7e8133b3bd87342621312930e338af5f22f1da57e1cde31af6bd69deaf  
ca3a8cfc844ef18cf03eda11ece551538417000b9a124f48c02afc593d26570852e0be21325936d373f40c1f8  
abbb7c243e36b56d737be9602e4478e26b4c79a6d80c0b2da9cbfbd21d9c9b7c84bce598ec390fa2fdefe7881  
ce1cb35f0cc168b132122b5b178650c7973cf255ca0cca5ef6d8ab008e9701ca8b7f8519903f169b6615ee185  
57f12d0d4058b7a4584f436658c2b44f926d2d4458d191f1f697282bda6739d1ca8a9d5b3f08377c3b2af680f  
d9ac42a4217924adeced1baa48d3a0e50c70a5fec53aac23a8c907facb5018efb39be12764491a011c6811e94  
bfe2ebc47a7227ab6bcd72ed24ab1b9b1eb916bd21dca9ee9e9d57f8df363058a51e249675d1bb776bddb389  
29defb76a3eafde0ba22a82682e757f7f61f2b505eb3a2b4d613e4eae7cb587dbe529867f8882279732f4b4d8d  
023887f026d3e4526c81099c14856267576e0fe693993defc2724436f31bf927b65fe01beaaefeb86e6c5121  
4c9e49bdd31fcfc5a1739e964875fb19128432a5d5a77a47a2106f3b24fd066a2dcc89626d5925272e20ce4cd  
47232493a577e04e68cfdc9cc887a68c8a5d22405d33705e78331296ef0cfd98d1f9eb82a0e93b7451de020d6  
992d199e1b4588e3058130c7f0f0f1e3a72575ec2ff58667d123e75aadb65c5fb3c3dcde11c38941002ca4ff0  
9celc17004bee5c2d913336616685ce223b89accffble43537476b6c1d0da14556066718de9182f53898e9fe8  
f9fe141527424b81848c8fb60000000000000000060c151c252f",

"raw\_public\_key": "424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942  
ab8bdbad7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd3667e60  
d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693868a460cbec03f4f  
c99a4e30bccffa8a475e5395396674ebb81a94937587880f6dbd27bf1c4f5a9ee43cdd8b0e53b3b7fb49c73ad  
fbc2d4f8c54303520c29bf97e26ee57db34cd2957c893936522d0942b041d82ee3772a00570adf6545c1143922b  
0496f826a4970064b36ddf534b5f8e1c1cd0b5565ea846b45431f0618143ee89777b61179ad20295fe0a  
6e062ae6eeebc2ef38f2ac1a22dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb  
8a999ad7a83e5e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0b84c44b9b0  
a8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a083f6ae07a114  
746d1bfdccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99ddd88f48aaa4e88bfdlea769d  
82c10779f2ded796db542971ca289b76863ede5997b7e9ce183b43ccce278b10d92b87442ce0435bb1625171d  
b5554b470239c50d2a0c3a41b2a38807db070b47bfb3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d70  
8844febaa8b6ddff01ab64d59358e6505c4ec1d7cbb14ed2212df458ecef03fe03037b1505a4c9444322f5f9  
8dfa91a4cb8c45860a2dad7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891c9078f62a8  
a9646a31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef06566cb34c  
79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d545365785ead8d63aef64a87c0b  
91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fal4bd3bf177d312ee52a6da023c0572  
2a8738274dda8dlb04e99831cf57c87282a256c565c296d0524a063a41a48a83009978d98d8abf61af68e80  
13b594fe151d9bec199902c4c70b49584201743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c  
94d4c57c0860b9d7b53d4cd261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43fd8aeebe5e0  
ce2f54e3f0367eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e0894ad7cb7  
elae7ebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b3e1117e194f0a1  
e4c783efbc62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b055f4e7a2070fb096f56c415549cde74f3864e  
8b9fc27e3299724b4639986044b55928fd6972785b280c25a3e21aab814ecbf0c3cbec0914907ec907f25a1d

```
88bce3d319ae8222a35945db62af7cc75cd29c1f5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a2
4d3e26c68e7bb10e459f2577b90080359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346d
ad5b55eddb4f977b326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a51177bcb08947
6b18cba09fa8b9b46d94a2946f358eldecbl998652c58a90852423e2c85e79d19724461627e6390d1a81fb1a7
2f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783b8f718676b1defbae98ba
496c2a935e92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea6dbdd957a534ad4e790efc974ee89938a
d99d53c5b680775399326834729bb37b082e795f8d87f52e6c8a8db68e515c277bbea82a7570d4280896c987a
0608903e306c632a223c55f0ea3682039c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f048
7b2707b86286f8c4f55659b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153d87a7f482d
284b5b894cela78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509b2fe475630
3a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdaa40f91a987e4a922ca81050e5
bc3530ca85493bdf2a825374d0a8310a6860284ec3ec732326eeffcc42bbd42bc91b73e5e7c6b599d01649063
7629f3876c3e42f8db590e66a85a7838c818f78fffb4853cbef09434989803545dca87657cf7c7e7e6afa7138
2bc10fa0bb6480f243eealb861101006fa0cff3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8
ffbdcl1b0d0f961120e971015ad5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8
b425f1d73caf8496d742ed237f4c9fcd5a4e84fba7e27fbla8ael2c4f0427ae24e910d951bd8c35d61f8a678d
b01caea8ef789a95b62eelb8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5bbf6b7ecfd5
7a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177f79ee5606c9df176f025ce4
9a6e5ff51a2a412ebf86ac0f40471c96ad4c119df230be6173df530ed656cbd8069214741ecdd0271c603fb6c
4a8614fff878d33e726cac6693e938ca3fba82c4995c14a2d4af9014fe4c4c50b794cac596b52189f66a7106fb
325b526ea"
}
```

Figure 4: ML\_DSA\_65

```
{
  "priv": "00000000000000000000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "tRnlJNikgMsABVQBlXeDHxAIcclh-2IX0UdDEzPt5XU",
    "kty": "AKP",
    "alg": "ML-DSA-87",
    "pub": "5F_8jMc9uIXCzi5ioYzY44AylxF_pWWIFKmFtf8dt7Roz8gruSnx2Gt37RTlrrhamU2h3LOUZEkEBB
eBfAXWukf22Q7US8STV5gvWi4x-Mf4Bx7DcZa5HBQHmVlpuHfz8_RJWVDPER-3VEYIElPyQxFJ14oNt7jX0lp1--m
cv0eQxi-9etuiX6LRRqiAt7QQRkq73envj9pkUbaIppqL2z_6SWRFlN51IXv7yQSPmVZEPYcx-DPrMN4Q2slv_-fPZ
eoERcPjHoYB4TO-ahAHZP4xluJncmRB8xdr_-_mm9YgGRPTnJ15X3isPEF5NsFXVDdHJyTT931NbjeKLDHTARJ8iLN
LtC7j7x3XM7oyUBMwOD3EvT34AdQ6eHkzZz_JdGUXD6blylPM1PEU7nWBhW69aPJoRZVuPnvrhd8P51vdMb_i-gGBE
zl7OHvVnWKmi4r3-iRauTLmn3eOLO79ITBpu4CZ6HPY6lfbgTGXovda4lEHW1Ha04-FNmnp1fmKNLUJiUGZOhWUhg
-6cf5TDuXCnljyl4r2iMy3Wlg4olnBEumOJahYOSjafwhh_Vjir7pd5aUuAgke9bQrwiDOnb788-YRlor2jzbgCPB
HEhd86-YnYHOB5W6q7hYcFym43lHb3kdNSMxojJ6icWK4eZPmDITtBMZCPLNnbZ61CyyrWjoEnvExOBliP6b7y8nb
HnzAJeoEGLna0sxsZu6V-izsJP7spwMYplFxa3IT9j7b9lpjM4NX-Dj5TsBxgiwkhRJiIFEHs9HE6SRnjHYU6hrwO
BBGGfKuNylAvs-mninLtf9sPiCke-Sk90usNMEzwApqcGrMxv_T2OT71pqZcE4Sg8hQ2MWNHldTzZWHuDXMNGy5pY
E3IT7BCDTGat_iulxQGo7y7K3Rtnej3xpt64br8HIST1Aw4g-QGN1bb8U-6iT9kreItAJf6umW0-SP1MZQ2C261-r
5NmOWmFEvJiU9LvaEfIUY6FZcyaVJXG__V83nmJiCxUp9tHCrLa-P_Sv3lPp8aS2ef71TLuzB14gOLKCzIWEovii0
qfHRUfrJeAiwwZi3tDphKprIZYEr_qxvR0YCd4QLUqOwh_kWynztwPdo6ivRnqIRVfhLSgTEAArSrgWHFU1WC8Ckd
6T5MpQjHn0x6x8qBePZGHAdYwz8qa9h7wiNLFWBRlj5DmQLl1CVxnpVrjw33MFso4P8n060N4ghdKSSZsZozkNQ5
b7O6yajYy-rSp6QpD8msb8oEX5imFKRaOcviQ2D4TRT45HJxKs63Tb9FtT1JoORzfkdv_E1bL3zSR6oYbTt2Stnpz
-7kVqC8KR2N45EkFKxDkRw3IXOte0cq8lxoU87S_ntf4KiVZaszuqb2XN2SGxnXB14EDnpehPmqkD92SAlLrQcTax
aSe47G28K-8MwoVt4eeVkj4UESfJN7rbCH2yKl2XJx5huDaS0xn2ODQyNRmgk-5I9hXMUiZDNLvEzx4zuyrcu2d0
oXFo3ZoUtVFNCB__TQCf2x27ej9GjLXLDAEi7qnl9Xfb94n0IfeVyGte3-j6NP3DWv8OrLiUjNTaLv6FaylyzfUaU
6LI86-Jd6ckloiGhg7ke0_hd-ZKakZxUlvh0Vzc6DW7MFAPky75iCZlDXoBpZjTNGo5HR-mCW_ozblu60U9zZA8bn
-voANuu_hYwxh-uYlsHTFZOqp2xicnnMChz_GTmlJe8XCkICYegeiHURYeHA6T6B_L9gW8S_R4ptMD0Sv6b1KHqgK
eubwKltCWPUsr2En9iYypnz06DEL5Wp8KMhrLid2AMPPli0j1CWGJExXHpbWjfiC8vbYH4YKVl-euRo8eDcuKosb5
hxUGM9JvylsiVXUpIKpkZt2YLP5pEBP_EVOoHPh5LJomrLmpORrlwBKbEkfom7npXlg817bK4IeYmZELI8zXUUtUk
x3LgNtckwjx90Vt6oVxpFEICIUDF_LAVMufttzz6JUvbwOZo8iAZqcnVslAmRXeY_ZPp5eEHFfHlsb8VQ73Rd_p8Xl
Ff5R1WuWiUGp2TzJ-VQvj3BTdQfOwSxR9RUK4xjqNabLqTfCQ7As246bHJXH6XVnd4DbEIDPNa8FaWb_DNEgQAiX
Gqa6n717aFq5_6Kp0XeBBM0sOzJt4fy8JC6U0DECMnWxKFDtMM7q06LubQYFCEEDQ5b1Qh2LbQZ898tegmeF--EZ4
F4hvYebZPV8sM0ZcsKBXyCr585qs00PRxr0S6rReekGRBIVXzMoJmid3dxc6DPdpV3x5zx1xaIBx03i_6axknSSdx
ns04_bemWqQ3CLf6mpSqtTIQJT1407GB4QINAAC9Ch3AXUR_n1jr64TGWzbIr8uDcnoVCJlOgmlXpmOwubigAzJat
tbWRi7k4QYBnA3_4QMjt73n2Co4-F_Qh4boYlpmwWG2SwcIw62PeXGr2LY2zwwPR4bcSyx1Z6UK5trQpWlpQCxgsvV
_RvGzpN22RtHoihPH74K0cBiZCz7tK-jgeuW1lA7af7Kmc66fPRBR5ykTL0sa17WblkcIB_jDvqKfEcdxhPWJUWmO
o4TIQS-xH8arLOY_NQFG2ml4_yxwUemXC-QxLUYi6_FicqwpBKjCdpQtadRdyftQSKO0SP-GxUvamMZzWI780rXuO
Bkq5kyYLy9QF9bf_-bL6QLpelWMCQl0eXZaCPoncgYoT0WZ17jB52Xb2lPWsyXYK54npszkBKJ40IqfvF8xqRXcVe
22VwJuqT9Uy4-4KKQgQ7TXla7Gdm2H7mKl8YXQlSGCT2Ypc8O4t0Sfw7qYAuaDGf752Hbm3f11bupcB2huIPlIaDP
6IRR9XvTYIW2f1bwYfHKLmoVKnG85uUi2qtqCjPOIuU3-peT0othfmwKQXaoOq0-V4r6wPL1VHXVfTIYmEdVt0Rcc
UOvpOVR_OAHG9uHOZTmueK5557Qxp0oJtZCHyN-hgoMZJLrvdKkTCxPNo2-mZQbHoVh2FnThZ9JbO49dB8lKXP4_M
U5xAnjXMGKXtbfI8w6ZWATE_XWgf2VQMuPpG4wpy44yWQTxHxh_4T9540BGwG0FU0bkgrwA_erseGZnepqdmz5_Sc
```

Cs8405Xr5MbYhJLCGgXy605GqS-ooB2w0Mt87Kbbe4bpYje9CAHH8FX3pDrJyLsyasA3zxmK40mGpG7Z70ofONJtH  
Re56R5287vFmuazEEutXn81kNzB-3aJT1ga3vnWZw4CSvFKoWYSA7auLgrHSHFZdITfOrgtmQmGbFhm9kSBdY1UCn  
pzf65oos3PZWRA2twfUxxLANPNtrxpRGyvtSapw71jUagZmuyh3hLcJhAxYmnoEldbyIWvpCqSlEtVjLlyb\_nuLEz  
gvmZuV02fHxGuWgHTOMVGXpf81Rce3eoBK3lapWlwkezk3tca2bZ0tA9qbxdsbVR37kemzQ9K1e3Y00WhtSj",  
"priv": "AA"  
},  
"jws": "eyJhbGciOiJNTClEU0EtODciLCJraWQiOiJ0Um4xSk5Ja2dNc0FCVlFCbFhlREh4QUljY2xoLTJJWDB  
VZERFelB0NVhVIn0.SXTigJlZIGegZGFuZ2VyY3VzIGJlc2luZXNzLlCBGcm9kbywgZ29pbmcb3V0IHLvdXlZG9v  
ci4.hmMrKkUgZwGpQV\_WUoXUVq\_Z9WOenDZbfMmHpKritl0btWi29TC8eIyQyT1FAuW2kg3h6ALsvCrjX5tn3QKFQ  
ZYC0sBdRt0VNiDm0BjyJ4jWcomSCgb0-cGxALlODAz-njGridYfOlDpGMWHHshuKuvECv4qnX3XgZPE-6C8La43TZ  
rY08brzBXGiuyGMLq-TSmXavOeiadtpp6iTuqJDBgQSYvPB6PvipeCPlQH2ZQi8qkraxspi0lgy8Jh2aRyJ44DX2Z  
Kq-Ml-hfBJB4iHRpWmwPEH7Ed4LkBiLaqZoPccrPgpGQpyz4\_FcahrJc8CGGT05I34o5BcuZeJ7WOQvJ6mRmvYq  
IrYwoLs-3\_YFZkVdX4KU38oprMvAHjObOhY\_vZZArMnCgfYlCKrANbhOZG800BXgqow5Bqv\_oRiztGQZMrivp\_lCS  
0hELarwkWjdqyH5R747ndV26IQkeyn6y9daXRZlWxaC9KmAaDsm5-YsRVpiAAR0Qmfav51z065\_r5qZmOMFIBERVi  
9Bbm\_Z7ipJkoIL2SqVsePATfHeWB8huFpVFxdeEkJUPDuBtthax0HhxpRuECpFNJf2xA70Hp5C5VZIsi5EO2lHuRp  
ixiNkMXP5whhsn\_uv\_B7R4f4DX6X6A53lFrUfPFirTfOQvBAvMEUUTSGcPeT-F7f\_1lz34uFyN3ZT4FCeCh4n4yyZ  
Y1fSPVMNtOfK8GrLrRoWdi8gMk30oTKgb9zFkFU7uZhVEVRV86A\_060bgFSHWDz5dlXLfyCoJsbsHl09WBibTCkrM  
v6lnjh4czprro2prRtJAJB2jVwSldv2mo4wP1lFYqY63yM9I9deU4fxy6mkwig7XwcVJskg8jX\_0agATqmrKfYWMI  
4yGQ9fciYacgN8X2uSHqiPULcgQ8VUGsASaw4POdZpmcUt\_DacVLT8-qwnq6NWpm8bqm\_uUQu3JjqcHLz7zWKope  
LG\_ZY7a45IqUQpwbMg9ICE1ZNTe5nsMHAJnevgLfWk14wnvVQyRVvlSvatdUTg0EjBc6P35a4lY12vIOq2ENpA-m5  
2TfXexXK0vtZft9SY33thi4EfZABWL\_jQyio6b6Akrh6\_PgQ-bh2H2Fpu8Z3GImrbHodcbnqFpmKYlMLwxDhNKP  
xY7PpyyV8HswfEjQvLAX56stAIIG4\_owwzMMZMcFwgucAP176TwaXJqm9v2-DXisD2cNjyG1J\_rec670rv61thjiJ  
F2uZrB9Z2zoQVYnc3Y9sJMMPPmunUcXpNVZWSsPlFDoPalABoFnRbP8rO-qbNGP5N7xY2DuPRYOp3CdyxeyDPmGBC  
2556FNeLRj-PhPAkd6lfgXsQZyS9N2jHmFUIKbL8o-e3bQnqW7ebEn7zAjs\_LQ2DtGIdIneUu84hh8Aduow9ky\_aO  
pqvBumdHUUZHQiSSdeCPNeOssVBbuDd3gbcQf\_VWvplwcjTTrJPsqzQpirjfvGPFUCVAz6kd0vhFcvTdQt6DGqys  
6lXg\_VOfj6wxpKsXuXDuqwaeb4KpGniHx-23nECgK686N\_1BBX8RRAvYnksxIIXIgxgrng-y44CV9FL\_wGfP0Plx6  
JjSUFOLlgDZTc5NrAPoOztEolFbJ2Lq8gqBR9Ku9Yza3aYANAjQvAraTXza0t1j6qcmh-WtXeIlGE-8neOJtlRVbz  
T5RvPiRjZAVmu9Pgg7wbLLQNPJJoqIYp-c9mieGsDxAi75C2MlArRnCa4kJJXrupgzQzzFefWyaRkIvC2MP9MwB\_Z\_  
NY3mp3opcNlT1TdKLrlsncLUkk3qJ0Pwyr-5dsKrC6aenapBHO7G0OnA0qtI8-Oy91VqJYYcVjcOUQaxNeMtnk-pL  
JL7j3MzqNiDkc-OfRl9fcWvDmmd9Z8wtj20khL4mTdN7qTUo-PsVR7GnpqkImmEmE8sa4ZlPHA4\_IcZGFbdcwp9xu  
OndINlzWGRiKywFPQ1x26zXDEa7fOx5f01aX8dIU\_KWNAGdaZxPilqLW5qbC6dipSqf9NwblZLJs5DCiLV8nHS-QM  
26xQJVUNH22n\_3Z\_8zlSA8AX8d7j0-g1Pf7NZC8e8Ipm4B3YGpA7nn47laTbJb4OUamfgys17MV\_hPDK\_f7FF7NX  
p06-dtVYDmcs-87ZkrDuluOkUarivKULwJEtSbiikZAKirGfAOuwyCbbzygEpqYvEztABSmDYd\_F\_autklob\_0deK  
uvvRYFpVCaxeayQ7WIkpfBbMxeh9Qci7kPfgYB5H9ajWEJV3fgRk10Q1RaWyTUddQ\_jWaluiDa3GD\_t39sUrG7QhX  
c2OzlNPPNoY6-A4jFbFctXSF1muzztqy0xaworcNiHY18yeL4Cw2iYLJ1Q304NnFo3E-wIXmYF4CLxZifr2Jkd6Ix1  
w-wlsN6vyCds8JeAgeJn0\_OahklmgvRbVz8FFeidSdFqJBxGKbfZ32F\_auJwrsLyjN\_ShxTsfOfyKQy2XCfoVMko  
4eu5o6md66xBmjZvTvtITXL7f-ed0JxiSBSBkZG3mRfApZKbpdI1Lea681ZbCxrTYpxUR7MctS0Q5S9PCN5EluZ\_a  
xFeupIIBCTE4S0-ZQuIdQcQ2pn1j-4t2c04jtLE6WFI-1ASBCedlZmrZUIRegbezE0lhmifnfn32BhBu7ZcnlBCdW  
wj9hUfpEduJIGA3acXhysGs40nqRzR9imvX9CBQYJZjrCHr-wORF6svmvF5FADRgwbM7Cc9puJgLBiQwXrhD43B6  
kjX\_OXi5O2UNZFkAPr0WONBjsip8CgR6ptlu\_mIKlIrYM9kM-idJGGT0DZ9UU4LMx0-9\_2KCKkjDqgYNlrS9DA\_\_G  
P9tS3dJ-XLSlk2URQuoHm4Xubv4vwgJUS7JzAxcQWHB0HtHfOz3-tYVw\_GRbRwyODm3E-N5O3L\_R-pva9fv1PjkCN  
Mrf2IlxAXBKMLlgCxsSqhFr5yoPeW40LTxMF\_dYPNLjC3l7mRRl\_wfY\_FhvayI7hrGcyfMgWeb-cXyx5eXumt9lMF  
OD3dQtEGlIUbdE7pVXG-barWK0Zl43DtQMNQzoCK\_BLxfCsambyRRcI6E4QTfge5lWtVf8Wi4KproenWyCjjzEjJQ  
dWw4g-ae\_bjGjFzCp38RgsXtWgI\_tuzKyRF5WwjYn9VEoRXd8W2DctmBejHF2XDYZbMfKJ-384SokPX6intnlqBGM  
s0ssxriJhsFOA-vgDra6REx3DUMB8\_u\_Umc-zp4E6isX4D-eRYgElmj0ez945nqxp3Yli08mRLMW6E4OupLthfw4v  
mK3YqTAuXcnGxYrf7JqAkMfz5uAPi0SqPWDQZq7ycu9BmkMXAihMb19XBDjL7hZGDWDrRn9yBBcYlPaFPNXjMJWJH  
\_xxUKNsTFGg5-J\_WdxXi8Zn6tDMxbxqqjIpw\_FuAm00jJ2MhpbkzhEx7X85pBR47ScRgr6WJpf4ZLSFuV7N1WI3P  
Iba\_bYeCiq29fp3Shm-1bRfdJG\_lGZd97TuAMF\_QU6-KDXbv5i8kzUf1NXdJUZ-YaA0RRVNFgMGM5n0pKB5IFncAPK  
-taTzHLiZJ9uuBdP2y2Hxwbw8YQlmy2-MT5XE5Ae\_9kxuvIILSzjpfLlN9012HSnX4t28x3aWwof3E7s3jjzw7qbBt  
oUkYYpIGVOKf2EpmhEgevsLXYWpBYN3X2ZYjsrA9CL9PTvrPdyWLwKBmfh7cDjBjNXJSQLeKL7oHzicrllABzR9Ck  
kz7b24XGV1klcat\_Og4oB9qxi02zJZWz2GDtAL0hosUlHLWnrQYvqFzzdIOzGlifwIyGgoRNb44IRMzzsErxuoqkd  
jZewVc4PzruHRLV3cWK6M7ZUiWltxtMzas2sfAERY8BdS7ISLzj5PERoWyYXSW-898WD3ze5MJcpSsAYNEmPCBtdx  
F91-Qz1LxuDa8hOCQ2Wzefla2WFF5pCBaZRCaK\_kef65xRst6WFpjWZGCLZUqHBhFDLEOd7Ikbw7d9V8dc4nAO65N  
Qcxft9JDUZadS2jmQJip8GLD4P9lGS1Ry-8rHCnMN7zXDp43TfyYhSgv9uj4xKi2wmAMMYBl0n2RNemx8nt-K\_dkn  
GgYYGOyBdkg2uAUoXdxP33KfiRjbRPyqZVAiq0S45QLAixxGiDJoZrNyIscdM6lryQtXj0P067vRf6ifxC3wLv97H  
HUKergpXcAg-4\_rNj\_Zx\_xiHmfCAe2q3DGla\_DcSmu5ulOPkBMzHB9Vs8HV0E2-z44sl3Exqb5L8pMYpDnZ7QW-Q  
b1-S-zoESUy\_AKkhRWPC7GmvMJJHUR6SRGSK0X2KyszkEYoe-8NhwpvLrYnNuV7QknBS91KH2q8C0B8FKqcY40  
S5ILkImp9iOGIXYl5ZVRleoDBpH9BootWH2az5l7c\_e-vfBGs7XpudoAq5wzhe\_-AMBvKPCm0BoCX5B\_NGUasXvEW  
obqUb6lmpKcuVJdzVtexk-m8Jfvmcd8ooPJED\_oosY5\_S1LuHoc7GHLnoYdDVb2FhIPhOJCLQCef-Y3dtNthQEO  
534Zg7R72nSeSQhdqlhCBUSc50U2oF90lOnV9z5hsfNwIxdU9bdoXRYfMosmtpmDfGxAem0s5iPJ0EJ\_8szlaX2p  
i6k6VP-ci-n7J8pEBwL2R3c-ei2iqB7JdLi7Gg6iXVMPqIFTxswh0HbgGtyZXgr-Am91XRszm\_kAlqAHTAJ7B-0Z  
5bJgMGEY2StBdhGzel\_gNPVaxemC3DT0904GbCU2Z3avUHcedebI02\_MdILdQxyXbw145KjqC15CqeaG--6x6Wzpa  
uSjrFQRuz6Z5UyibW6Ay9R3P25c-gwmaRM8rPW5YkQtQdfzrtvGZ6wyhIcBXvbpU02OoChfRDF4xI2LvnaW3g6hQI  
UGe5lueI13ArYRAhZC0LHKPuVfv50KeMqxYRtcN3YK6Ddc1t6lrsA7MUlCAKzOGsiQ7aNYNBQHOV6z-W4-ws\_DnZK  
YRMz0D\_hwbeHO0ZKhciXng5VDCX4hyb47LExm05NlmfihN3iHEkX\_19rIgunfkSb9gd9B\_AaazAttBEPPLtbsoZne  
QXBR13PWiDpC\_yXiLTWAdl3AOBYHzBMKeJ4hplUqsAGTaGSztbpvV92wz\_YX9kMEucHMu5hoM-TJbuWoheiiiKSFb

NRK\_g\_rqXZo1UZjDOnPhPGJxOnlJBPP94Zvvh8sKLOpOd4qeOMLbnYKiaG00a15x\_3fBXq-KI0Y310JfgDdCaKAQ0  
DUX71HN6XDOLvU1Iwh48iASJHDQGDmjhcs8YoeX9omwPiYhcbGJGzEVrn3H7h24eIf\_7bVRpicMhjwghB0xtqTT0e  
Vam118krl-5kem7Dr2Kyqm2HpEwbi3KPXKYDXQRbHElEhazMCYr2wnjx\_Bx2ai2uZa8uQyJn1zh1cjWHH0TicL2eA  
yc6YPKfKpmc5QwLrgT0ddQDhvXkCkN50fOR1Sbl56iFoAl8goFl3QA5wBk51vsDsquEt7nlz6sGTHzknENb-eEayr  
Xnw-Q5FueFwqzoJpUrEYDXTxgOU8XVhrPv0Ot-BO6ORfzn3\_lgREchjhrC6RdF01NNqzyzVG0BdckywvAnzUGskWd  
CfP62dKdx461AIRVPd3xG4tViaQ79GAeMvNqSeCLXbOyqfnJwhOT2fgQzLwxcjltqGBBd3Pfx2d5-10WiL\_mis0ve  
n6golqaLq1EQsveb9AJpkYgJxdBeyHZXxNLMh4\_XAUk1ZIs9F8CzlvFEVcAFipev-cFyRvsdcNI2-HK2nOGkypEcu  
VATyLtA0jKeyPtE4TJ3\_l8KXltEZjWycQAd\_8Tj9is3wisC8bfzjll8UBjFZp-rzmCr8kA4cZih9gl27TiCmhyKhg  
MfDUIUmuDL\_Rn9DLxEat3Ebl1SW0ToCciNtKTH9oO-wnkPd-jglHCooLcg-K\_QkOTptJNZRFbXpooKqwh5Z9qsCxu  
rZxnS\_MscnE0qTa4EqrLpiDnj4FBs4q9SEPlKequfYzFmJQisliwsReutf6pHmsvRmz9gx5vd6NMIkI05IeLNDElv  
lOGD04mlvR4ZISdmdHaAgaW9\_AUPGx0vPlRqe36cvebwUYSnzdbZ7y1s7PH7GXF5r7zNEZy9bHmXvsjb3N\_u9Bken  
wkQfZGS6ez0AAAAAAAAAALGSA1Kzg7Qw",

"raw\_to\_be\_signed": "65794a68624763694f694a4e54433145553045744f4463694c434a72615751694f  
694a30556d3478536b354a6132644e63304643566c46436246686c5245683451556c6a5932786f4c544a4a574  
442565a455246656c42304e566856496e302e53585469674a6c7a494745675a4746755a3256796233567a4947  
4a3163326c755a584e7a4c434247636d396b627977675a323970626d63676233563049486c76645849675a473  
976636934",

"raw\_signature": "86632b2a452067018f415fd65285d456afd9f5639e9c365b7cc987a4aae2b65d1bb56  
8b6f530bc788c90c93d4502e5b6920de1e802ecbc2ae35f9b67dd0285419602d2c05d46dd153620e6d018f227  
88d67289920a06f4f9c19768b94e0c0cfe9e31ab89d61f3b50e918cc071ec86e2aebc40afe2a9d7dd78193c4f  
ba0bc2dae374d9ad83bc6ebcc15c68aec8630babe4d29976af39e89a76da69ea24d4a890c1810498bcf07a3ef  
8a97823e5407d99422f2a92b6b1b298b4960cbc261d9a4588f8e035f664aabe325fa17c1241e221d1a569b03e  
9107ec47782e404895aa99a0f71cacf829190a72cf8fc571a86b25cf02186b533b9237e28e4172e65e8fb58e4  
2f27a9919af62a22b630a0bb3edff60566455d5f8294dfca29accbc01e339b3a1cbfbd9640acc9c281f62508a  
ac035b84e646f0ed015e0aa8c3906abffal1233b4641932b8afa7fd424b48442daaf09308ddab21f947be3b9d  
d576e884247b29facbd75a5d16485b1682f4a9806834a6e7e62c455a6200af44267da579d73d3ae7faf9a999  
8e305201111562f416e6fd9ee2a4992820bd92a95b1e3c04df1de581f21b85a5517175e1242543c3b81b6d85a  
c741e1c6946e102a453497f6c40ef41e9e42e55648b22e443b6d47b91a62c6234a9973f9c2186c9ffbaaffcled  
1e1fe035fa5fa039de516b51fa4522b4df390bc102f9845144d219c3de4fe17b7ffd65cf7e2e172377653e050  
9e0a1e27e32c996357d23d530db4e7caf06acbad1a16762f20324df4a132a06fdcc590553bb99855115455f3a  
03fd3ad1b805487583cf97655cb7f20a826c6ec1e53bd58189b4c292b32fea59e3878733a6bae8da9ad1b4900  
90768d5c12d5dbf69a8e303f594562a63adf233d23d75e5387f1cba9a4c2283b5f071526c920f235ffd1a8004  
ea9ab29f616308e32190f5f72261a72037c5f6b921ea88f53572043c5541ac480b30e0f39d66999c52dfc369c  
54b4fcfaac27aba356a66f1baa6fee510bb7263a9c1ca2f3ef358aa2978b1bf658edae3922a510a706cc83d20  
213564d4dee67b0c1c02677af80b7d6935e309ef550c9156f952bba5d51383412305ce8fdf96b8958d76bcb83  
aad8436903e9b9d937d7797c572b4bed65f4fd498df7b618b811f6400562ff8d0ca28a8e9be8092db87afcf810  
f9b8761f6169bbc6771889ab6c7a1d71b9ea16998a62530bc310c79ca3f163b3e9cb257c1ec59f123a959405f  
9eacb402081b8fe8c30ccc64c705c20b9c00fd7be93c2369726a9bdf6f835e2b03d9c363c86949feb79cebbd  
2bbfad6d863889176b99ac1f59db3a105589dcd8f6c24c30f3e6ba751c5e93556564ac3e5143a0f6b5001a05  
9d16cff2b3bea9b3463f937bc58d83b8f4583a9dc2772c5ec833e61810b6e79e8535e2d18fe3e13c091deb57e  
05ec419c92f4dda31e615420a6cbf28f9eddb427a96ede6c49fbcc08d2fcb4360ed8087489de52ef38861f007  
6ea16f64cbf68ea6abc15267671d4c191d089249d7823e710eb2c5416ee0ddde06dc41ffd55afa65c1c8d34eb  
24fb2aa99a62ae37d518f154095033ea40f4be115cbd3750b7a0c6ab2b3ad7183f54e7e3eb0c692ac5ee5c3ba  
acla79be0aa469e21f1fb6de710280a1bce8dff50415fc45102f62792cc48231231832ae783ecb8e0257d14bf  
f019f3f43e5c7a26349414e2f580365373936b00fa0eced128d456c9d8bab8c2a051f4abbd6336b769800d009  
42f02b6935f3034b758faa9c9a1f96b57788d4613ef2778e26d95155bcd3e51bcf8912590159aef4f83def06c  
b2d034f2608a86829f9cf6689e1ac0f1022ef90b6633502b46709ae242495ebba9833433c5579f5b2691908bc2d  
8c3fd33007a67f358de6a77a2970d953d5374a2ebd6c9dc2d4924dea2743f0cabff976c2ab05ba69e9daa411ce  
ec6d0e9c0d2a4e2f3e3b2f7556a25861c56370e51106b135e32d9e4fa92c92fb8f7333a8d88391cf8e7d1d7d7d  
c5af0e699df59f30b63db49212f89930e7eea4d4a3e3ec551ec69e9aa4226984984f2c6b86653c76b8fc87191  
856dd730a7dc6e3a7748365cd61ab20acb014f435c76eb35c311aedf3b1e5fd35697f1d214fca58d00675a671  
3c896a2d6e6a6c2e9d8a94aa7fd3706e564b26ce430a22d5f271d2f90336eb1409554347db69ffdd9ffccf548  
0f005fc77b8f4fa0d4f7fb3590bc7bc2299e6e01dd81a903b9e7e3bd5a4db25be0e51a99f832b35ecc57f84f0  
cafdfec517b357a74ebe76d5580e672cfbcd992b0ee96e3a451a462bca50bc2312d49b8a229900a8ab19f00e  
bb0c826dbcf2804a6a62f133b4005298361dfc5fdabad925a1bfff475e2aebef4581695426b179a610ed6224a5  
f05b3317a1f50722ee43df8320791fd6a3584255ddf811935d10d51696c9351d750fe359a96e8836b7183fedd  
fdb14ac6ed08577363b3d4d3cf36863af80e2315b142b57485d66bb3b6acb4c5ac28adc3621d8d7cc9e2f80b0  
da260b2754373b8367168dc4fb021799817808bc5989faf626477a231d70fb096c37abf209c0ecf0978081e26  
7d3f39a864d682f461573f0515e89d49d16a241c4629b7d9df617f6ae270a2c2f28cdfd28714d21687f2290c  
b65c27e854c928e1ebb9a3a99deba419a366f4ef22d5cbdedff9e0f427121206c064646de616b02964a6dda48  
d6511aebcd596c2c514d8a71511ecc7136ecd10e52f4f08de44954cff6b17deba92086c24c4e12d3e650b8875  
0710da99f58fee2dd9cd388ed2c4e96148fb501204279d9599ab6548917a06decc4d3584c8859df377d81841b  
bb65c9e5042756c23f6151fa4476e24881a03769c5e1cac1ace349ea47347d8a6bd7f42050609663ac21ebfb0  
39117ab2f9af1791400d18306cccec273da6e2602c1890c17ae10f8dc1ea48d7fce5e2e4ed9435916400faf458  
e34126c8a9f02811ea9b75bbf9882a522b60cf6433e89d246193d0367d514e0b331d3ef7fd8a0829230ea8183  
75ad2f4303ffc63fdb52ddd27e5cb4a593651142ea079b85ee6efe2fc208d44bb2730317105870741ed1c5a19

dfeb58570fc645b470c8e0e6dc4f8de4edcbfd1fa9bdaf5f5be53e390234cadfd8897103104a30bd600b1b12aa  
116be72a0f796e342d3c4c17f7583cd2e30b797b991465ff07d8fc586f6b223b86b80261f32059e6fe717cb1e  
5e5ee9adf65305383ddd42d106d4851b744ee95571be6daad62b4665e370ed40c350ce808afc12f17c2b1a99b  
c9145c23a1384137ea7b9956b557fc5a2e0aa6ba1e9d6c828e3cc48c941d5b0e20f9a7bf6e31a37d90a9dfc46  
0b17b56808fedbb32b2445e56c23c8df5512845777c5b60dcb6605e8c71765c36336cc16427edfcel2a243d7e  
a29ed9e5a8118cb34b2cc6b88986c14e03ebe00eb6ba444c770d431bf3fbbf52673ece9e04ea2b17e03f9e458  
8049668f47b3f78e67ab1a7762588ef2644b316e84e0eba92ed85fc38be62b762a4c0b977271b162b7fb26a02  
431fcf9b803e2d12a8f583419abbc9cbbd06690c5c022131bd7d5c10e32fb859183c0346b9fdc8105c6253da1  
4f3578cc256247ff1c5428db13146839f89fd67715e2f199fab433316f1aaa8c8a70fc551a334d23276321a5b  
933844c7b5fce69051e3b49c460afa589a5fe192d216e57b353d562373c805afdb61e0a2ab6f5fa774a133ed5  
b4457491bf94665df7b4ee00c17f414ebe2835c1bf98bc914675357749533f98680d1145534580c18ce67d292  
81e481677003cafad693cc72c8649f6eb8174fdb2d87c706f0f184259b2dbe313e5713901effd931baf208952  
ce3a5f2cdf74d761d29d7e3d67cc77696c287f713bb378e3cf0eea6c1b68524618a4819538a7f61299a112a7a  
f4a55d85a90583775f66588ecac0f422fd3d3beb3ddc962f028199f87b70325b8cd5c94902de2885e89f389ca  
e594007347d0a4933edbdb85c65752a571ab7f3a0e2807dab188edb32595b3d860d300bd21a2c5251cb5a7ad0  
62fa85cf37483b31a589fc08c8682844d6f8e0844ccf3b04af1ba8aa476365ec157383f3aeeld1955ddc58ae8  
ced952258bb71b4ccdad36b1f004472f01752ec848bce3e4f111a16c985d25bef3df160f7cdee4c25ca52b006  
0d1263c206d77117d97e433d4bc6e0daf213824365b379fd5ad96145e6908169945c00afe479feb9c51b2de96  
1698d664608b654a870611432c439dec891bc3b77d57c75ce2700eeb93507317d3f490d465a752da3990262a7  
c18b0f83fd9464b5472fbcac70a730def35c3a78dd37f26214a0bfdba3e312a2db098030c6019749f644d7a6c  
7c9edf8afdd9271a061818ec9b0e4836b805285ddc4fdf729f8918db46962a655022ab44b8e502c0231c46883  
2686519f222c71d33a96bc90b578f43ceebbbd17fa89fc42df02eff7b1c750a7ab8295dc020fb8feb363fd9c7  
fc621cc7c201edaadc31b56bf0dc4a6bb9bb538f9011e6cc707d56cf07574136fb3e38b25dc4c6a6f92fca4c6  
290e767b416f906f5f92fb3a04494cbfffc02a191158f0bb1a6be6249247babe9244648ad17d8acacce4118ale  
fbc361c29bcbad89cdb9593b4249c16bdd4a1f6abc0b407c14aa9c638d12e482e42263fd88e1885d897965546  
57a80cla47f41a28b561f66b3e65edcdefaf7c11aced7a6e76802ae70ce17bff80301bca3c29b4068097e41f  
cd1946ac5ef116alba946fad66a4a0ae54977356d7b193e9bc25fbe675cf28a0f244603fe8a2c639fd2d4bb87  
alcec61cb9e861d0d56f616120f84e2422d009e7fe63776d35386a384a39df8660ed1ef69d2792421750d6170  
152c739d14da817d3a53a757dcf986c7cdc08c5d50ef5b7685d16059a8b26b699837c6c407a6d2ce623c9d042  
7ff2cce5697da98ba93a54ff9c8be9fb27ca440702f647773e7a2da2a81ec974b8bb1a0ea25d5329408153c6c  
c21d076e01adc995e047ff8033dd5746cce6fe4025a801d3009ec1fb46796c980c1846364ad05d846cde97f80  
d3d56b17a60b70d3d3dd3819b094d99ddabd41dc79d79b234dbf31d20b750c725dbc35e392a3a82d790aa79a1  
befbac7a5b3a40b928eb15046ecfa67953289b5ba032f51dcfdb973e83099a44cf2b3d6e58910b5075fcebb6f  
199eb0ca121c057bdba54d363a80a17d10c5e312362ef9da5b783a85021419ee65b9e235dc0ad84408590b42c  
728fb957efe4e29e32ac5846d70ddd82ba0dd735b7ad46bb00ecc5357002b3386b2243b68dc8d0501ce57acfe5  
b8fb0b3f0e764a611333d03felc1b7873b464a85c8979e0550c25f88726f8ecb13198ee4dd667e284dde21c4  
917ff5f6b220ba77e449bf6077d07f01a6b302db4110f3cbb5bb286677905c1465dcf5a20e90bfc9788b4d601  
dd7700e0581f304c29e278869954aac0064da192ced6e9bd5f76c33fd85fd90c12e70732ee61a0cf9325bb96a  
217a28a22921413512bf83faea5d9a355198c33a71e91c62713a794904fa7de19bf087cb0a2cea4e778a9e38c  
2db9d82a26a0d346a5e71ff77c15eaf8a234637d4e25f80374268a010d03517ef51cde970ce96f535230878f2  
20122477501839a385c4bc628797f689b03e262171b1891b3115ae7dc7eel1db87887ffeddb551a6270c863c208  
41d31b6a4d3d1e55a9b597c92bd7ee647a6ec3af62b2aa6d87a44c1b8b728f5ca6035d045b1c494485accc098  
af6c278f1fclc766a2dae65af2e4328cdd738757235871f44e270bd9e03273a60f29f2a999ce50c0bae04f475  
d40386f5e40a4379d1f391d526e5e7a885a002fc828165dd0039c01939d6fb03b2ab84b7b9e5cfab064c7ce49  
c435bf9e11acab5e7c3e43916e785c2ace826952b1180d74f180e53c5d586b3efd0eb7e04ee8e45f7df60  
4447078eladce91745d3534dab2cf2546d0175c932c2f027cd41ac9167427cf674a771e3a94021154f777c4  
6e2d562690efd18078c5679a27822d76cecaae7e727084e4f67e04332cf0c5c8f5d6a18105dddcf7f1d9de7ed745  
a22ff9a2b34bde9fa8896a68bab5110b2f79bf70269918809c4d32ec87657c4d2cc878fd702e2b5648b3d17c  
0b3d6f14455c0058a97aff9c17246fbd170d236f872b69cel1a4ca911cb95013c8bb40d2329ec8fb44e13277fe  
5f0a5e5b446635b271001dffc4e3f62b37c22b02f1b7f38e597c5018c5669fabce60abf240387198a1f60976e  
d38829a1c8a86031f0d42149ae0cbfd19fd0cbc44013dc46e5d525b44e809c88db4a4c7f683bec2790f77e8e0  
d470a8a0b720f8afd090e4e9b493594456d7a68a0aab01f967daac0b1bab6719d2fccb1c9c4d2a4dae04aab96  
98839e3e0506ce2af5210f94a7aab9f6331668d08acd62c2c45ebad7faa479acbd19b3f60c79bdde8d308908d  
3921e2cd0c496f94e183d389b5bd1e1921276674768081a5bdfc050f1b1d2f3f546a7b7e9cbde6f05184a7cdd  
6d9ef2d6cecflfb197179afbccd13363d6c7997bec8dbdcdfef4191e9f09107d9192e9ecf400000000000000  
000b1920252b383b43"

"raw\_public\_key": "e45fffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b468cf  
c82bb929f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f124d5e60bd68b8c7e3  
1fe01c7b0dc65ae470501cc565a6eldfcfcfd12565433cafedd511821e2e9610c45275e2836dee35ced69d7e  
fa672fd1e4318bef5eb6e897e8b451aa20ded042b2aaef77a7be3f699146da229a8bdb3ffa496445967e7521  
7bfbc9048f9956443d8731f833eb30de10dac96fffe7cf65ea0445c3e31e8601e133be6a100764fe3196e2677  
26441f31751fbf9a6f5880644f4e7275e57de2b0f105e4db055d50dd1c9c934fdddf535b8de28b0c74c0449f22  
2cd2ed0bb8fbc775ccee8c940665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee758185  
6ebd68f26845956e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab932e69f778e2  
ceefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a3655098941993a1594  
860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8dac1f861fd58e2afba5de5a52







35a112c0266f79b9ae7ac996feab2c5874c65f59a72bf671b568d06e57b89f6fa168f48050f869e9fe0b95490  
487597e1746d7f54ef04eca32710bd4655a2269fd9afdfa0c7630c09ad59273d5d76f6bc026b623e5fee4fe39  
78efb4fdc5f905d8a346259cad9cd8ad826cdea818fccca6804bd78ddddd70d46d723ec63980fe7bb2eb8dab84  
692cb6f6a560eb80381dc0d5ded38d1de896772702f99637f6b9a9b207be86e2a401187bb250f68230f7840ec  
f9787bb6073e2e29f1287cd73bdf1dae8302fcf23f942305c4c9807aba037af66f8b278003c98a30084f9ad3f  
2e4c4b31eb1b3f20170c70f0310f71932a4e0065a2bd79eedc70e59f9cc261aed96fd7ebec86be2490789ad0d  
ffc76f4cccc28ed675a769edf9f8d6e9fd78d59393687fb19b641626f70bbbed7c6496a3a1393be6751f533e7a  
f8f20f9ef32c7b58b231feb4231aa407ecf5e0be7921c449a537ab58871b4cef2f8b1212b189ddc9e207b0ebe  
8135be534b30f25ce0aa33371a94971da4b6b78bb2cb708035b539f3706348d1f6ef0e2ab9c741f1ffce5bd34  
c20c2ded6272c583188d2f48404cbd10f6aa759fecb1e5b87c755573db0d86ef17fec7231179f47a19b0bcda  
fadad9a8b20dfe1d2792cc2d78d13c76722739d6c31563bc938fb07a0bc5d96d3a4e852141815b526ac74fa21  
0c48ce1e2ffa3faa682191aea55a476a6cd7e0ab42902180b1444a2e08302c17608b5831daa4c4008dbb54f0b  
4ce566c069ed48d4a9c5b542816f3156cde0d7323bb071cccc98ee35672248e873b5907d02a153a57e5777c67  
67fd75e833df46813c2abe44dc6492e8de4487f4ab1d1377d4ae273d28869c6630ba4865e65676d9dc9ca0998  
a0082e95c78314d543068f6fd38a27bdbcb98f8b5fefaf21e704e4bc8ac7ed46ea5c03eb700cf0e549b8a1c50b5  
d051bd7c2588938f7c9f5499e7b95430b1e567a2e36b4a55252829d7fb319c7edab4e19108fa2a784c96ec102  
7f19f571448132b6c8c4441a7a7488ddda530b84ba0221120c95311eab37660b1329a70365117eebbb7e0240c  
c5052ec723e0121c2a175053c762b88943ac7b965d10239c4b8f8d39a1a57ace097a1631c7e93c36abc8a085a  
21a18a14b621cff49369707891e06e508e41970b26490c8f5c038bcb2e62a72d24591f563c42fed3dfa3539f7  
5dacbc7918919642220a01da483a2c0413360e424c6cc30dfc502858a57ffdc20d30bb57c1659a7d44beb6794c  
4675524e813a27e3807547d0bc16e91242d7925b01f0a8cf03f5c6e867710373ad02e53816f82a21b2c9f359e  
7d586ec0590c0a1780a6755e1723981ebd866d251e20a0a5b2dc08e05beb325797aa7c2746596c534964cc751  
ff341d49e39c8b6f8a903549779189c5732b841abde352eddf9f9fb67f20b9c27d30078994ac96c8250b3428c  
65a714c05c91c897a18ee58f908557062bd733444a9d73ed89a637c62143e46e1cb3723c6a8fd2df0d90d03b6  
cdfb4e6c033f67c51a803b6eaea79e0ecfe4a3b22c5dc951d51683ea716149958c59ab43f1085d8e5896aa3c8  
d972d54998d3de2b27c2d67e0059b78dff6f804cd491dfae0308b4c8983ea1c574b4414df8ca772fbb60dc492  
49f8dbab9c43357016893f7a4b2eb28c0a8de635157b717e20ad60d5a52d37e2ebf5b87dcdcccd1f40825d5  
6b948e60015118e8988f6000dd157ce92a0f0ec1d5459890317ee861a0d29f7305331047886e1918b8438d1df  
534e685c93f2f11317b000b0bd7da766e5f1d4a0816a7af878be4c8dc8fdd208abd5c7f98aa0e882772387ef5  
032f60e71a7c1c630a8eacd2e2a7c5e86277b20e1317cd8b9892e8509647d55143dcca07ffdd678d5856eaab  
93f55df72ff4c909146de54393aeed095cbd9fcl1a24b7f7950cb80eb423ed114cdc21e59593b2a5fcbdbf1613  
810fd63c8dd45e39bc5bd02d71328cfea87d2deadda75089ca7d4529e0b5b64fb887fc38cb9531033386255c6  
a155af95447b2154354e6d163b752bef91f248b5068f3e620365c8c497cfcbe61930d0cf08387308310f485bf  
a23c31bf2d01900e801352a388c97212ef58b6a81f5082f08831433a7ca8c0df910cc462b36d61f532325eeee  
540547b6c07c738b010daf7384f8cf01975761101e556e8639848dfd049ee5360bb9b62bb38aef0fc84970dad  
3e78c0f3413573042abe52805b5aec545bcb43142f5d44a9c1d2b6cdf3ded20907f02ebc78e78f598beadd0fc  
1faa676560eddfb7a83b61795bc29b6fbc47c6e9097139dbb85b54a8b446a37f2fd6ba7db528f1c5da5fe367  
823f8fa39adae0bd23196f689059e2de3cfcbaad6bec710464156cd72be70d5950075953286feb605f6898746  
586750e3aef767b0e80136453c1ab388ff5462bfc0316ed78937ea235dd883e9fedbd66f9060b542272ac9747  
fe3109a27a89403fcl1c2380ccb1e3f199077582aa565fba4621092c5665f2f7803f5ecfdaf86878ec045a780e  
a3751bd32333cd02fef8b4eb9386f51fa7a5f3bb81c55fb0de38c905ba4002dadfcc5123bf561bef2d32c4057  
7dc487736162c69444279d917abd0d2320fb715299c1043defb582a20fec3190a6c0e484360910388889c122c  
4a13adc73031a0969e3c1a9008d8467c4c4d59c848d9ca2441ec57b02034fd5872b4cf75185d5fb14e6af1aea  
d0e1727db42db39877f01d674558f7b59b0e0f10363e3f505d82a7c0c7cadd1618233541424f57596476777d8  
0a6b8dfe6eefcfd0515196c8e99c3cfd2ebf2020b0c16202b3337484e525657a4b5bec3cad2d4d5d6dd000000  
0000000000000000e232e45",

"signl\_diag": "18([h'a201382f045820b8969ab4b37da9f0684e42647eb8a0be8b5b661ebf5d76f0583b  
f5b8d3a8059a', {}, {h'68656c6c6f20706f7374207175616e74756d207369676e617475726573', h'26572  
37b7520fd4cb8803f69a6e4ab613f4816420cd38e6474e548a370c6f0a18851ce8b7bb1b43c658b795303d0f2  
2d23aad9afc7077877ab77d7cc92947bcf800e09626d7ceb809f74d2dc435200b272ecc92a993901087a42eae  
aa6b9009df00f26055e6032ccca2995bf9c455e93c95adb9dda970ba07d778a9b4950169b289a86ec272bb810  
f9506b960941fa4ac804de49cb80f9bd54f51adef76670c06f94bf948ad7675ab28aa3254944753aac0cddb85  
94752a438552e846fb476be3e31df0c91222db5e5d70bddb05b624a78103654d4e9ec514f6be91cfe8fa3b852  
9b2659a89e70227f35d0059362ed51c7523bf4a8ca7ceb0da6216bea77576548cd98f5ad6f87326facc8b308d  
ebce4461f1f2c4b190bd4950eec52cb66da70c9913e8a476826a0ea05edd8f2d3ca53e485ffcebc4e7ae33aee  
b1d8dc3ee6b8d09cea138377ceeaed4fef57d868c16311e18c64b9df501791a6142085083850b3ad2e7490129  
8c09b7fc4d87a660031e955b39cf9e6fbbbe3cae5b36360f6b61f904771d55d542fbc68be5468738f5b8c44eb6  
24da535a112c0266f79b9ae7ac996feab2c5874c65f59a72bf671b568d06e57b89f6fa168f48050f869e9fe0b  
95490487597e1746d7f54ef04eca32710bd4655a2269fd9afdfa0c7630c09ad59273d5d76f6bc026b623e5fee  
4fe3978efb4fdc5f905d8a346259cad9cd8ad826cdea818fccca6804bd78ddddd70d46d723ec63980fe7bb2eb8  
dab84692cb6f6a560eb80381dc0d5ded38d1de896772702f99637f6b9a9b207be86e2a401187bb250f68230f7  
840ecf9787bb6073e2e29f1287cd73bdf1dae8302fcf23f942305c4c9807aba037af66f8b278003c98a30084f  
9ad3f2e4c4b31eb1b3f20170c70f0310f71932a4e0065a2bd79eedc70e59f9cc261aed96fd7ebec86be249078  
9ad0dfffc76f4cccc28ed675a769edf9f8d6e9fd78d59393687fb19b641626f70bbbed7c6496a3a1393be6751f5  
33e7af8f20f9ef32c7b58b231feb4231aa407ecf5e0be7921c449a537ab58871b4cef2f8b1212b189ddc9e207  
b0ebe8135be534b30f25ce0aa33371a94971da4b6b78bb2cb708035b539f3706348d1f6ef0e2ab9c741f1ffce

[illegible]

7660b1329a70365117eebbb7e0240cc5052ec723e0121c2a175053c762b88943ac7b965d10239c4b8f8d39a1a  
57ace097a1631c7e93c36abc8a085a21a18a14b621cff49369707891e06e508e41970b26490c8f5c038bcb2e6  
2a72d24591f563c42fed3dfa3539f75dacbc7918919642220a01da483a2c0413360e424c6cc30dfc502858a57  
ffdc20d30bb57c1659a7d4beb6794c4675524e813a27e3807547d0bc16e91242d7925b01f0a8cf03f5c6e8677  
10373ad02e53816f82a21b2c9f359e7d586ec0590c0a1780a6755e1723981ebd866d251e20a0a5b2dc08e05be  
b325797aa7c2746596c534964cc751ff341d49e39c8b6f8a903549779189c5732b841abde352eddf9ffb67f2  
0b9c27d30078994ac96c8250b3428c65a714c05c91c897a18ee58f908557062bd733444a9d73ed89a637c6214  
3e46e1cb3723c6a8fd2df0d90d03b6cdfb4e6c033f67c51a803b6eaea79e0ecfe4a3b22c5dc951d51683ea716  
149958c59ab43f1085d8e5896aa3c8d972d54998d3de2b27c2d67e0059b78dff6f804cd491dfae0308b4c8983  
eal1c574b4414df8ca772fbb60dc49249f8dbab9c43357016893f7a4b2eb28c0a8de635157b717e20ad60d5a52  
d37e2ebf5b87dcdcccd1f40825d56b948e60015118e8988f6000dd157ce92a0f0ec1d5459890317ee861a0d  
29f7305331047886e1918b8438d1df534e685c93f2f11317b000b0bd7da766e5f1d4a0816a7af878be4c8dc8f  
dd208abd5c7f98aa0e882772387ef5032f60e71a7c1c630a8eacd2a7c5e86277b20e1317cd8b9892e850964  
7d55143dcccc07ffdd678d5856eaab93f55df72ff4c909146de54393aedd095cbd9fcl1a24b7f7950cb80eb423  
ed114cdc21e59593b2a5fcbdbf1613810fd63c8dd45e39bc5bd02d71328cfea87d2deadda75089ca7d4529e0b  
5b64fb887fc38cb9531033386255c6a155af95447b2154354e6d163b752bef91f248b5068f3e620365c8c497c  
fcbe61930d0cf08387308310f485bfa23c31bf2d01900e801352a388c97212ef58b6a81f5082f08831433a7ca  
8c0df910cc462b36d61f532325eeee540547b6c07c738b010daf7384f8cf01975761101e556e8639848dfd049  
ee5360bb9b62bb38aef0fc84970dad3e78c0f3413573042abe52805b5aec545bcb43142f5d44a9c1d2b6cdf3d  
ed20907f02ebc78e78f598beadd0fc1faa676560edffbd7a83b61795bc29b6fbc4c7c6e9097139dbb85b54a8b  
446a37f2fd6a7db528f1c5da5fe367823f8fa39adae0bd23196f689059e2de3cfcbad6bec710464156cd72be  
70d5950075953286feb605f6898746586750e3aef767b0e80136453c1ab388ff5462bfc0316ed78937ea235dd  
883e9fedbd66f9060b542272ac9747fe3109a27a89403fc1c2380ccb1e3f199077582aa565fba4621092c5665  
f2f7803f5ecfdaf86878ec045a780ea3751bd32333cd02fef8b4eb9386f51fa7a5f3bb81c55fb0de38c905ba4  
002dadfcc5123bf561bef2d32c40577dc487736162c69444279d917abd0d2320fb715299c1043defb582a20fe  
c3190a6c0e484360910388889c122c4a13adc73031a0969e3c1a9008d8467c4c4d59c848d9ca2441ec57b0203  
4fd5872b4cf75185d5fbl14e6af1aead0e1727db42db39877f01d674558f7b59b0e0f10363e3f505d82a7c0c7c  
add1618233541424f57596476777d80a6b8dfe6eefcfd0515196c8e99c3cfd2ebf2020b0c16202b3337484e52  
5657a4b5bec3cad2d4d5d6dd00000000000000000000000000000000e232e45",  
"raw\_public\_key": "ba71f9f64e11baeb58fa9c6fbb6e14e61f18643dab495b47539a9166ca0198131c44  
f826bbd56e34e55db5e5e2d733485e39ea260fc6000c5ea4ba80d3455cde53b46f34482aedfd5450fc2e1ba4f  
25d15f9c144242fb39bb52287189030c50498e1717b7c758b190a6748ea9aa3f7acaaf2c7cb526ed717c9f79a  
eb84214fa5cd8ded92a0c3fa1558810f12c7050a367708d196cd24e5af974904aed8e4ce8872e8696b0b7bca5  
0e452cd7d30ea9a4adac0311d672c6bde8496240b07431463708895cd9bafcf31632d7397649388fdafcbf7d30  
5a3de9a495eca7433a8f83ba0f0b25c413c6e39c96eb7d691b34d37ce37f1eead1cf217e25ef34eefcf3f7c60f  
84b8edfdde8405d4f832576c61ef98e0a2f128da187700953924f686b94614705bcf53d33fedd4348edddbdf28  
b5065e1f20775043e85cf931f829179363a1a7e7404a838ec00086b0976386fe637c98244757e3f769ddd4467  
471bfad670f9a05f8246ee50a7b1eaf87fc4069c3ae2aa2033258117792f0bcd49e083fd1bcb7496abff29cc94  
e4868b21214ed316525399a610fbdd4a80e7c80715f29578e2a84bb40bddd9f47a11b6e7da118a1b658d359  
e8aef55eb46b5376b5b655979984a922beebfc59bcd600d5309dccc72dbf0787db8ba757b537cleaf5c0f50e  
a4bc9583549e2829a42c28cac248c96d78124c47159b18aedd754aba17b19d430fb78f633ea9d26f54a9bd50f  
8d8f6b73594f828976e7ea09c53bbb9f11a56c9507fb89b9a5ebc037a37267a95f85b8d64ca97192b10a66f41  
7b3f61fe9ca57130a48fd925eae2ab5502d571c8a51903c1d398f4c1f76a7e11743976afdbc697f23094a3cd7  
61ff9685de32e09fb3c28add453490300bc7c89dc01780096071722945775f264e1b0623bcf4619c712c83876  
1205d87691b75ef360196cbb9e9b92a0d4c4ed62326e5024d77510b8ee2c7426cc22eae209dc9f13bde6bf08f  
5e7181bd3b459450b451a51539a715c21d67dd330eb5970db00d9edbf2822b036fa13bafefb86d8dc78866e3f  
8d43e53d78cca5595a6faf886b5dc112f1cf4adcf8a75800d90b48883af97316fe1506873fc157e570eacbf2  
22868d14234101966afb6bf9940829253a953ada89cf756b6a849f70ac9838e69faa50bba75e3e89c2adb57e  
86d088ab9b04a28e670709172243ec5e0008a5ceaf3f8722f487302596ffdf755ad1b82a49c34b3469515b46aa  
290cd86ee38ea7a9be3f103610335b531cca333ddfe32b14510f4b07ef95fc6684e8c454a92c10dbb5d59c7a7  
c63fb305fe881967d99e669eb632840582560bb403431d40f75a4954908482278292821f4ea91e42e78fa48ca  
ee3c836146dcfd738d117e92e9a15137d28e8e6a4b4622650cb413504cb3a335d44beec5746c1c294b1e8cb99  
cb608d928f8ce3563632c521f23d13c61a8f61c01df8c96c7360db4f3c68aa5d2fdd342a62ff3459c11638942  
1ab43e8584c45882b50e6e4e96db6f0b8fde890d5dbfadcd88690b449e64240ddb2023747f308363e301aa777  
57169fc6150628d5920b5aa1ab1c8cbf44cb00e025d7879d72b479e3af5311c785725590da9c89b9fc3b84507  
69554eb44d203eba2bbaef9cad2237011c2ea44eff00f299a48ffe28ca93ddf85f76608242ef8d6cc24610a1e  
2078fcac4f9385c314905ecaa82e553916d94d1a7c1ec652aa08897083daa2ebbb1775fbc471ae27777d7904ea  
9f1b92bcac3d8a3158426087b645b1108f0d65fec93789c053743ca14fd63d05e98b652df2b9c2ff9ce05f194  
0703ffb273f80e0e2732eca9960d981b4cfd3b7bb8045b3c3830546b9dd8db0d"}  
}

Figure 6: ML\_DSA\_44



```

{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "key": "a5025820b788acf242f1f1d6532926d816e76e1636874267f2a48c84c4e65789ab80cc020107033
830205907a0424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942ab8bdbad7d
708abbbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd3667e60d539ebe449
30219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693868a460cbec03f4fc99a4e30bc
cffa8a475e5395396674ebb81a94937587880f6dbd27b1c4f5a9ee43cdd8b0e53b3b7fb49c73adfbcb2d4f8c5
4303520c29bf97e26ee57db342d957c893936522d0942b41d82ee3772a00570adfb545c1143922b0496f826a0
a970064b36ddf534b5f8e1c1cd0b5565ea846b45431f0618143ece89777bb3f61179ad20295fe0a6e062ae6ee
cbc2ef38f2ac1a22dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb8a999ad7a8
3e5e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0b84c44b9b0a8bd831fcf
f2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a083f6ae07a114746d1bfdcc
bee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99ddd88f48aaa4e88bfd1lea769d82c10779f2
ded796db542971ca289b76863ede5997b7e9ce183b43cccec278b10d92b87442ce0435bb1625171db5554b4702
39c50d2a0c3a41b2a38807db070b47fbfb3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d708844febaa8
b6dddf01ab64d59358e6505c4ec1d7cbb14ed2212df458ecfc03fe03037b1505a4c9444322f5f98dfa91a4cb
8c45860a2dad7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891c9078f62a8a9646a3138
7a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef06566cb34c79bc0b25e4
095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d545365785ead8d63aef64a87c0b91a2e55003
83956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fa1c4bd3bf177d312ee52a6da023c05722a8738274d
da8dlb04e99831cf57c87282a256c565c296d0524a063a3a41a48a83009978d98d8abf61af68e8013b594fe15
1d9bec199902cd4c470b49584201743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c94d4c57c08
60b9d7b53d2cd261f332a1851565d52ac37f008747cafe320f363d99beb6e4117db43fd8aeebe50c2ef54e3f0
367eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e0894ad7cb7e1ae7ebd4f
8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b3e1117e194f0a1e4c783efbc
62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b055f4e7a2070fb096f56c415549cde74f3864e8b9fc27e32
99724b4639986044b55928fd6972785b280c25a3e21aab814ecbf0c3cbec0914907ec907f25a1d88bce3d319
ae8222a35945db62af7cc75cd29c1f5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a24d3e26c68e
7bb10e459f2577b90080359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346dad5b55eddb
4f977b326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a51177bcb089476b18cba09f
a8b9b46d94a2946f358e1dec1998652c58a90852423e2c85e79d19724461627e6390d1a81fb1a72f9c7edc4b
d747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783b8f718676b1defbae98ba496c2a935e
92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea6dbdd957a534ad4e790efc974ee89938ad99d53c5b6
80775399326834729bb37b082e795f8d87f52e6c8a8db68e515c277b6ea82a7570d4280896c987a0608903e30
66c32a223c55f0ea3682039c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f0487b2707b862
86f8c4f55659b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d8415387a7f482d284b5b894c
e1a78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509b2fe4756303a9a3659fe
32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdad40f91a987e4a922ca81050e5bc3530ca85
493bdf2a825374d0a8310a6860284ec3ec732326eefffc42bbd42bc91b73e5e7c6b599d016490637629f3876c
3e42f8db590e66a85a7838c818f78fffb4853cbef09434989803545dca87657cf7c7e7e6afa71382bc10fa0bb
6480f243eealb861101006fa0cff3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8fffbdc11b0d
0f961120e971015ad5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8b425f1d73c
af8496d742ed237f4c9fcd5a4e84fba7e27fbl1a8ae12c4f0427ae24e910d951bd8c35d61f8a678db01caea8ef
789a95b62eelb8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5bbf6b7ecfd57a18fb7557
d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177f79ee5606c9df176f025ce49a6e5ff51a
2a412ebf86ac0f40471c96ad4c119df230be6173df530ed656cbd8069214741ecdd0271c603fb6c4a8614ff87
8d33e726cac6693e938ca3fba82c4995c14a2d4af9014fe4c450b794cac596b52189f66a7106fb325b526ea2
1582000000000000000000000000000000000000000000000000000000000000",
  "key_diag": "{2: h'b788acf242f1f1d6532926d816e76e1636874267f2a48c84c4e65789ab80cc02', 1
: 7, 3: -49, -1: h'424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942ab
8bdbbad7d708abbbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd3667e60d5
39ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693868a460cbec03f4fc9
9a4e30bccffa8a475e5395396674ebb81a94937587880f6db
```

[illegible]





bafa512b6fc81f7702857d350744958be7050aac6d1f040bfd866df38727df3bdfd1ff3896f68550dfcb520c30  
8fea4d1716790b1b6d51ef9c815e05d537c64460893be9d82c350393ad15992e1c1ba16fff59a87c5d6fa19b4  
e88e2c433e0e96fffc6a8a7d49f84769ff9057bef8daf353e8516a852247e2f17ff13c81be266fff7c916c9b72  
6a83058c66ac0366335ee6e7b079095cf367bf79a3cc38da62d53e84a3b1a4ca97f40dd147e0d6c90dec5aa93  
c178096884fc7718a675eee7900e4cb3ccc3601a08bf0003c3a029ca62a1924cc5bb83b29817f892c5a5e7253  
abeb536d58d885008914a94bb2747f8a22478f35490d6f9693d0ff50073289adda762b62823a9e4b134478642  
d9f1c44e20559bc5506df6baf76056c9cfbf15bb7134cd95f29527f006a0a49ebc4bb8e8ccfe3757alf61c83a  
25ef44d2856f15d13272de73bfe726df6a775b18157c85d419d20a7614dc18eb74dfb26af89fb2996ebcefe37  
dbdff37d3d2408411f9aad75f6d2cael22bf90e51ad6c4f6bbf85c50a50e78afaf86fa5e367d00c4fdade2714  
8949fb8db485eb7950d63c90013313db410ecf9b314a94c102dc8bf7e9e27ffdbedd64b9441bc687a53487473  
9c52759d1af213bf8ebd916e456561973f822e26aae6827b06ec4fcd45c146ac5c6637168e024c188f93315dd  
57e7fb8a12879d1a83fbd2421368aldbf54898b487951c24ad2535a0344d7f7380808d44b207ac16b490c5115  
5d275da3b863f775a13c8483f05c76aa6b64e8faf96fb2ff78672361d139183abe3957c6f431b342779e2fa96  
b07de7a530469d7096c01567c0c1ec7d3556d0ac636a9482a84aef2087ad2c2bbb5fc49739c16d771203529b1  
134da0d0373a4e2305741711a21016a132cd213fe2867b37465a103b68e16ce6ada0cbe1da2a0590f2a6dlafa  
8e06e29b4dc3c9ae21ef6ca67e3c34a0e8f43dcaa0882d24e7fcc770ff28450efa19b88de83e8327e499b1555  
29745473ce9e1da81e9ce0fala816100c8d08741bfc8260fb0a6624c373b5823b587b34d16dlbddd6a03501f6  
e8ccac59b877ee751cc841f2290eb8c37fbf119b93dbe6b0a700e3ee8e7a697b80d1a304a71e3c1ebe734a412  
a8403c80d9ca3096c3a764bf8f6524427efd2648210a387fddcfbd05e4bbb6c353437750324b320458aaff555f  
e41765bb827c3c43d80bee1ef45dd3993d06ab1245e9c95aa7976f54ba17aa031c8694e9b167a986cc289e534  
f1359f14ae335f7c41683dc85ccaf4ee2b4c1cdd2116552f396ac8d6567e0f458c8cc0342086c31c0f8bffa3a  
c0d31677b10494c45e68e66432b3f270a25cd389c126943b1d877ac6396d88a2df32c74eff79b9dbf1504b3cd  
55bcbffa8ab2a16979dfa53631a5d7d948bdc26c37eed9d2e2855338d029365b63b6b22abc21led2ac1d39745  
50d2d783be4c8b286fd8868a7c221ba15a527b1ccd14c50fc85907016930691f44f593a9c4ed3a1cec24f0267  
35b719275fe27af036d234baeb812c5d60babae2f2b7032f0ad34a09cf98537a8bb623f266ee28151acaa735a  
f300ad6ce3e33c982b46db37479d5e3ad808b22b1453451dee5dbac26a03ae64990917b7060ee48281e1b8c48  
6218a8c20d371f621fdd4466254c5d3cab08fc07dc96b41c83d755377fe0363d11969802431cd4f2ff5cb92eb  
362591f12cf6f69fcd25727309235aa75acdd915c5a09403194a27b2f3b11cf51240ffeb0a457d383dd49503d  
3021ee19e83ef1b5d7f0aa243c7a4b69978e1ef33911ecc320351a1e459eel672be88db2f0f5755758468a45  
09d067f5edafb45334179d1317a4130e45320019cdc3113222c7933f0d12f3a71b23461cb9ebf072c3f700179  
7c9124bb7f39778c7b393eeadeee2f6fd9ed76f39d16291722bf9bf68761e307438649ee7e0042e7801e8c46d  
741fb216b13ab8d243c608d7d5cc6cc758d429c90b9ac1dc1275314bd506fbd4e41767c8e8ec02282375b4f9e  
2d77b78c1c00dfd527c07506d0803dd2b9963535281cb9473f03c37fc34b22aca3fea6630dc1f53e7ce938c9d  
be3550076fd724675107f2cbbdf186389f189492f6388da43baf6f9ea72982f665dcb1ec9f861021ee974abb8d  
0e36da8187dbb5dbe0c7100f0c07fb6c0702e84e9591ee3c6cd9ca2482079556559ed691dbd97dc0bb1f052d6  
4a938e260795192a876f97bf34097eb4380cb16e7415f58021fdf7dec9df8e521575b62d618bfc331b7efc3ea  
92394f73a0808df15e8794818649d9675edf3daaed3c5170a843d448bd1ec5d2e8e5dfd4254e334f4ad27d73b  
614fe0f8542a0a644f6f824422e8e1e10cd125b9363da6f015354baa244921f8960ebc44f97ad1a29330ac6ad  
bce3269922e9a1990feb9e4c89a7e34368a04b79f5db62cda84af2ba028594de966674fa11ed21634922f8e5b  
4dbc0b9c9c899881dcaba8d6724d114b231b1dc3088337a45070f5846c742f6184b0f0a1e55fe87bf37822cfc  
3ddb356c397ef85d9c1c0c65db191a9d03469096c2ce42b919145708e3ee8b35e8d72db1c738d3a4389ae996f  
9604ea6903e61ac0bbe56c8ba108cda00d1bdcc6904644705c9a858adc8cdc08f4449ef11f4d0e28550586478  
ac6c8a8c8aed3927ca90e3b31fc8f5722aa68ad028642c14706b8ab0e413201305f9f1a899f2ddd5fb6eff998  
5d0e57009956bc24f1d2c7b420eb3716a284df6408e38cedc4c7ec1c11c205c8567cda8b12d4d8d97691015be  
532160a5a1731d8af5bd17a35f0d958ca423abfd1c6346f9472ba7d7aa70b845ff343acdf9153aa939bcd101f  
0578fafa84d4cc77c5b67eff3bdbc5bea27b703d4ca3cb5c4f4943855ff512517b2c57535bcc7726e7c2cc73  
9dc65cbf805b0181672ce1324ea5578f9af0378be281c2a3b8dfad5775a4249bbe587c06077eb20c1ddab672d4  
20c6bc8d048b461b92bddee4249408f132e3a36e63e8ebd8dced63ef150da21c8264bdc65379a39f0331895e6d  
589444d9dbd56f7626252d7145905dab7ed44ab0d14707fblc19198196da8fc7388056a7a59fb0e19cc05d88c  
e6a60802c73f9d785b48992318ae993397044f43c38709c319ef5a8e68a452bc5b79bd86ae50981e58f7cbc58  
c7e17946804ab019c18a570c499e8b425a600201ef63a40f7d918b60ec9eeba668201cdab4624c35fdc014cdf  
af2e7749e056f195fleefc1949420e5569c461bc26f888blaca0418552ad2dc1c5b62e6c972b60ba643344d52  
cbdade3286497595a5adc1c40d0f10366cc9dbf9fb0e22445d5e7ba14c759fbfd1d400000000000000000000  
00000000000000006080f181f25' ) )",

"raw\_to\_be\_signed": "846a5369676e6174757265315827a2013830045820b788acf242f1f1d6532926d8  
16e76e1636874267f2a48c84c4e65789ab80cc0240581d68656c6c6f20706f7374207175616e74756d2073696  
76e617475726573",

"raw\_signature": "d5bd2448903e4f81fb949158eefdeb93e2f40e58d3ffe5703d23954aeb547b2f49022  
6b7e4bc617a90156acd6afa662c0a5fe83bel1f9e2d458436f9b9119c853c71fa7c7591b6471d9d68366d5bf12  
833c182ac927f7f0edd816e52ecea715c66e71e35029083fd26d0f16040eld7a73b78950429fae8229af04951  
04549e2de909d6f8be09fc982e08425da663c181e862510b647f2f679ec16b7226fae6a9b90d8131c780a98  
4b231c45811156470c143a5a9a611248532b574d40c0ef9728264892ad97d523ca9146a8f965996dda13bc7ea  
cde9040a7745a92790c2ec6672d8a665761495c873ddd4b9dc347db786ccfeabfb4f584bae9086f43639ade01  
f6c81a8f15d3c01ec9aaf0b04699c38163de65967cc921acc66935cdbea43f393d9f65303a4640c081a6073f7  
62fd78c532911ecc60400688e329d7bca72d24fec7c8cd307130f0dfb37ce333470501d9e2ff16810ede1fc81  
1873fe8b38cflc656d1927c190d240c0020514b9e71f6ad14fee3baac3444111c6a1a1676dc92036e481c35b9



```
"raw_public_key": "424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1feab443f0942
ab8bdbad7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2cbd3667e60
d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693868a460cbec03f4f
c99a4e30bccffa8a475e5395396674ebb81a94937587880f6dbd27bflc4f5a9ee43cdd8b0e53b3b7fb49c73ad
fbc2d4f8c54303520c29bf97e26ee57db342d957c893936522d0942b41d82ee3772a00570adfb545c1143922b
0496f826a0a970064b36ddf534b5f8e1c1cd0b5565ea846b45431f0618143ece89777bb3f61179ad20295fe0a
6e062ae6eecbc2ef38f2ac1a22dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866ffa9683beb
8a999ad7a83e5e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0b84c44b9b0
a8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a083f6ae07a114
746d1bfddccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99ddd88f48aaa4e88bfdlea769d
82c10779f2ded796db542971ca289b76863ede5997b7e9ce183b43ccce278b10d92b87442ce0435bb1625171d
b5554b470239c50d2a0c3a41b2a38807db070b47bfb3e7d10f3cd979d69963c8d79f8029cc4a48eb04fcb3d70
8844febba8b6ddf01ab64d59358e6505c4ec1d7cbb14ed2212df458ecfc03fe03037b1505a4c9444322f5f9
8dfa91a4cb8c45860a2dadcd7515350bb6d431e49a6b8f5ba956e682b0e513321a97d1962602891c9078f62a8
a9646a31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef06566cb34c
79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d545365785ead8d63aef64a87c0b
91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fal4bd3bf177d312ee52a6da023c0572
2a8738274dda8d1b04e99831cf57c87282a256c565c296d0524a063a3a41a48a83009978d98d8abf61af68e80
13b594fe151d9bec199902c4c70b49584201743c6b53103d2fd24bdf078dc90b5a188b4f8d772179988d0416c
94d4c57c0860b9d7b53d4cd261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43fd8aeebe5e0
ce2f54e3f0367eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e0894ad7cb7
elaefebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b3e1117e194f0a1
e4c783efbc62c9f81c21562d0d34a5f042b5eaaaf32f31f95c5b055f4e7a2070fb096f56c415549cde74f3864e
8b9fc27e3299724b4639986044b55928fd6972785b280c25a3e21aab814ecbf0c3cbec0914907ec907f25ald
88bce3d319ae8222a35945db62af7cc75cd29c1f5d98fcb93f750dc3031076979bb51dfc37d23e8eea78073a2
4d3e26c68e7bb10e459f2577b90080359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420618783346d
ad5b55eddb4f977b326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a51177bcb08947
6b18cba09fa8b9b46d94a2946f358eldecbl998652c58a90852423e2c85e79d19724461627e6390dla81fbl7a
2f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783b8f718676b1defbae98ba
496c2a935e92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea6dbdd957a534ad4e790efc974ee89938a
d99d53c5b680775399326834729bb37b082e795f8d87f52e6c8a8db68e515c277bbea82a7570d4280896c987a
0608903e306c632a223c55f0ea3682039c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b2629ad30f048
7b2707b86286f8c4f55659b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153d87a7f482d
284b5b894cela78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509b2fe475630
3a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdaa40f91a987e4a922ca81050e5
bc3530ca85493bdf2a825374d0a8310a6860284ec3ec732326eefffc42bbd42bc91b73e5e7c6b599d01649063
7629f3876c3e42f8db590e66a85a7838c818f78fffb4853cbef09434989803545dca87657cf7c7e7e6afa7138
2bc10fa0bb6480f243eealb861101006fa0cff3275621943cc58eb4dc3a0428a5e425670fe82268de71c511d8
ffbdcl1b0d0f961120e971015ad5f448886b802e3fac11672319d487c84f1001339cb969784cb57344f2807f8
b425f1d73caf8496d742ed237f4c9fcd5a4e84fba7e27fbl8a8e12c4f0427ae24e910d951bd8c35d61f8a678d
b01caea8ef789a95b62eelb8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5bbf6b7ecfd5
7a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177f79ee5606c9df176f025ce4
9a6e5ff51a2a412ebf86ac0f40471c96ad4c119df230be6173df530ed656cbd8069214741ecdd0271c603fb6c
4a8614ff878d33e726cac6693e938ca3fba82c4995c14a2d4af9014fe4c4c50b794cac596b52189f66a7106fb
325b526ea"
```

Figure 7: ML\_DSA\_65

```
{
  "priv": "00000000000000000000000000000000000000000000000000000000000000000000000000000000",
  "key": "a5025820d9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd565247a166cb4fa0107033
83120590a20e45ffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b468cfc82bb929f1
d86b77ed14f5ael6a65368772ce51912410105e0456975ae91fdb643b512f124d5e60bd68b8c7e31fe01c7b0d
c65ae470501cc565a6eldfcfcfd12565433c4afedd511821e2e9610c45275e2836dee35ced69d7efa672fd1e4
318bef5eb6e897e8b451aa202ded042b2aaef77a7be3f699146da229a8bdb3ffa496445967e75217bfb9048f
9956443d8731f833eb30de10dac96fffe7cf65ea0445c3e31e8601e133be6a100764fe3196e267726441f3175
1fbf9a6f5880644f4e7275e57de2b0f105e4db055d50dd1c9c934fddf535b8de28b0c74c0449f222cd2ed0bb8
fbc775cceeb8c940665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee7581856ebd68f268
45956e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab932e69f778e2ceefd21304
fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a3655098941993a1594860fba71fe
530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8dac1f861fd58e2afba5de5a52e020904f5b
42bc0874e35befcf3e6119684768f36e008f04712177cebe627607381e56eaaee161c1729b8de51dbde474d48
cc68249ea27162b87993e60c84ed6cc6423cb3676d9eb50b2cab5a3a049ef131381d623fa6fbc9db1e7cc02
5ea0418b9dad2cc6ccd4e95fa2cec24feeca70318a751716b7213f63edbf65a63338357f838f94ec071822c24
851248885107b3dlc4e924678c7614ealaf038104619f2ae372940becfa69e29cbb5ff6c3e20a47be4a4f74ba
```



"sign1": "d2845827a2013831045820d9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd565247al66cb4faa0581d68656c6c6f20706f7374207175616e74756d207369676e617475726573591213e132b492fca022d5fd1d2205f52dbf1ad1aaef3ece4622b4e3875696d64d66dccc74df743c1b85552a0f3c1bdaaa8f789a15fdb3ce6329021f5815316cda1da5b012f1ccea4a47ef7e93efff319048ac9e3b6ed46cd58c6557af1b340da3bd7966f1588f8bd88e05383ae12a7248db3aec96ba5d9afd1d79d62865eee04cac9cc2176ae585ae914d614805d916c142b4969be7ad95a44bf9c154d19bd41d8a3882ad6f0b0802d1e037c7579453a0606bbbb31db164fc607646477572c63b71720f8d47bbb7615dd264f5829f726e22740cb3a1e1b5e381c4f692f7ecaa0979ae17aea3139d733491fe213eeddc5f68e06ee71b80f14ed693f407ce6e199cb3edb048d3e2905ce75b31bd6837a1d4b5eeffa35431d0ca407200e60768b2dc5b0370e91a6c03c3d0e5fc47225616034f55fb0a30a66fd2074847be3c1230b93650d119492efc20338af0c4cb6a176191d7c5bbc7427f6c09cb9b49a0d73e7f026cf3855547fc7ca9369733313963ffe4647e155a93cfa5403edebfc7842e75dad9ae2accba720487e476ffe3bc0a60cf32271429242023d0d0a8f6e4e77a874afd2074a11ff20bae28d00fd5d990f839ca99c6db28a55da94a785290a6b536893a237224639717ba5cf833d57db2cca0a7aeed874597c6ee71e0dc35e06851e9d2bd022c37b5fbcd2a4d5e8daea98a44cb9c97df43a0aa512005358c8d5d5db88fba610e47d5a863f53f9ec7a8f3cb0b0ec2f02b1dfe9867a1437e84e941392b149275e868b959c58b9e814fb618c61208cb683881247bb0dcab96e84a77e0195b4e93f693c1e98dcb99e495632f6cd5839d3bcccdfa2bf6b26921759d0a293595a96e6ddd42c83d8d9a7b10a001b34f47c20fd46d1e09100e532e5b1900b89f14400bbcdd5ee0cf61alca353398a498da488b0f117effcf999f5aafe4a587deaa3ff78cc431637adcbba4e40ec385fac23e8176b74e0e750460f7d2002bf7465944caa2708835d3849199732090b7c514575311ef9999c9bfcf737a4d906af914d0507f5a7c2e61ff12359999d173f88db9ef85a6d71ac2e3a8074bed9472e00aedac26c48ab9c2d1lad96eeffe6e200686efa17086317a541ffad5c8b5707279aecb12ca48f7e7d755e8cdc2bc990c6391abf9351c2f5305bda2c57bf54e419dce477947a64de07eb0432e5f1cc87234ed673fa810d562095d0d0eed260bef5f3c3daed8506756acb9059257b025471d8df2d4e697a3e7c74c47081b569519e1de636a971668a376b4d84d95c30a554894475be8f01bda7c6d78989572aea4c4e976a0874a04b406e79e176163dccc1ffa7a7e9bd6ef6f854128097aa760ed3f36ad279f7ea4ad6003f43cfb75de79c0bf8113a6f788e35e92f30185695f4abb18e924b29abf218e708977cb2776a7abf46a41e46afe24863eed4fe890916f95d5b1fbe6cea096c

eb4ad478fc994214f59c5e68c8b9695c27f8fada32c90ed324925540912da750451f033359177579e4e4a04e5  
d5b9bfa72616df63df20f17038e7d4bbe61562583046c35e3a71a0f596f119ef183786ed76e1da6d3be98277d  
b1583c8f2c8784c08f5c098abfd31baa9fc6abdc0cc441b6f93961b6630c45b9e7dda60d88be7c9577b6fbc5e  
df65de4ed0b53f4377ce83b1e55c4d62015569b96ea094644e0f9cbe89cff4c539f77c629a5101c259c56cb9d  
31e20160dfe28386b37e610c2db9ecf6a000bfb2a85756e585ae6b97915e5113970946df068e6da7f0af0a488  
02b9e0464bfac7e0c6b7dee953665061ac7486d9eee3bf21137383e97eb393a708e91a94f5012fa1d072c04f5  
c5ca2bbf894e7b275805fe5d81341d75b9f7fcb89b3ff7da2b623c35d717d0da7180e258384ff39a914c2f30f  
893af4e1520d64a15bb0997b852f3ec6ca398d245361fc2297c83867f388c8aa35e704d3f7081a961c528751f  
aa64fd7efbcc03bed69e99ae1517d499117227cb08254d7b8aa079530af39fb19b246d45a4d41a9955095636c  
786dcc3c30c817ee3c8e60689fd9a494c9e774463df7b884a78dfe80f1e247b3f122401b0834e54fdeb57d783  
5f0409126983e40d8922bbd54981e2b651cc3fdee9193468c041201c2c472749300250628225052f935d37ab9  
dd8e466b6a3acb63ee93023013443ddeb91347b84eb6ecf37423996d682967a5aab7ccaaa73a690a9cbd45b15  
ee38f2ae698aac3cb2117ecc9160870993a3e50ea7647b0c03cb5f6daa290492dd693a0b8a9a9759d0d977b66  
2d45c4af5dce95084062f7a0f39d0bc3bdabaa31d8f815047244303e6a6e5d977ec757a56797f0630ef1d4f02  
f7a0e7680c0865c4404c97bbf7014bfa64d0f89b02a2b981f616c0e16090c4b7fe9998a0232469b0c059d3daf  
f58af6148cee567e52f1a41730b28d6af79358ad3679cf4c3dec0df780eccc91d004a4ec0a4d20cc6771dbb3f  
42da69dc2140994c228a60adc0e97438a2332db657e91e5b7f5029541d13ce8456d93bb4933522c94e16ee476  
6af28b5754b5a74c71efb6ff445dclaed5f3e21cfe512cf9862489582925c763251376279f69e633a43aaadcf  
4c104744cfca747f477claf8c18f65109b06680cd392d14e3e0ed0ba117643c8794bc8d036e85222d543063a0  
1f91cb9bceb80d884b1305d0065ef355d6f64be4893816e0e9be111c65c9cb1840774ddd4ed5906ae2a73c7c  
a6103ecd3bb506747681e192dd6c259b66dc63c39dbdc33dac1d564b54db4d8de935370abca642e05c6e95ee8  
27fb71d6086691bc6d1be2a0c7e491ce22163d3e8d48541cd7aca76eecc93f4e02ac0179cf7073d5000b3ff33  
8d096bc87eada3f4019fdf1a5d12470a33f65c2990c217680710069de75e0338d1e26c179b1cf9ef853edaaab  
2c0519026b3d9f574b82b5bd316686b26c9e9e87870041fdfala5c538cb98cb39200856b4c9bdacaalc7717a2  
2b883c066ca0f78229cd59362614361cc5ec9e76d836d2dafc1ed51066afa7297db869508cc80543b1efcdcc62eb  
7c4ffabe3fafbc02f4802b4992ff0be194ae123880ceee6187e08c7db96b22438ac4bdabadd8aba7af68b8e2a  
c0c60c0f9aad5e4elbf886db18212e9cb46d8bc201e4ala6fb231d91a309dbca30b6b1269ec31bda1bb6b6d8f  
f41d84baf7db7ac30de5ad5d9259398bbfb5ffbb89cce88a15f0f7413c9c71487b56eea23573697a583fa57d3  
537588ba5558363d8abd679f2968dbca3ff00b141d68d5baed53fa66480029f46f6b195e3dc99a0e09f990841  
c62735db8e4b6b867ee416cd946b65fae48acd2c580c5ee461fdc78c2d671abb657f9296f976cb74c0249676a  
111e7608785ede2acde6f8af297f88ce9ad0e6b4cfdac1c586519042ac700a4178f5c23add6634c26588f47bf  
b7ec9e244ae8c71382042c24606410ef598ccfcaa459923e748d608caf3c82dd141c8eb32a500a03bb7fbd5d6  
28b625fecdd3d9399254d7c569ab1418c6af0db64009f09d457e287b0e8b83bf40d529379464df999d7519a454  
bb3fa9684f398c965c4f980061d33fd8883c5ad2964806f27dfdb09458b1bb2daaced0fbc0c68d46d62224f63  
725932b58ae0a694ec7fa0d4e5fcdcc75840b467e12514f1cd006befcf3410cf7a5c81adf3d29cd93ef5680c1a  
953daa0645273d0f5fdc8e6e0f8c632b67a674fb4f390c392720c6dfc83f123ae4f8420b91217ad71f406b1a  
4c7f2c438ffff7844a097cdfb00a2f1a94ee6bdd597756a754681111d66040c13a661b978440b05ba8c16e2a42  
55ebff56e5adada6fb92292d501d30e351f4fb5b907d9f1510e9801489da0a3cf4997eed6df4fb06b86f81af3  
735781513c6654e030a03e358970fa129fdb8cb49365a86f1cdd1a9b5f966794c8bca163c3af148406c24f0e1  
49da338e6a1fb5f365b1a6bf0fe426ec424823588dcel1dfe7de3b3aa740d27fac9b6d9c60909b4afe2f88dde  
858069e330e6f9a7ecc779022d3925ea0bd73e67041945e04691152683453f3126cb3699b607dd598af05fd44  
1c157bb3b8d69243705cd1e71442b502b7ea987c8837a3bd896e5bf2796052a23d302c70b23a62383278e1f3c  
878c2bdcb68524c078fc73148f227951566c19248240d972d5547350909c63d6f505ad889884fe9710154d2ec  
05aa15a4f734e5b88480916ec73e1518fbd2605954580ec2b0a8f9c4bd4d075461b6b3015c344e83382c36b16  
1e57a6c3933e98209ce308190531f85f5d5fd9451d37f40f6f36af830b376ed2d48ab20b2b58b7c6e5956b7d4  
142b19ccb19a88db70e5829047751950e2975bb4d0e9991fc3bbcb4fa5adf2d9d1e25e4ded5396731bd2808b82  
27a30233cc7a1ab7759623357547e46060a4c6c54a8d24116680186ca97291afd32be4ffdc9bealc4b1ad80a3  
e7be17fb5585eeb72dfc303655040993f12f58d21d3ea499clecacf70725f2e1334509c1e75ce657300fd85ae  
0f44e470336dbd5df32fbc0a8ffbe3c66058e45ac5f1b0ea3889313214b6b2ec98a91e6414b33dda04d9c418577  
07bbdcf4763ee3846c7f4df034eldc8fefc8a2a5dcd9f91940cdcd1f7b98b93c08bc9f1c198e80fcde8a5eff  
e4ea4363a56cae57de4a7248fd8bde5767f1ae699b5bd998d9f613306346472e96954dc32baccd31c3f44b0f1  
1b8e6810bb3f27af7de6a57550288f56015b1b76f1c1e492d5b998493b72a38ba4f2619b891aeeccfd96c27fe8  
0b958e08728581ca4d6e7da5f2760b48734a049e8fb29aa6fff373911d712091ef6bbbed204da3b1237c1195654  
c7f66aa6776e950e7a27aed6c9a4ffbebe76671ff1dea7b1ee5d0434c976d2d23bb481b6d80d242a2c942329db  
e051396d0a9add08068634f6c7f8aadfd55e4109cde60f693229f605d71f896f5e1c9d3b94fb9a497a9b95596  
0307811296f2ed263ad57780c6f2f96b42eb71e817bbed0654000c6bc20d3087f7971b8d517c00cdf97322942  
85c6faa24b405e3b31e6fb856b57aabaee81e72a8876f06cc0fbda5ca4479a5ceecdee7b5bd0fff8f8c788e2d80  
3dad28ca110f6013672323540b94eb5a7638116cfec790f2d899d7f6bc075cbb78ad925845bc75b8086078356  
b0c6dc722283e774cb7a5ee24a6b976ca6dcc04fef3ea10e77cc50a0523ab4df32971a19c9c6e889edb99ea9d  
863e7f9922d02303b80a29899397f4abacc5ecf6da98574e2ee2afcd18077063d7419e4ee3671891085217c905  
f6cefcb2041ee6f49df05151152f45609a0d06d951b0351431651bde5b5434c06b1465097267cd5b76f182c135  
3ee94e6ef98901cdba4b6cfc1dda01628ff86b21e2be53da4a8c2c9fclb50b28ada2836959ed1398c70018b5f  
3c35d9f3c8768af0966a0e8ee6b16dd17455acccd377fd259379e7e22f187876db740c3c09a0307891484f9b1  
2da66916d9d4018ac34b9d70a094a655ece0282839a9e60b8cea041316803b262a4928d375889017f3da58b97  
21ac9d7a4e69b06fb26d46a904b062728286ee2e44c18354be39252482e5135fbfd1ea4f85dfc96b63e0fc881  
5a3a0f1be7476e60712a566911663159e74838f27a0068b2131aec8653b5f697ede4dd8c769234ba5d018ede3

20aeace49e263844b93d3c2410af9c5df83c0e7eb617930eea8a272e16a6d58e6ce1ce9a3b42ad94436abe73e01b95839038d5430676ef6a7a3c77cd541fe860d40bd9414133a8983280e139161d85dc0c395eac1ffc6fe52d637fd5f327d112f8ed15172925b0a21334d8b5dbaeaa1bdbfcf9bcb8c9bd72b58aa6745f07fae50343191f90983e4d138a278f46433a8c404565c4d15a55c4d61f396444b639bf7191515c558155bf2a09576e7b3376236a23baeb2f7826e1b5e95e100bae7d0b9226864839d04f2145cf0a0c0dbb0194f2224aa63cb144a0038cd63ac6b42bd9c74e7d1eff9cc1419043a8bbec602e5665d45ddfa09c1831c0c04fa116ff8ad7fd93a0d005dedb329407c84b809d4552c6e31174ca01f7fe336dd1759b3d4bafdcf5df63f5bca512caf29a4e645e5315c0777478f1640afa2d30f2e8f5293571d3b94f65be0cc98f24261633ae9b0a44e6048c35ce44eca75d6362ce6b5698806addecf26d1928a2ac14939923ca63d54afa103e7a1c8f23fa9880e381d17ee89b4e65922ebe81d58b3dfe637f554f0dbb499073cb4ca9c2ee30a6bd0c5fc56675e0215a8b4577dd6c1490087bf4b2039b5b52ad49c08212a8171d0cb6fb4f84855cf426d36147f5e46fd3f7722481ce26b0511d6603087fbb9d1382a69011de7aedadd0d29b7c0ffea5640c8079acf8818de222664728df79967e54962537fa06bde323de630bf63ae92e57e33f242fd508e767da3f2dfa14c0726b12bce09c4310502807ef00b88afbe76ff01a941ce512504c25d552e8863afa3c89bdb53d757d09161a5e65b4c1d6f4fe00879d1e247d8a93f30b252d5d6d7308676a76c4d9eed11131b2c2f7f8092b0d2e417225f6d7c82a4eff0f7204765a4bcd2dafd00000000000000000000000000000000a0d1319202b353d",

"signl\_diag": "18([h'a2013831045820d9bc439f97bd6d4093e68f0f3fcf09c9a97adf888ed7308dd565247a166cb4fa', {}, h'68656c6c6f20706f7374207175616e74756d207369676e617475726573', h'e132b492fc022d5fd1d2205f52dbfladlaaef3ece4622b4e3875696d64d66dccc74df743c1b85552a0f3c1bdaaa8f789a15fdb3ce6329021f5815316cda1da5b012f1ccea4a47ef7e93eff319048ac9e3b6ed46cd58c6557af1b340da3bd7966f1588f8bd88e05383aeel2a7248db3aec96ba5d9afd1d79d62865eee04cac9cc2176ae585ae914d614805d916c142b4969be7ad95a44bf9c154d19bd41d8a3882ad6f0b0802d1e037c7579453a0606bbbb31db164fc607646477572c63b71720f8d47bbb7615dd264f5829f726e22740cb3a1e1b5e381c4f692f7ecaa0979a17aea3139d733491fe213eeddcd5f68e06ee71b80f14ed693f407ce6e199cb3edb048d3e2905ce75b31bd6837a1d4b5eefa35431d0ca407200e60768b2dc5b0370e91a6c03c3d0e5c47225616034f55fb0a3ca66fd2074847be3c1230b93650d119492efc20338af0c4cb6a176191d7c5bbc7427f6f0c9bb49a0d73e7ff026cf3855547fc7ca9369733313963ffe4647e155a93cfa5403edebfc7842e75dad9ae2accba720487e476ffe3bc0a60cf32271429242023d0d0a8f6e4e77a874afd2074a11fff20bae28d00fd5d990f839ca99c6db28a55da94a785290a6b536893a237224639717ba5cf833d57db2cca0a7aeed874597c6ee71e0dc35e06851e9d2bd022c37b5fbcd2a4d5e8daea98a44cb9c97df43a0aa512005358c8d5d5db88fba610e47d5a863f53f9ec7a8f3cb0b0ec2f02b1dfe9867a1437e84e941392b149275e868b959c58b9e814fb618c61208cb683881247bb0dcab96e84a77e0195b4e93f693c1e98dcb99e495632f6cd5839d3bcccdfa2bf6b26921759d0a293595a96e6ddd42c83d8d9a7b10a001b34f47c20fd46d1e09100e532e5b1900b89f14400bbcd5ee0cf61a1ca353398a498da488b0f117effcf999f5aafe4a587deaa3ff78cc431637adccb4e40ec385fac23e8176b74e0e750460f7d2002bf7465944caa2708835d3849199732090b7c514575311ef9999c9bfcf737a4d906af914d0507f5a7c2e61ff12359999d173f88db9ef85a6d71ac2e3a8074bed9472e00aedac26c48ab9c2d1ad96eeffe6e200686efa17086317a541ffad5c8b5707279aebc12ca48f7e7d755e8cdc2bc990c6391abf9351c2f5305bda2c57bf54e419dce477947a64de07eb0432e5f1cc87234ed673fa810d562095d0d0eed260bef5fc3daed8506756acb9059257b025471d8df2d4de697a3e7c74c47081b569519e1de636a971668a376b4d84d95c30a554894475be8f01bda7c6d78989572aea4c4e976a408b4a04b406e79e176163dcc1ffa7a7e9bd6ef6f854128097aa760ed3d6ad279f7ea4ad6003f43cfb75de79c0bf8113a6f788e35e92f30185695f4abb18e924b29abf218e708977cb2776a7abf46a41e46afe24863eed4fe890916f95d5b1f6be6cea096ceb4ad478fc994214f59c5e68c8b9695c27f8fada32c90ed324925540912da750451f033359177579e4e4a04e5d5b9bfa72616df63df20f17038e7d4bbe61562583046c35e3a71a0f596f119ef183786ed76e1da6d3be98277db1583c8f2c8784c08f5c098abfd31baa9fc6abdc0cc441b6f93961b6630c45b9e7dda60d88be7c9577b6fbc5edf65de4ed0b53f4377ce83b1e55c4d62015569b96ea094644e0f9cbe89cff4c539f77c629a5101c259c56cb9d31e20160dfe28386b37e610c2db9ecf6a000bfb2a85756e585ae6b97915e5113970946df068e6da7f0af0a48802b9e0464bfac7e0c6b7dee953665061ac7486d9eee3bf21137383e97eb393a708e91a94f5012fal072c04f5c5ca2bbf894e7b275805fe5d81341d75b9f7fcb89b3ff1c2da2b623c35d717d0da7180e258384ff39a914c2f40f893af4e1520d64a15bb0997b852f3ec6ca398d245361fc2297c8386f7388c8aa35e704d3f7081a961c528751faa64fd7efbccc03bed69e99ae1517d499117227cb08254d7b8aa079530af39fb19b246d45a4d41a9955095636c786dcc3c30c817ee3c8e60689fd9a494c9e774463df7b884a78dfe80f1e247b3f122401b0834e54fdeb57d7835f0409126983e40d8922bbd54981e2b651cc3fdee9193468c041201c2c472749300250628225052f935d37ab9dd8e466b6a3acb63ee93023013443ddeb91347b84eb6ecf37423996d682967a5aab7ccaaa73a690a9cbd45b15ee38f2ae698aac3cb2117ecc9160870993a3e50ea7647b0c03cb5f6daa290492dd693a0b8a9a9759d0d977b662d45c4af5dce95084062f7a0f39d0bc3bdabaa31d8f815047244303e6a6e5d977ec757a56797f0630ef1d4f02f7a0e7680c0865c4404c97bbf7014bfa64d0f89b02a2b981f616c0e16090c4b7fe9998a0232469b0c059d3daff58af6148cee567e52f1a41730b28d6af79358ad3679cf4c3dec0df780eccc91d004a4ec0a4d20cc6771dbb3f42da69dc2140994c228a60adc0e97438a2332db657e91e5b7f5029541d13ce8456d93bb4933522c94e16ee4766af28b5754b5a74c71efb6ff445dc1aed5f3e21cfe512cf9862489582925c763251376279f69e633a43a aadcf41c104744cfca747f477c1af8c18f65109b06680cd392d14e3e0ed0ba117643c8794bc8d036e85222d543063a0f191cb9bce80d884b1305d0065ef355d6f64be489381e0e9be111c65c9cb1840774ddd4ed5906ae2a73c7ca6103ecd3bb506747681e192dd6c259b66dc63c39dbdc33dac1d564b54db4d8de935370abca642e05c6e95ee827fb71d6086691bc6d1be2a0c7e491ce22163d3e8d48541cd7aca76eecc93f4e02ac0179cf7073d5000b3ff338d096bc87eada3f4019fdf1a5d12470a33f65c2990c217680710069de75e0338d1e26c179b1cf9ef853e daaab2c0519026b3d9f574b82b5bd316686b26c9e9e87870041fdfa1a5c538cb98cb39200856b4c9bdacaal7c717a22b883c06ca0f78229cd59362614361cc5ec76d836d2dafc1ed51066afa7297db869508cc80543b1efcddc62eb7c4ffabe3fafbc02f4802b4992ff0be194ae123880ceee6187e08c7db96b22438ac4bdabadd8aba7af68



b8e2ac0c60c0f9aad5e4e1bf886db18212e9cb46d8bc201e4a1a6fb231d91a309dbca30b6b1269ec31bda1bb6  
b6d8ff41d84baf7db7ac30de5ad5d9259398bbfb5ffbb89cce88a15f0f7413c9c71487b56eea23573697a583f  
a57d3537588ba5558363d8abd679f2968dbca3ff00b141d68d5baed53fa66480029f46f6b195e3dc99a0e09f9  
90841c62735db8e4b6b867ee416cd946b65fae48acd2c580c5ee461fdc78c2d671abb657f9296f976cb74c024  
9676a111e7608785ede2acde6f8af297f88ce9ad0e6b4cfdac1c586519042ac700a4178f5c23add6634c26588  
f47bfb7ec9e244ae8c71382042c24606410ef598ccfcaa459923e748d608caf3c82dd141c8eb32a500a03bb7f  
bd5d628b625fec3d9399254d7c569ab1418c6af0db64009f09d457e287b0e8b83bf40d529379464df999d751  
9a454bb3fa9684f398c965c4f980061d33fd8883c5ad2964806f27fdfb09458b1bb2daaced0fbc0c68d46d622  
24f63725932b58ae0a694ec7fa0d4e5fcdc75840b467e12514f1cd006befcf3410cf7a5c81adf3d29cd93ef56  
80c1a953daa0645273d0f5fcdc8e6e0f8c632b67a674fb4f390c392720ec6d8e3f1234e84f8420b91217ad71f4  
06b1a4c7f2c438fff7844a097cdfb00a2f1a94ee6bdd597756a754681111d66040c13a661b978440b05ba8c16  
e2a4255ebff56e5adada6fb92292d501d30e351f4fb5b907d9f1510e9801489da0a3cf4997eed6df4fb06b86f  
81af3735781513c6654e030a03e358970fa129fdb8cb49365a86f1cdd1a9b5f966794c8bca163c3af148406c2  
4f0e149da338e6a1fb5f365b1a6bf0fe426ec42f8d23588dce11dfe7de3b3aa740d272fac9b6d9c60909b4afe2f  
88dde858069e330e6f9a7ecc779022d3925ea0bd73e67041945e04691152683453f3126cb3699b607dd598af0  
5fd441c157bb3b8d69243705cd1e71442b502b7ea987c8837a3bd896e5bf2796052a23d302c70b23a62383278  
elf3c878c2bdc68524c078fc73148f227951566c19248240d972d5547350909c63d6f505ad889884fe971015  
4d2ec05aa15a4f734e5b88480916ec73e1518fbd2605954580ec2b0a8f9c4bd4d075461b6b3015c344e83382c  
36b161e57a6c3933e98209ce308190531f85f5d5fd9451d37f40f6f36af830b376ed2d48ab20b2b58b7c6e595  
6b7d4142b19ccb19a88db70e5829047751950e2975bb4d0e9991fc3bbc4fa5adf2d9d1e25e4ded5396731bd28  
08b8227a30233cc7a1ab7759623357547e46060a4c6c54a8d24116680186ca97291afd2be4ffdc9bealc4b81a  
d80a3e7be17fb5585eeb72dfc030655040993fe12f58d21d3ea499c1ecac70725f2e133450e9c1e75ce657300  
f85ae0f44e470336dbd5df32fbc0a8ffbe3c66058e45ac5fb0ea3889313214b6b2ec98a91e6414b3dda04d9c4  
1857707bbdcf4763ee3846c7f4df034eldc8f8efc8a2a5dcda9f91940cdcd1f7b98b93c08bc9f1c198e80fcd8e  
a5effe4ea4363a56cae57de4a7248fd8bde5767f1ae699b5bd998d9f613306346472e96954dc32baccd31c3f4  
4b0f11b8e6810bb3f27af7de6a57550288f56015b1b76f1c1e492d5b998493b72a38ba4f2619b891aeeccfd96c  
27fe80b958e08728581ca4d6e7da5f2760b48734a049e8fb29aa6ff373911d712091ef6bbbed204da3b1237c11  
95654c7f66aa6776e950e7a27aed6c9a4fffebe76671ff1dea7b1ee5d0434c976d2d23bb481b6d80d242a2c942  
329dbe051396d0a9add08068634f6c7f8aadfd55e4109cde60f693229f605d71f896f5e1c9d3b94fb9a497a9b  
955960307811296f2ed263ad57780c6f2f96b42eb71e817bbed0654000c6bc20d3087f7971b8d517c00cdf973  
2294285c6faa24b405e3b31e6fb856b57aabae81e72a8876f06cc0fbd5ca4479a5ceccdee7b5bd0fff8f8c788  
e2d803dad28ca110f6013672323540b94eb5a7638116cfec790f2d899d7f6bc075cbb78ad925845bc75b80860  
78356b0c6dc722283e774cb7a5ee24a6b976ca6dcc40fef3ea10e77cc50a0523ab4df32971a19c9c6e889edb9  
9ea9d863e7f9922d02303b80a29899397f4abacc5ecf6da98574e2ee2afcd18077063d7419e4ee36189108521  
7c905f6cefbb2041ee6f49df051511152f45609a0d06d951b0351431651bde5b5434c06b146509727cd5b76f18  
2c1353ee94e6ef98901cdba4b6cfc1dda01628f86b21e2be53da4a8c2c9fclb50b28ada2836959ed1398c700  
18b5f3c35d9f3c8768af0966a0e8ee6b16dd17455aced377fd259379e7e22f187876db740c3c09a030789148  
4f9b12da66916d9d4018ac34b9d70a094a655ece0282839a9e60b8cea041316803b262a4928d375889017f3da  
58b9721ac9d7a4e69b06fb26d46a904b062728286ee2e44c18354be39252482e5135fbfdlea4f85dfc96b63e0  
fc8815a3a0f1be7476e60712a566911663159e74838f27a0068b2131aec8653b5f697ede4dd8c769234ba5d01  
8ede320aeace49e263844b93d3c2410af9c5df83c0e7eb617930eea8a272e16a6d58e6ce1ce9a3b42ad94436a  
be73e01b95839038d5430676ef6a7a3c77cd541fe860d40bd9414133a8983280e139161d85dc0c395eac1fffc6  
fe52d637fd5f327d112f8ed15172925b0a21334d8b5dbeaea1bdbfbcf9bcb8c9bd72b58aa6745f07fae5034319  
1f90983e4d138a278f46433a8c404565c4d15a55c4d61f396444b639bf7191515c558155bf2a09576e7b33762  
36a23baeb2f7826e1b5e95e100bae7d0b9226864839d04f2145cf0a0c0dbb0194f2224aa63cb144a0038cd63a  
c6b42bd9c74e7d1eff9cc1419043a8bbec602e5665d45ddfa09c1831c0c04fa116ff8ad7fd93a0d005dedb329  
407c84b809d4552c6e31174ca01f7fe336dd1759b3d44bafdcf5bdf63f5bca512caf29a4e645e5315c0777478f1  
640afa2d30f2e8f5293571d3b94f65be0cc98f24261633ae9b0a44e6048c35ce44eca75d6362ce6b5698806ad  
decf26d1928a2ac14939923ca63d54afa103e7a1c8f23fa9880e381d17ee89b4e65922ebe81d58b3dfe637f55  
4f0dbb499073cb4ca9c2ee30a6bd0c5fc56675e0215a8b4577dd6c1490087bf4b2039b5b52ad49c08212a8171  
d0cb6fb4f84855cf426d36147f5e46fd3f7722481ce26b0511d6603087fbb9d1382a69011de7aedadd0d29b7c  
0ffaeae5640c8079acf8818de222664728df79967e54962537fa06bde323de630bf63ae92e57e33f242fd508e7  
67da3f2dfa14c0726b12bce09c4310502807ef00b88afbe76ff01a941ce512504c25d552e8863afa3c89bdb53  
d757d09161a5e65b4c1d6f4fe00879d1e247d8a93f30b252d5d6d7308676a76c4d9ee11131b2c2f7f8092b0d2  
e417225f6d7c82a4eff0f7204765a4bcd2dafd00a0d1319202b353d' ) )",

"raw\_to\_be\_signed": "846a5369676e6174757265315827a2013831045820d9bc439f97bd6d4093e68f0f  
3fcf09c9a97adf888ed7308dd565247a166cb4fa40581d68656c6c6f20706f7374207175616e74756d2073696  
76e617475726573",

"raw\_signature": "e132b492fc022d5fd1d2205f52dbf1ad1aaef3ece4622b4e3875696d64d66dccc74df  
743clb85552a0f3clbdaaa8f789a15fdb3ce6329021f5815316cdalda5b012flccea4a47ef7e93eff319048ac  
9e3b6ed46cd58c6557af1b340da3bd7966f1588f8bd88e05383ae12a7248db3aec96ba5d9afd1d79d62865ee  
e04cac9cc2176ae585ae914d614805d916c142b4969be7ad95a44bf9c154d19bd41d8a3882ad6f0b0802d1e03  
7c7579453a0606bbbb31db164fc607646477572c63b71720f8d47bbb7615dd264f5829f726e22740cb3ale1b5  
e381c4f692f7ecaa0979ae17aea3139d733491fe213eeddc5f68e06ee71b80f14ed693f407ce6e199cb3edb0  
48d3e2905ce75b31bd6837ald4b5eefa35431d0ca407200e60768b2dc5b0370e91a6c03c3d0e5c47225616034  
f55fb0a30a66fd2074847be3c1230b93650d119492efc20338af0c4cb6a176191d7c5bbc7427f6f0c9bb49a0d

73e7f026cf3855547fc7ca9369733313963ffe4647e155a93cfa5403edebfc7842e75dad9ae2accba720487e4  
76ffe3bc0a60cf32271429242023d0d0a8f6e4e77a874afd2074a11fff20bae28d00fd5d990f839ca99c6db28a  
55da94a785290a6b536893a237224639717ba5cf833d57db2cca0a7aeed874597c6ee71e0dc35e06851e9d2b  
d022c37b5fbcd2a4d5e8daea98a44cb9c97df43a0aa512005358c8d5d5db88fba610e47d5a863f53f9ec7a8f3  
cb0b0ec2f02b1dfe9867a1437e84e941392b149275e868b959c58b9e814fb618c61208cb683881247bb0dcab9  
6e84a77e0195b4e93f693c1e98dcb99e495632f6cd5839d3bcccdfa2bf6b26921759d0a293595a96e6ddd42c8  
3d8d9a7b10a001b34f47c20fd46d1e09100e532e5b1900b89f14400bbcd5ee0cf61a1ca353398a498da488b0  
f117effcf999f5aafe4a587deaa3fff78cc431637adcb4e40ec385fac23e8176b74e0e750460f7d2002bf7465  
944caa2708835d3849199732090b7c514575311ef9999c9bfcf737a4d906af914d0507f5a7c2e61fff12359999  
d173f88db9ef85a6d71ac2e3a8074bed9472e00aedac26c48ab9c2d1ad96eeffe6e200686efa17086317a541f  
fad5c8b5707279aecb12ca48f7e7d755e8cdc2bc990c6391abf9351c2f5305bda2c57bf54e419dce477947a64  
de07eb0432e5f1cc87234ed673fa810d562095d0d0eed260bef5f3daed8506756acb9059257b025471d8df2d  
4e697a3e7c74c47081b569519e1de636a9717668a376b4d84d95c30a554894475be8f01bda7c6d78989572aea4  
c4e976a408b404b406e79e176163dcc1ffa7a7e9bdc6ef6f854128097aa760ed3d6ad279f7ea48a478df6003f43cfb  
75de79c0bf8113a6f788e35e92f30185695f4abb18e924b29abf218e708977cb2776a7abf46a41e46afe24863  
eed4fe890916f95d5b1fbb6cea096ceb4ad478fc994214f59c5e68c8b9695c27f8fada32c90ed324925540912  
da750451f033359177579e4e4a04e5d5b9bfa72616df63df20f17038e7d4bbe61562583046c35e3a71a0f596f  
119ef183786ed76e1da6d3be98277db1583c8f2c8784c08f5c098abfd31baa9fc6abdc0cc441b6f93961b6630  
c45b9e7dda60d88be7c9577b6fbc5edf65de4ed0b53f4377ce83b1e55c4d62015569b96ea094644e0f9cbe89c  
ff4c539f77c629a5101c259c56cb9d31e20160dfe28386b37e610c2db9ecf6a000bfb2a85756e585ae6b97915  
e5113970946df068e6da7f0af0a48802b9e0464bfac7e0c6b7dee953665061ac7486d9eee3bf21137383e97eb  
393a708e91a94f5012fa1d072c04f5c5ca2bbf894e7b275805fe5d81341d75b9f7fcb89b3fff7da2b623c35d71  
7d0da7180e258384ff39a914c2f30f893af4e1520d64a15bb0997b852f3ec6ca398d245361fc2297c83867f38  
8c8aa35e704d3f7081a961c528751faa64fd7efbcc03bed69e99ae1517d499117227cb08254d7b8aa079530af  
39fb19b246d45a4d41a9955095636c786dcc3c30c817ee3c8e60689fd9a494c9e774463df7b884a78df6e80fle  
247b3f122401b0834e54fdeb57d7835f0409126983e40d8922bbd54981e2b651cc3fdee9193468c041201c2c4  
72749300250628225052f935d37ab9dd8e466b6a3acb63ee93023013443ddeb91347b84eb6ecf37423996d682  
967a5aab7ccaaa73a690a9cbd45b15ee38f2ae698aac3cb2117ecc9160870993a3e50ea7647b0c03cb5f6daa2  
90492dd693a0b8a9a9759d0d977b662d45c4af5dce95084062f7a0f39d0bc3bdabaa31d8f815047244303e6a6  
e5d977ec757a56797f0630ef1d4f02f7a0e7680c0865c4404c97bbf7014bfa64d0f89b02a2b981f616c0e1609  
0c4b7fe9998a0232469b0c059d3daff58af6148cee567e52f1a41730b28d6af79358ad3679cf4c3dec0df780e  
ccc91d004a4ec0a4d20cc6771ddb3f42da69dc2140994c228a60adc0e97438a2332db657e91e5b7f5029541d1  
3ce8456d93bb4933522c94e16ee4766af28b5754b5a74c71efb6fff445dc1aed5f3e21cfe512cf986248958292  
5c763251376279f69e633a43aaadcf4c104744cfca747f477c1af8c18f65109b06680cd392d14e3e0ed0ba117  
643c8794bc8d036e85222d543063a01f91cb9bceb80d884b1305d0065ef3555d6f64be4893816e0e9be111c65  
c9cb1840774ddd4ed5906ae2a73c7ca6103ecd3bb506747681e192dd6c259b66dc63c39dbdc33dac1d564b54d  
b4d8de935370abca642e05c6e95ee827bf71d6086691bcb6d1be2a0c7e491ce22163d3e8d48541cd7aca76eecc  
93f4e02ac0179cf7073d5000b3fff338d096bc87eada3f4019fdf1a5d12470a33f65c2990c217680710069de75  
e0338d1e26c179b1cf9ef853edaaab2c0519026b3d9f574b82b5bd316686b26c9e9e87870041fdfala5c538cb  
98cb39200856b4c9bdacaa1c7717a22b883c06ca0f78229cd59362614361cc5ec76d836d2dafcled51066afa7  
297db869508cc80543b1efcddc62eb7c4ffabe3fafbc02f4802b4992ff0be194ae123880ceee6187e08c7db96  
b22438ac4bdabadd8aba7af68b8e2ac0c60c0f9aad5e4e1bf886db18212e9cb46d8bc201e4a1a6fb231d91a30  
9dbca30b6b1269ec31bdalbb6b6d8fff41d84baf7db7ac30de5ad5d9259398bbfb5ffbb89cce88a15f0f7413c9  
c71487b56eea23573697a583fa57d3537588ba5558363d8abd679f2968dbca3fff00b141d68d5baed53fa66480  
029f46f6b195e3dc99a0e09f990841c62735db8e4b6b867ee416cd946b65fae48acd2c580c5ee461fdc78c2d6  
71abb657f9296f976cb74c0249676a111e7608785ede2acde6f8af297f88ce9ad0e6b4cfdac1c586519042ac7  
00a4178f5c23add6634c26588f47bfb7ec9e244ae8c71382042c26406410ef598ccfcaa409923d748d608caf3  
c82dd141c8eb32a500a03bb7fbd5d628b625fecfd39399254d7c569ab1418c6af0cb64059f09d457e287b0e8b  
83bf40d529379464df999d7519a454bb3fa9684f398c965c4f980061d33fd8883c5ad2964806f27dfdb09458b  
1bb2daaced0fbc0c68d46d62224f63725932b58ae0a694ec7fa0d4e5fcd75840b467e12514f1cd006befcf34  
10cf7a5c81adf3d29cd93ef5680c1a953daa0645273d0f5fcd8e6e0f8c632b67a674fb4f390c392720ec6d8e3  
f1234e84f8420b91217ad71f406b1a4c7f2c438fff7844a097cdfb00a2f1a94ee6bdd597756a754681111d660  
40c13a661b978440b05ba8c16e2a4255ebff56e5adada6fb92292d501d30e351f4fb5b907d9f1510e9801489d  
a0a3cf4997eed6df4fb06b86f81af3735781513c6654e030a03e358970fa129fdb8cb49365a86f1cdd1a9b5f9  
66794c8bca163c3af148406c24f0e149da338e6a1fb5f365b1a6bf0fe426ec424823588dce11dfe7de3b3aa74  
0d27fac9b6d9c60909b4afe2f88dde858069e330e6f9a7ecc779022d3925ea0bd73e67041945e046911526834  
53f3126cb3699b607dd598af05fd441c157bb3b8d69243705cd1e71442b502b7ea987c8837a3bd896e5bf2796  
052a23d302c70b23a62383278e1f3c878c2bdcdb68524c078fc73148f227951566c19248240d972d5547350909  
c63d6f505ad889884fe9710154d2ec05aa15a4f734e5b88480916ec73e1518fbd2605954580ec2b0a8f9c4bd4  
d075461b6b3015c344e83382c36b161e57a6c3933e98209ce308190531f85f5d5fd9451d37f40f6f36af830b3  
76ed2d48ab20b2b58b7c6e5956b7d4142b19ccb19a88db70e5829047751950e2975bb4d0e9991fc3bb4fa5ad  
f2d9d1e25e4ded5396731bd2808b8227a30233cc7alab7759623357547e46060a4c6c54a8d24116680186ca97  
291afd2be4ffdc9bealc4b81ad80a3e7be17fb5585eeb72dfc030655040993fe12f58d21d3ea499c1ecac7072  
5f2e133450e9c1e75ce657300f85ae0f44e470336dbd5df32fbc0a8ffbe3c66058e45ac5fb0ea3889313214b6  
b2ec98a91e6414b3dda04d9c41857707bbdcf4763ee3846c7f4df034eldc8fefc8a2a5dcda9f91940cdcd1f7b  
98b93c08bc9f1c198e80fcde8a5effe4ea4363a56cae57de4a7248fd8bde5767f1ae699b5bd998d9f61330634

6472e96954dc32baccd31c3f44b0f11b8e6810bb3f27af7de6a57550288f56015b1b76f1c1e492d5b998493b7  
2a38ba4f2619b891aeeccfd96c27fe80b958e08728581ca4d6e7da5f2760b48734a049e8fb29aa6ff373911d71  
2091ef6bbbed204da3b1237c1195654c7f66aa6776e950e7a27aed6c9a4fffebe76671fff1dea7b1ee5d0434c976  
d2d23bb481b6d80d242a2c942329dbe051396d0a9add08068634f6c7f8aadfd55e4109cde60f693229f605d71  
f896f5e1c9d3b94fb9a497a9b955960307811296f2ed263ad57780c6f2f96b42eb71e817bbbed0654000c6bc20  
d3087f7971b8d517c00cdf9732294285c6faa24b405e3b31e6fb856b57aabae81e72a8876f06cc0fbda5ca447  
9a5cecddee7b5bd0fff8f8c788e2d803dad28ca110f6013672323540b94eb5a7638116cfec790f2d899d7f6bc0  
75cbb78ad925845bc75b8086078356b0c6dc722283e774cb7a5ee24a6b976ca6dcc40fef3ea10e77cc50a0523  
ab4df32971a19c9c6e889edb99ea9d863e7f9922d02303b80a29899397f4abacc5ecf6da98574e2ee2afcd180  
77063d7419e4ee361891085217c905f6cefcb2041ee6f49df051511152f45609a0d06d951b0351431651bde5b5  
434c06b146509727cd5b76f182c1353ee94e6ef98901cdba4b6cfc1dda01628ff86b21e2be53da4a8c2c9fclb  
50b28ada2836959ed1398c70018b5f3c35d9f3c8768af0966a0e8ee6b16dd17455aced377fd259379e7e22f1  
87876db740c3c09a0307891484f9b12da66916d9d4018ac34b9d70a094a655ece0282839a9e60b8cea0413168  
03b262a4928d375889017f3da58b9721ac9073b4e69b06fb26d46a904b062728286ee2e44c18354be39252482e  
5135fbfd1lea4f85dfc96b63e0fc8815a3a0f1be7476e60712a566911663159e74838f27a0068b2131aec8653b  
5f697ede4dd8c769234ba5d018ede320aeace49e263844b93d3c2410af9c5df83c0e7eb617930eea8a272e16a  
6d58e6celce9a3b42ad94436abe73e01b95839038d5430676ef6a7a3c77cd541fe860d40bd9414133a8983280  
e139161d85dc0c395eac1ffc6fe52d637fd5f327d112f8ed15172925b0a21334d8b5dbeeaealbdbfcf9bcb8c9b  
d72b58aa6745f07fae50343191f90983e4d138a278f46433a8c404565c4d15a55c4d61f396444b639bf719151  
5c558155bf2a09576e7b3376236a23baeb2f7826e1b5e95e100bae7d0b9226864839d04f2145cf0a0c0dbb019  
4f2224aa63cb144a0038cd63ac6b42bd9c74e7d1efff9cc1419043a8bbec602e5665d45ddfa09c1831c0c04fa1  
16ff8ad7fd93a0d005dedb329407c84b809d4552c6e31174ca01f7fe336dd1759b3d4bafdcf5df63f5bca512c  
af29a4e645e5315c0777478f1640afa2d30f2e8f5293571d3b94f65be0cc98f24261633ae9b0a44e6048c35ce  
44eca75d6362ce6b5698806addecf26d1928a2ac14939923ca63d54afa103e7a1c8f23fa9880e381d17ee89b4  
e65922a8e81d58b3dfe637f554f0dbb499073cb4ca9c2ee30a6bd0c5fc56675e0215a8b4577dd6c1490087bf4  
b2039b5b52ad49c08212a8171d0cb6fb4f84855cf426d36147f5e46fd3f7722481ce26b0511d6603087fbb9d1  
382a69011de7aedadd0d29b7c0ffae5640c8079acf8818de222664728df79967e54962537fa06bde323de630  
bf63ae92e57e33f242fd508e767da3f2dfa14c0726b12bce09c4310502807ef00b88afbe76ff01a941ce51250  
4c25d552e8863afa3c89bdb53d757d09161a5e65b4c1d6f4fe00879d1e247d8a93f30b252d5d6d7308676a76c  
4d9ee11131b2c2f7f8092b0d2e417225f6d7c82a4eff0f7204765a4bcd2dafd000000000000000000000000  
000a0d1319202b353d",

"raw\_public\_key": "e45fffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff1db7b468cf  
c82bb929f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f124d5e60bd68b8c7e3  
1fe01c7b0dc65ae470501cc565a6eldfcfcfd12565433c4afedd511821e2e9610c45275e2836dee35ced69d7e  
fa672fd1e4318bef5eb6e897e8b451aa202ded042b2aaef77a7be3f699146da229a8bdb3ffa496445967e7521  
7bfbcf9048f9956443d8731f833eb30de10dac96fffe7cf65ea0445c3e31e8601e133be6a100764fe3196e2677  
26441c31751fbf9a6f5880644f4e7275e57de2b0f105e4db055d50dd1c9c934fddf535b8de28b0c74c0449f22  
2cd2ed0bb8fbc775ccee8c940665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f12eee758185  
6ebd68f26845956e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab932e69f778e2  
ceefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a3655098941993a1594  
860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8dac1f861fd58e2afba5de5a52  
e020904f5b42bc0874e35befcf3e6119684768f36e008f04712177cebe627607381e56eaaee161c1729b8de51  
dbde474d48cc68249ea27162b87993e60c84ed6cc6423cb3676d9eb50b2cab5a3a049ef131381d623fa6fbcbc  
9db1e7cc025ea0418b9dad2cc6ccd4e95fa2cec24feeca70318a751716b7213f63edbf65a63338357f838f94e  
c071822c24851248885107b3d1c4e924678c7614ealaf038104619f2ae372940becfa69e29cbb5fff6c3e20a47  
be4a4f74bac34c133c00a6a706accc6ffd3d8e4fbd69a99704e1283c850d8c58d1e5753cd9587b83c4c346cb9  
a58137213ec10834c66adfe2bb5c501a8ef2ecadd1b677a3df1a6bed86ebf0722c4f5030e20f9018dd5b6fc53  
eea47d92b3e1b54025fae996d3e48fd4cef50d82dbad7eaf936639698512f26253d2ef6847c8518e8565cc9a5  
495c6fff57cde7323882c54a7db470ab2daf8ffdb794fa7c692d9e7fbd532eecc1d7880e2ca0b3216128be2  
8b4a9f1d151fac97808b0bd98b7b43a612a9ac865812bfeac6f47460277840b52a3b087f916ca7cedc0f768ea  
2bd19ea21155f84b4a04c4000ad2ae0587154d560bc0a477a4f9329a8984dd31eb1f2a05e3d918701d630cfca  
9af61ef088d2c5581ac6463e439902e5d425719e956b8d6df7305b28e0ff27d3ad0de2085d292499b19a3390d  
4396fb3bac9a8d8cbad2a7a4290fc9ac6fca045f98a614a45a39cbe24360f84d14f8e472712aceb74dbf45b5  
3d49a0e4737e476ffcd45b2f7cd247aa186d3b764ad9e9cfeee456a73c291d8de3912414ac43911c372173ad7  
b472af35c6853ced2fe7b5fe0a89565ab33baa6f65cdd928319d7065e040e7a5e84f9aa903f7648094bad0713  
6b16927b8ec6dbc2bef0cc2856de1e795923e1412c49f24deeb6c21f6c8a9765c9c7986e0da4b4c67d8e0d0c8  
d466824fb923d8573148990cd2ef133c78ceecab72ed9dd285c5a3766852d54534207ffd34027f6c76ede8fd1  
a32d72c30048bbaa797d5df6fde27d087de5721ad7b7fa3e8d3f70d6bfc3ab2e252335368bbfa15acb5cb37d4  
694e8b23cebe25de9c925a221a183b904d3f85df9929a919c54d6f8745f733a0d6ecc1403e4cbb6e20999435e  
80696634cd1a8e4747e9825bfa336e5bbad14f73640f1b9febe800dbaeef1630c61fae635b074c564eaa9db18  
9c9e7302873fc6464d97bc5c29080987a07a21d4af210703a4fa07f2fd816f12fd1e29b4c0f44afe9bd4alea  
a8a7ae6f02a5b4258f52caf6127f62632a67cf4e8310be56a7c28c86b2e277600c3e92c8d23d42586244c571e  
90568df202f2f6d81f860a565f9eb91a3c78372e2a8b1be61c5418cf49bf2d6c8955d4a482a9919b7660b3f9a  
4404ffc454ea073e1e4b2689ab2cca4e46bd7004a6c491fa26ee7a57d60f35edb2b821e6266442c8f335d452d  
524c772e0353724c23c7dd15b7aa155e91442022140c5fcb0153147edcf3e8952f6f0399a3c88066a72756c94  
09915de63f64fa797841c57c796c6fc550ef745dfe9f179457f94755ae5a2506a764f327e550be3dc14dd41f3

```
b04b147d454938c63a8d69b2ea4c5710ec0b36e3a6c72571fa5d59dde036c42033df35af056966ff0cd120400
8971aa6ba9fb97b685ab9ffa2a9d1778104cd2c3b326de1fcabc242e94d0311c3275b12850ed30ceead3a2ee6d
060508411d4396f5421d8b6d067cf7cb5e826785fbe119e05e21bd879b64f57cb0cd1972c2815f20abe7ce6ab
34d0f471af44baad179e90644122f5f33288e689dddc5ce833e9755df1e73c65c5a201c4ede2ffa6b1927492
7719d2d38fdb7a65aa43708b7fa9a94aa7d3210253d78d3b181e1020d0000bd0a1dc05d447f9f58eb84c65b
36c8afcb83727a1508994e826957a663b0b9b8a003325ab6d6d6462ee4e106019c0dffe10323b7bde7d82a38f
85fd08786e860ba66c161b64b0708c363de5c6af62d8db3c243d1e1b712cb1d59e942b9b6b4295a5a500b182c
bd5fd1bc6ce9376d91b47a2284f1f0ad1c048cc2cfbb4afa3a9eb9697503b69feca990eba7e9441af9ca44c
b3ac6b5ed66e591c201fe30efa8a7c471dc613d6254c263a8e132104bec47f1aacb3b2fcd4051b69b5e3fcb1c
147a65c2f90c4b5188baf521cab03c12a309da50b5a7517727ed41228ed123fe1b152f6a6319cd623bf34ad7
b8e064ab993260bcb405f5b7fff9b2fa40ba5ed5630242539e5d96823e89dc818a13d16675ee3079d976f694
f5acc9760ae789e9b3391b289e0e22a7ef17cc6a4577157b6d95c09baa4fd532e3ee0a290810ed35e56bb19d9
b61fb98a97c617425b06093d98a5cf0ee2dd127f0eea600b9a0c67f7e761db9b77e5d5bba9701dalb883e521a
0cfe88451f57bd36085b67e56f061f84a2e6a152a71bce6e522daab6a0a33ce22e537fa9793d28b617e6c0a41
76a83aa3be578afac0f2f5547c5516d218984755b7445c7143afa4e551f0071bdb873b34e6b9e2b9e79ed0c
69d288ed6421f237e860a0c6492ebbd2a44c2c4f368dbe99941b1e8561d859d3859f496cee3d741f252973f8
fcc539c409e35cc80a5ed6df23cc3a65601313f5d681fd9540c5291a9e30a72e38c96413c47c61ff84fde78d0
11b01b4154d1b920af003f7abb1e1999dea6a766cf9fd2702b3ce0ee57af931b62124b0861b163a3b91aa4bea
28076c3432df3b29b6c4elba588def420071fc157de90eb2722ecc9ab00df3c669383a61a91bb67bd287ce349
b4745ee7a479dbceef166b9acc412eb579fcd6437307edda253d606b7be7599c38092bc52a8598480edab8b82
b1d21c565d2137ceae0b6642619b16133d91205d6355029e9cdfef9a28b373d95916b6b707d4c712c09cf36da
f1a511b2bedb1aa70ee58d46a0666bb287784b0a3840c589a7a04d5d6f2216be90aa4a512d5632f5c9bfe7b8b
13382f999b95d367c7c46b968074ce315197a5ff3545c7b77a804ade56a95b5c24cdece5937b5c0366d93ad03
da9bc5db1b551dfb91e9b343d2b57b763439686d4a3"
}
```

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