JOSE
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

L. Prabel
S. Sun
Huawei
J. Gray
Entrust

7 July 2025

PQ/T Hybrid Composite Signatures for JOSE and COSE
draft-prabel-jose-pq-composite-sigs-03

Abstract

This document describes JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for PQ/T hybrid composite signatures. The composite algorithms described combine ML-DSA as the post-quantum component and ECDSA as the traditional component.

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://example.com/LATEST. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-prabel-jose-pq-composite-sigs/.

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

Source for this draft and an issue tracker can be found at https://github.com/lucasprabel/draft-jose-pq-composite-sigs.

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/.

Copyright Notice

Table of Contents

1. Introduction

The impact of a potential Cryptographically Relevant Quantum Computer (CRQC) on algorithms whose security is based on mathematical problems such as integer factorisation or discrete logarithms over finite fields or elliptic curves raises the need for new algorithms that are perceived to be secure against CRQC as well as classical computers. Such algorithms are called post-quantum, while algorithms based on integer factorisation or discrete logarithms are called traditional.

While switching from a traditional algorithm to a post-quantum one intends to strengthen the security against an adversary possessing a quantum computer, the lack of maturing time of post-quantum algorithms compared to traditional algorithms raises uncertainty about their security.

Thus, the joint use of a traditional algorithm and a post-quantum algorithm in protocols represents a solution to this problem by providing security as long as at least one of the traditional or post-quantum components remains secure.

This document describes JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for hybrid composite signatures. The composite algorithms described combine ML-DSA as the post-quantum component and ECDSA as the traditional component.

2. Conventions and Definitions

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.

This document follows the terminology for post-quantum hybrid schemes defined in [I-D.draft-ietf-pquip-pqt-hybrid-terminology].

This section recalls some of this terminology, but also adds other definitions used throughout the whole document:

"Asymmetric Traditional Cryptographic Algorithm": An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms, elliptic curve discrete logarithms, or related mathematical problems. A related mathematical problem is one that can be solved by solving the integer factorisation, finite field discrete logarithm or elliptic curve discrete logarithm problem. Where there is little risk of confusion asymmetric traditional cryptographic algorithms can also be referred to as traditional algorithms for brevity.

"Post-Quantum Algorithm": An asymmetric cryptographic algorithm that is intended to be secure against attacks using quantum computers as well as classical computers. As with all cryptography, it always remains the case that attacks, either quantum or classical, may be found against post-quantum algorithms. Therefore it should not be assumed that just because an algorithm is designed to provide post-quantum security it will not be compromised.

"Post-Quantum Traditional (PQ/T) Hybrid Scheme": A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.

"PQ/T Hybrid Digital Signature": A multi-algorithm digital signature scheme made up of two or more component digital signature algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

"Composite Algorithm": An algorithm which is a sequence of two component algorithms, as defined in [I-D.draft-ietf-lamps-pq-composite-sigs].

"Component Algorithm": Each cryptographic algorithm that forms part of a cryptographic scheme.

3. Algorithm Key Pair (AKP) Type

This document makes use of the Algorithm Key Pair (AKP) type which is defined in [I-D.draft-ietf-cose-dilithium].

As a reminder, the AKP type is used to express public and private keys for use with algorithms. The parameters for public and private keys contain byte strings.

This document makes use of the serialization routines defined in [I-D.draft-ietf-lamps-pq-composite-sigs] to obtain the byte string encodings of the composite public and private keys.

The process to compute JWK Thumbprint and COSE Key Thumbprint as described in [RFC7638] and [RFC9679] is detailed in [I-D.draft-ietf-cose-dilithium].

4. Composite Signature Algorithm

The structures of the composite keys and composite signatures follow an approach similar to [I-D.draft-ietf-lamps-pq-composite-sigs]. The composite design is chosen so that composite keys and signatures can be used as a drop-in replacement in JOSE / COSE object formats. This section gives some details about their construction.

4.1. Composite Key Generation

Composite public and private keys are generated by calling the key generation functions of the two component algorithms and concatenating the keys in an order given by the registered composite algorithm.

Composite Public Key <- Public Key of the 1st Algorithm || Public Key of the 2nd Algorithm and

Composite Private Key <- Private Key of the 1st Algorithm || Private Key of the 2nd Algorithm

For the composite algorithms described in this document (ML-DSA with ECDSA), the Key Generation process is as follows:

```
(pk_1, sk_1) <- ML-DSA.KeyGen()
(pk_2 = (x,y), sk_2 = d) <- ECDSA.KeyGen()

Composite Public Key <- SerializePublicKey(pk_1, pk_2)
Composite Private Key <- SerializePrivateKey(sk_1, sk_2)
```

This document makes use of the serialization routines from [I-D.draft-ietf-lamps-pq-composite-sigs] to obtain the byte string encodings of the composite public and private keys. These encodings are then directly use with the AKP Key Type. For more information, see the SerializePublicKey, DeserializePublicKey, SerializePrivateKey and DeserializePrivateKey algorithms from [I-D.draft-ietf-lamps-pq-composite-sigs].

Point compression for the ECDSA component is not performed for the AKP JSON Web Key Type but can be performed for the AKP COSE Key Type.

In this document, as in [I-D.draft-ietf-cose-dilithium], the ML-DSA private key MUST be a 32-bytes seed.

4.2. Composite Sign

When signing a message M with the composite Sign algorithm, the signature combiner prepends a prefix as well as a domain separator value specific to the composite algorithm used to bind the two component signatures to the composite algorithm and achieve weak non-separability, as defined in [I-D.draft-ietf-pquip-hybrid-signature-spectrums].

It also makes use of a signature randomizer, in a similar fashion to [I-D.draft-ietf-lamps-pq-composite-sigs], in order to prevent specific attacks unique to composite signature schemes. More details about the security benefits added by the use of a signature randomizer can be found in [I-D.draft-ietf-lamps-pq-composite-sigs].

However, only the pure ML-DSA component algorithm is used internally.

A composite signature's value MUST include the randomizer and the two signature components and the two components MUST be in the same order as the components from the corresponding signing key.

A composite signature for the message M is generated by:

* computing a 32-byte randomizer r;
* computing the pre-hash of the message M;
* concatenating the prefix, the domain separator, a byte 0x00, the randomizer and the pre-hash;
* encoding the resulting message;
* calling the two signature component algorithms on this new message;
* concatenating the randomizer and the two output signatures.

For the composite algorithms described in this document (ML-DSA with ECDSA), the signature process of a message M is as follows:

```
M' <- Prefix || Domain || 0x00 || r || PH(M)
M' <- Encode(M')

sig_1 <- ML-DSA.Sign(sk_1, M', ctx=Domain)
sig_2 <- ECDSA.Sign(sk_2, M')

Composite Signature <- SerializeSignatureValue(r, sig_1, sig_2)
```

The serialization routines from [I-D.draft-ietf-lamps-pq-composite-sigs] are again used to obtain the byte string encoding of the composite signature. The SerializeSignatureValue routine simply concatenates the randomizer r, the fixed-length ML-DSA signature value and the signature value from the traditional algorithm. For more information, see the SerializeSignatureValue and DeserializeSignatureValue algorithms from [I-D.draft-ietf-lamps-pq-composite-sigs].

The prefix "Prefix" string is defined as in [I-D.draft-ietf-lamps-pq-composite-sigs] as the byte encoding of the string "CompositeAlgorithmSignatures2025", which in hex is 436F6D706F73697465416C676F726974686D5369676E617475726573323032 35. It can be used by a traditional verifier to detect if the composite signature has been stripped apart.

The domain separator "Domain" is defined in the same way as [I-D.draft-ietf-lamps-pq-composite-sigs] as the DER encoding of the OID of the specific composite algorithm. The specific values can be found in Table 4.

Similarly to [I-D.draft-ietf-cose-dilithium] which indicates that the ctx parameter MUST be the empty string, the application context passed in to the composite signature algorithm MUST be the empty string. To align with the structure of the [I-D.draft-ietf-lamps-pq-composite-sigs] combiner, the byte 0x00 is appended in the message M′ after the domain separator to indicate the context has length 0. However, a second non-empty context, defined as the domain separator, is passed down into the underlying pure ML-DSA component algorithm, to bind the Composite-ML-DSA algorithm used.

Table 2 (resp. Table 3) indicates the pre-hash algorithms to use for JOSE (resp. COSE).

For JOSE (resp. COSE), M′ is base64url-encoded (resp. binary encoded) before signature computations.

4.3. Composite Verify

The Verify algorithm MUST validates a signature only if all component signatures were successfully validated.

The verification process of a signature sig is as follows:

* separate the composite public key into the component public keys;

* separate the composite signature into the randomizer and the 2 component signatures;

* compute the message M’ from the message M whose signature is to be verified;

* encode the resulting message M’;

* verify each component signature.

```
(pk_1, pk_2) <- DeserializePublicKey(pk)
(r, sig_1, sig_2) <- DeserializeSignatureValue(sig)

M’ <- Prefix || Domain || 0x00 || r || PH(M)
M’ <- Encode(M’)

if not ML-DSA.Verify(pk_1, M’, ctx=Domain)
    output "Invalid signature"
if not ECDSA.Verify(pk_2, M’)
    output "Invalid signature"
if all succeeded, then
    output "Valid signature"
```

The DeserializePublicKey and DeserializeSignatureValue serialization routines from [I-D.draft-ietf-lamps-pq-composite-sigs] are used to get the component public keys, the randomizer r, and the component signatures. For more information, see the DeserializePublicKey and DeserializeSignatureValue algorithms from [I-D.draft-ietf-lamps-pq-composite-sigs].

4.4. Encoding Rules

In each combination, the byte streams of the keys are directly concatenated, and the byte streams of the signatures are directly concatenated with the randomizer r.

Randomizer r || Signature of the 1st Algorithm || Signature of the 2nd Algorithm

Since all combinations presented in this document start with the ML-DSA algorithm and the key or signature sizes are fixed as defined in [FIPS.204], it is unambiguous to encode or decode a composite key or signature.

Table 1 lists sizes of the three parameter sets of the ML-DSA algorithm.

	Private Key (seed)	Private Key	Public Key	Signature Size
ML-DSA-44	32	2560	1312	2420
ML-DSA-65	32	4032	1952	3309
ML-DSA-87	32	4896	2592	4627

Table 1: Sizes (in bytes) of keys and signatures of ML-DSA

Note that the seed is always 32 bytes, and that ML-DSA.KeyGen_internal from [FIPS.204] is called to produce the expanded private key from the seed, whose size corresponds to the sizes of the private key in the table above.

5. Composite Signature Instantiations

The ML-DSA signature scheme supports three possible parameter sets, each of which corresponding to a specific security strength. See [FIPS.204] for more considerations on that matter.

The traditional signature algorithm for each combination in Table 2 and Table 3 was chosen to match the security level of the ML-DSA post-quantum component.

The [FIPS.204] specification defines both pure and pre-hash modes for ML-DSA, referred to as "ML-DSA" and "HashML-DSA" respectively. This document only specifies a single mode which is similar in construction to HashML-DSA, with the addition of a signature randomizer. However, because the pre-hashing is done at the composite level, only the pure ML-DSA algorithm is used as the underlying ML-DSA primitive.

5.1. JOSE algorithms

The following table defines a list of algorithms associated with specific PQ/T combinations to be registered in [IANA.JOSE].

Name	First Algorithm	Second Algorithm	Pre-Hash	Description
ML-DSA-44-ES256	ML-DSA-44	ecdsa-with-SHA256 with secp256r1	SHA256	Composite Signature with ML-DSA-44 and ECDSA using P-256 curve and SHA256
ML-DSA-65-ES256	ML-DSA-65	ecdsa-with-SHA256 with secp256r1	SHA512	Composite Signature with ML-DSA-65 and ECDSA using P-256 curve and SHA256
ML-DSA-87-ES384	ML-DSA-87	ecdsa-with-SHA384 with secp384r1	SHA512	Composite Signature with ML-DSA-87 and ECDSA using P-384 curve and SHA384

Table 2: JOSE Composite Signature Algorithms for ML-DSA

Examples can be found in Appendix A.1.

5.2. COSE algorithms

The following table defines a list of algorithms associated with specific PQ/T combinations to be registered in [IANA.COSE].

Name	COSE Value	First Algorithm	Second Algorithm	Pre-Hash	Description
ML-DSA-44-ES256	TBD (request assignment -51)	ML-DSA-44	ecdsa-with-SHA256 with secp256r1	SHA256	Composite Signature with ML-DSA-44 and ECDSA using P-256 curve and SHA256
ML-DSA-65-ES256	TBD (request assignment -52)	ML-DSA-65	ecdsa-with-SHA256 with secp256r1	SHA512	Composite Signature with ML-DSA-65 and ECDSA using P-256 curve and SHA256
ML-DSA-87-ES384	TBD (request assignment -53)	ML-DSA-87	ecdsa-with-SHA384 with secp384r1	SHA512	Composite Signature with ML-DSA-87 and ECDSA using P-384 curve and SHA384

Table 3: COSE Composite Signature Algorithms for ML-DSA

Examples can be found in Appendix A.2.

5.3. Composite Domain Separators for JOSE and COSE

The JOSE and COSE composite domain separators values are listed in Table 4.

They are defined as the DER encoding of the OID of the specific composite algorithm, in order to reuse the same values as in [I-D.draft-ietf-lamps-pq-composite-sigs]. These domain separators are currently based on the prototyping OIDs assigned on the Entrust arc, and they may change in future versions of the document.

"alg" Header Parameter	Domain Separator (in Hex encoding)
ML-DSA-44-ES256	060B6086480186FA6B50090103
ML-DSA-65-ES256	060B6086480186FA6B50090108
ML-DSA-87-ES384	060B6086480186FA6B5009010C

Table 4: JOSE/COSE Composite Domain Separators

6. Security Considerations

The security considerations of [RFC7515], [RFC7517], [RFC9053] and [FIPS.204] also apply to this document.

All security issues that are pertinent to any cryptographic application must be addressed by JWS/JWK agents. Protecting the user's private key and employing countermeasures to various attacks constitute a priority.

For security properties and security issues related to the use of a hybrid signature scheme, the user can refer to [I-D.draft-ietf-pquip-hybrid-signature-spectrums]. For more information about hybrid composite signature schemes and the different hybrid combinations that appear in this document, the user can read [I-D.draft-ietf-lamps-pq-composite-sigs].

In particular, to avoid key reuse, when generating a new composite key, the key generation functions for both component algorithms MUST be executed. Compliant parties MUST NOT use, import or export component keys that are used in other contexts, combinations, or by themselves as keys for standalone algorithm use.

7. IANA Considerations

7.1. JOSE Algorithms

The following values of the JWS "alg" (algorithm) are requested to be added to the "JSON Web Signature and Encryption Algorithms" registry. They are represented following the registration template provided in [RFC7518].

7.1.1. ML-DSA-44-ES256

* Algorithm Name: ML-DSA-44-ES256

* Algorithm Description: Composite Signature with ML-DSA-44 and ECDSA using P-256 curve and SHA-256
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): n/a
* Algorithm Analysis Documents(s): TBD

7.1.2. ML-DSA-65-ES256

* Algorithm Name: ML-DSA-65-ES256
* Algorithm Description: Composite Signature with ML-DSA-65 and ECDSA using P-256 curve and SHA-256
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): n/a
* Algorithm Analysis Documents(s): TBD

7.1.3. ML-DSA-87-ES384

* Algorithm Name: ML-DSA-87-ES384
* Algorithm Description: Composite Signature with ML-DSA-87 and ECDSA using P-384 curve and SHA-384
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): n/a
* Algorithm Analysis Documents(s): TBD

7.2. COSE Algorithms

The following values are requested to be added to the "COSE Algorithms" registry. They are represented following the registration template provided in [RFC9053], [RFC9054].

7.2.1. ML-DSA-44-ES256

* Name: ML-DSA-44-ES256
* Value: TBD (request assignment -51)
* Description: Composite Signature with ML-DSA-44 and ECDSA using P-256 curve and SHA-256
* Capabilities: [kty]
* Change Controller: IETF
* Reference: n/a
* Recommended: Yes

7.2.2. ML-DSA-65-ES256

* Name: ML-DSA-65-ES256
* Value: TBD (request assignment -52)
* Description: Composite Signature with ML-DSA-65 and ECDSA using P-256 curve and SHA-256
* Capabilities: [kty]
* Change Controller: IETF
* Reference: n/a
* Recommended: Yes

7.2.3. ML-DSA-87-ES384

* Name: ML-DSA-87-ES384
* Value: TBD (request assignment -53)
* Description: Composite Signature with ML-DSA-87 and ECDSA using P-384 curve and SHA-384

* Capabilities: [kty]

* Change Controller: IETF

* Reference: n/a

* Recommended: Yes

8. References

8.1. Normative References

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

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

[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>.

[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>.

8.2. Informative References

[FIPS.204] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Digital Signature Standard", August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>.

[I-D.draft-ietf-cose-dilithium] Prorock, M., Steele, O., Misoczki, R., Osborne, M., and C. Cloostermans, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-07, 12 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-07>.

[I-D.draft-ietf-lamps-pq-composite-sigs] Ounsworth, M., Gray, J., Pala, M., Klauテ殤er, J., and S. Fluhrer, "Composite ML-DSA for use in X.509 Public Key Infrastructure", Work in Progress, Internet-Draft, draft-ietf-lamps-pq-composite-sigs-06, 18 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-pq-composite-sigs-06>.

[I-D.draft-ietf-pquip-hybrid-signature-spectrums] Bindel, N., Hale, B., Connolly, D., and F. D, "Hybrid signature spectrums", Work in Progress, Internet-Draft, draft-ietf-pquip-hybrid-signature-spectrums-07, 20 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-hybrid-signature-spectrums-07>.

[I-D.draft-ietf-pquip-pqt-hybrid-terminology] D, F., P, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, draft-ietf-pquip-pqt-hybrid-terminology-06, 10 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqt-hybrid-terminology-06>.

[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>.

Appendix A. Examples

A.1. JOSE


```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "PL7f9-uTJKx0Q_21YdJ4zGEHPcHdqJNACd_fLup8VrE",
    "kty": "AKP",
    "alg": "ML-DSA-44-ES256",
    "pub": "unH59k4RuutY-pxvu24U5h8YZD2rSVtHU5qRZsoBmBMcRPgmu9VuNOVdteXi1zNIXjnqJg_GAAxep
LqA00Vc3lO0bzRIKu39VFD8Lhuk8l0V-cFEJC-zm7UihxiQMMUEmOFxe3x1ixkKZ0jqmqP3rKryx8tSbtcXyfea64
QhT6XNje2SoMP6FViBDxLHBQo2dwjRls0k5a-XSQSu2OTOiHLoaWsLe8pQ5FLNfTDqmkrawDEdZyxr3oSWJAsHQxR
jcIiVzZuvwxYy1zl2STiP2vy_fTBaPemkleynQzqPg7oPCyXEE8bjnJbrfWkbNNN8438e6tHPIX4l7zTuzz98YPhL
jt_d6EBdT4MldsYe-Y4KLyjaGHcAlTkk9oa5RhRwW89T0z_t1DSO3dvfKLUGXh8gd1BD6Fz5MfgpF5NjoafnQEqDj
sAAhrCXY4b-Y3yYJEdX4_dp3dRGdHG_rWcPmgX4JG7lCnser4f8QGnDriqiAzJYEXeS8LzUngg_0bx0lqv_KcyU5I
aLISFO0xZSU5mmEPvdSoDnyAcV8pV44qhLtAvd29n0ehG259oRihtljTWeiu9V60a1N2tbZVl5mEqSK-6_xZvNYA1
TCdzNctvweH24unV7U3wer9XA9Q6kvJWDVJ4oKaQsKMrCSMlteBJMRxWbGK7ddUq6F7GdQw-3j2M-qdJvVKm9UPjY
9rc1lPgol25-oJxTu7nxGlbJUH-4m5pevAN6NyZ6lfhbjWTKlxkrEKZvQXs_Yf6cpXEwpI_ZJeriq1UC1XHIpRkDw
dOY9MH3an4RdDl2r9vGl_IwlKPNdh_5aF3jLgn7PCit1FNJAwC8fIncAXgAlgcXIpRXdfJk4bBiO89GGccSyDh2Eg
XYdpG3XvNgGWy7npuSoNTE7WIyblAk13UQuO4sdCbMIuriCdyfE73mvwj15xgb07RZRQtFGlFTmnFcIdZ90zDrWXD
bANntv7KCKwNvoTuv64bY3HiGbj-NQ-U9eMylWVpvr4hrXcES8c9K3PqHWADZC0iIOvlzFv4VBoc_wVflcOrL_SIo
aNFCNBAZZq-2v5lAgpJTqVOtqJ_HVraoSfcKy5g45p-qULunXj6Jwq21fobQiKubBKKOZwcJFyJD7F4ACKXOrz-HI
vSHMCWW_9dVrRuCpJw0s0aVFbRqopDNhu446nqb4_EDYQM1tTHMozPd_jKxRRD0sH75X8ZoToxFSpLBDbtdWcenxj
-zBf6IGWfZnmaetjKEBYJWC7QDQx1A91pJVJCEgieCkoIfTqkeQuePpIyu48g2FG3P1zjRF-kumhUTfSjo5qS0YiZ
Qy0E1BMs6M11EvuxXRsHClLHoy5nLYI2Sj4zjVjYyxSHyPRPGGo9hwB34yWxzYNtPPGiqXS_dNCpi_zRZwRY4lCGr
Q-hYTEWIK1Dm5OlttvC4_eiQ1dv63NiGkLRJ5kJA3bICN0fzCDY-MBqnd1cWn8YVBijVkgtaoascjL9EywDgJdeHn
XK0eeOvUxHHhXJVkNqcibn8O4RQdpVU60TSA-uiu675ytIjcBHC6kTv8A8pmkj_4oypPd-F92YIJC741swkYQoeIH
j8rE-ThcMUkF7KqC5VORbZTRp8HsZSqgiJcIPaouuxd1-8Rxrid3fXkE6p8bkrysPYoxWEJgh7ZFsRCPDWX-yTeJw
FN0PKFP1j0F6YtlLfK5wv-c4F8ZQHA_-yc_gODicy7KmWDZgbTP07e7gEWzw4MFRrndjbDb9ZLZYWQdL8rdrhiozb
esJyigGscX-Q4dHzFdwpsHwee3Ah5jhQivTsrihZx0knrzXobgPR5Yf8XkcqLxDYVrc",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws": "eyJhbGciOiJNTC1EU0EtNDQtRVMyNTYiLCJraWQiOiJQTDdmOS11VEpLeDBRXzIxWWRKNHpHRUhQY0h
kcUpOQUNkX2ZMdXA4VnJFIn0.SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb3V0IHlv
dXIgZG9vci4.D9GXY_VoL3fYHHXGqpMXlypSZEooR_d4qjHpP1maVEvUlvZz2WDntamafsn-huxfkYUho4OQlFfUQ
EjfM1PHyV1obWuO2EPRNe3GB3YAG6Pih7s-O8K2CzDy3g_xFPFwNCPsaDWi_aG1TIH1kibKKaKmazJ3jKKZ0Rs-FB
TkiyQq_FUL1PNIHGgS5nSWDKI-QVzPbxEiSzhGrGFXiHUVBlR4lEaoXwul2Risg9_Oc9pRz9JXaWFGNmxUn-z4W-3
AkthQC3SCfklawqUwhPZRCTOgbTa2ez8MKMummmzUo_apfmI1Lh-Jmb4IOPIorDg2tjqafpockcLVy-M-cwpstbB6
zmIvYPvuh8lM11agNvDbmqE-k_dliAJ51BQvAGE3QS0EglKC-RO2p_S4L9SCv85aeWP7C4kSsRybBl6gRMHj_cFkA
rdE3L6O3EF4FcqUmQx7vpVRp9tdvJW-vVNRXVp98iHrMriMQkPBsqaboGCILgy6RDnl8N8SGYtAKUlNrcSpQhPDPj
aurawis9bxdGolFFyfLikyiYIpZYXHypCfCe6FX5TkZi2cfF4vPMpa5-9pSIScMlNj8N9Ui8QeMUUsDCbvT6IPw-P
KMXXY-KHCNORJU129CgAOxD9buFq2ztfk2yALu9zuMfCi8fOXvOifHh4M_M358mNjmXbX-pH1GblxGjwzjXPiL20p
OTLMn-geEhAM51so230_YkWHQsUoXHygPCMCKRtJU8L5HgVqeq7VIAPkyWk7X_eqHZ_iuIP9NttekOvxwtm58yk51
INsXOJPsF0blkorGGeDKGR4zJ3sD3ro2hR12UryNAtB9jBL2HXvUdC0IUMeb-_kbmm1Ly_78UZs0UZTgCNE4RQ9-5
8Cy6wU1T74Lx3qQJKiHU_kY8pgtCSsdhzHQU6PICmyhhQ-GugloemjSygKxUaQppPm-GZk8fX-qEU_LGT5B8ot0sk
f7b0afERMye_PRTBrbSsezkGt4HjGhBUPsIR_itnMdyLcVAfG5Aw9pNXxVmevupo13xMoz1SmfGQUxFfKzIRHoY9z
C84mfAYG4L2yi-r2Uv3VvqDcdN8N19R4rf1fzNdPK0MOY3heT-Q3o4nbHDMUtUxznn_FIMpeFHx3nPeriI2PLbOrI
zI4Bh0U_IYIT5Rz1d-cRWiUU1kcNDsBSX7h8AXEMxsq0e_Oa7E8xQBQGfHA2Ig-7m7TCMIeY5PTEaV_HrkCidhPUU
Ua_hLzW8GZOWz0XnJxWXYKjR7TZTgUJDni0atwNpA8HduZMzZQdY7sB8erYeUwz794mGfQ99sXbQf-w4lceRpgj0l
dxuDm2Gn3yZ0PC4p49RfLJyAdMSPUotvX6Xf8vfmXwY1PkMeahz78PdDvOGJPboj5OkotrsEWHOr_MmyOfjlQ3RCY
8o5-SqaLL4Q7Ed8BSMYDAgTd8RLmBhfKCV30ZoIclV53kLdxAnE_lR1HWrQfbyElErqLYWkgYlntaILGbXuLVcAsv
oOgeoD8mFb8quPe3_-q4pJDQj1gSocjo9T5KhXuNAnTdjxUD2WIrcun5T3NyT-2gT6Z6BJMIMtEH5fk-pGtPBM_o6
8lRT4GgshPRLAyf8ncww6t0uvD-KGmLOAfLB8rTtOZz3orASTvuBAkdlxH2_KrhHttq0yAWPoJK87Yb9Ney-4V5mE
UeVH3SejciX08NJFZ__zJ9aoaqkdUT05lMuLf8WSYCQoDsPYEzGORQb41b4jw2T29N_tmpY3sxLnsaygyXY-L8cnV
iF7Q9tQy3atauZjqzwp6JGm9OvCWxHaWOS9S4FUqRSLIQFqVp_k0PNuigysM-ZuZXZG59vJ35VAno0J_UrrCaLgDD
mDbIPl1F5SkvC-nFZL3neG4BSD57Nq67l3DP6s-D_29QQ1K-V3luxsmJI7Aou6ZKs5EEu6H90tcPqBdpifRoOQLIa
4GhsQ1wcjtekX9nFUsyLdE0HAWC0RlSYytCyGaED2AtokeITXlPT1PFTBZrLMb7WVL5s_SCmCYzPtgMiA2sI1Jvwn
fTf58_jkdfN4jnp8G9DN75EQEh7QDP5ybOUonHYJhS9DSAMw9-xGlv_zUIA2_3cge2EDM3aDqt8mKaaTPTL9K3z7g
zLD4rkCRo0F5OZy7DKx541vhPNK7KL1eoi9cBVYzgpT7z_41RBaPxexKa3ocZREUa2GoQPS5QJNkbMxOaWSwkAELm
2U2648v1vEDxPI8lqCb7f9LMIG7c7xhUSeyP0vXs7QePSyzqepjI3NV7H33g4LzN-24DTHiH69afur7pQapfgW-Pd
SCrLt6vJ1gpg2B6JbhezOWniZHkhnF4TALhxOy8JgQQQhZhW6hpzKy69LgZT0aCz93WB83BGcup2O9iMQHFd62mdi
```

```
NXvkdFEomXmAK12O8IBTfxMa-YrRsmAp0ILi9m_jlNOl8MMqw7ypJcwsSUbNoKilxYELf4mP-Z8BZPifxJFb0mpVD
TBjLR2ghFzz7IBUCz1zSbLXZ_pa0SMQT9JatAm2s1m5Od5aRCFDyPMmI6fpcS4hmtq28WiA-o3PI0XLf9Jw-Vz_CG
CRYLlyJRBwdlE7jNtqu5fNXVNkg4hPzmXq5epAmFzXj1-nGlIvoOJyMha9E6Z235Xb9_kg7-8THP2J86WE_bSZaHy
mTVX8kQfj7UT8XY9wJKAeo0n68bXebqpzKBnQdogTgAdxcbRY8sIO-Z0DAxNWZRin129E2MBsVNr0XDVRcA1c208g
QtNkdwbpZhQLbB6-FBzNC9VN7EWdXk2EbKrWN7qTE69ydZGIrR2gOfj922GtvwlNFMteoQw1XB-0fCNZ_3KhB-JiT
PsQNdDDEw4ouV0qimPlIuULotzi2ziYyQtRU1lVuTkqWXdC3VVQkqG4iFwWBOQRunbui94ubxOaQ-UpszGMRB1Sxy
eN3w2CRCbVOFATGkFRfllthYbwonmCpQ9YmwkEgX8kiJyV5w86i1ZHJMMXtzXH8mEfVvPjprYu0OCue3_8haQyFwj
MnHnRrS5iKd03ieK2y7y5KFAny1qIBjsU7Z3PzmRd_aCsH3x6u7MRstVuh_8RfLgf11pUrwk20hF7KJ-fOeQcEzp-
quYvSYCvAlNHt-GmQ-VtCM3TKHxLSnCvXhkDKOG7hbK6krmWDgLq_5gAFFyssMFWWmKrI4OTp7AAwNVqAgYyTlqy_
xs7p8fIDBQoQNEuLoKm1z-wYJy41R0tUZHaCho7HzvYAAAAAAAAAAAAAAAAAAAAAAAAAAAAADx8rOtwyUs6Vrwwgx
3-9gwj_0TKeQqdIymRzWjNa8MJmTR-a1pxX67V2By7QycfQffrH73lTOkLyGZ1Zd-Kj1rmxsEc",
  "raw_randomizer": "0fd19763f5682f77d81c75c6aa9317972a52644a2847f778aa31e93f599a544b",
  "raw_to_be_signed": "436f6d706f73697465416c676f726974686d5369676e617475726573323035060b6086480186fa6b50090103000fd19763f5682f77d81c75c6aa9317972a52644a2847f778aa31e93f599a544b15ab5eb43417274ea7e3e40bbd0eea7394cd3c5de78b7b931f2dab08ee854148",
  "raw_composite_signature": "0fd19763f5682f77d81c75c6aa9317972a52644a2847f778aa31e93f599a544bd496f673d960e7b5a99a7ec9fe86ec5f918521a383909457d44048df3353c7c95d686d6b8ed843d135edc60776001ba3e287bb3e3bc2b60b30f2de0ff114f1703423ec6835a2fda1b54c81f59226ca29a2a66b32778ca299d11b3e1414e48b242afc550bd4f3481c6812e674960ca23e415ccf6f11224b3846ac615788751506547894
46a85f0ba5d918ac83dfce73da51cfd257696146366c549fecf85bedc092d8500b74827e495ac2a53084f6510933a06d36b67b3f0c28cba69a6cd4a3f6a97e62352e1f8999be0838f228ac3836b63a9a7e9a1c91c2d5cbe33e730a6cb5b07ace622f60fbee87c94cd756a036f0db9aa13e93f765880279d4142f006137412d04825282f913b6a7f4b82fd482bfce5a7963fb0b8912b11c9b065ea044c1e3fdc16402b744dcbe8edc417815ca94990c7bbe9551a7db5dbc95bebd53515d5a7df221eb32b88c4243c1b2a69ba060882e0cba4439e5f0df12198b4029494dadc4a94213c33e36aeadac22b3d6f1746a25145c9f2e29328982296585c7ca909f09ee855f94e4662d9c7c5e2f3cca5ae7ef6948849c325363f0df548bc41e31452c0c26ef4fa20fc3e3ca3175d8f8a1c234e449535dbd0a000ec43f5bb85ab6ced7e4db200bbbdcee31f0a2f1f397bce89f1e1e0cfccdf9f263639976d7fa91f519b9711a3c338d73e22f6d293932cc9fe81e12100ce75b28db7d3f62458742c5285c7ca03c2302291b4953c2f91e056a7aaed52003e4c9693b5ff7aa1d9fe2b883fd36db5e90ebf1c2d9b9f32939d4836c5ce24fb05d1b964a2b186783286478cc9dec0f7ae8da1475d94af2340b41f6304bd875ef51d0b421431e6fefe46e69b52f2ffbf1466cd14653802344e1143dfb9f02cbac14d53ef82f1dea4092a21d4fe463ca60b424ac761cc7414e8f2029b286143e1ae825a1e9a34b280ac54690a693e6f86664f1f5fea8453f2c64f907ca2dd2c91fedbd1a7c444cc9efcf45306b6d2b1ece41ade078c684150fb0847f8ad9cc7722dc5407c6e40c3da4d5f15667afba9a35df1328cf54a67c6414c457cacc8447a18f730bce267c0606e0bdb28beaf652fdd5bea0dc74df0dd7d478adfd5fccd74f2b430e63785e4fe437a389db1c3314b54c739e7fc520ca5e147c779cf7ab888d8f2db3ab233238061d14fc86084f9473d5df9c45689453591c343b01497ee1f005c4331b2ad1efce6bb13cc5005019f1c0d8883eee6ed308c21e6393d311a57f1eb90289d84f51451afe12f35bc199396cf45e727159760a8d1ed36538142439e2d1ab7036903c1ddb99333650758eec07c7ab61e530cfbf789867d0f7db176d07fec3895c791a608f495dc6e0e6d869f7c99d0f0b8a78f517cb27201d3123d4a2dbd7e977fcbdf997c18d4f90c79a873efc3dd0ef38624f6e88f93a4a2daec1161ceaff326c8e7e3950dd1098f28e7e4aa68b2f843b11df0148c6030204ddf112e60617ca095df466821c955e7790b77102713f951d475ab41f6f212512ba8b6169206259ed6882c66d7b8b55c02cbe83a07a80fc9856fcaae3dedfffaae29243423d604a8723a3d4f92a15ee3409d3763c540f6588adcba7e53dcdc93fb6813e99e8124c20cb441f97e4fa91ad3c133fa3af25453e0682c84f44b0327fc9dcc30eadd2ebc3f8a1a62ce01f2c1f2b4ed399cf7a2b0124efb81024765c47dbf2ab847b6dab4c8058fa092bced86fd35ecbee15e661147951f749e8dc897d3c349159fffcc9f5aa1aaa47544f4e6532e2dff16498090a03b0f604cc639141be356f88f0d93dbd37fb66a58decc4b9ec6b28325d8f8bf1c9d5885ed0f6d432ddab5ab998eacf0a7a2469bd3af096c47696392f52e0552a4522c8405a95a7f9343cdba2832b0cf99b995d91b9f6f277e55027a3427f52bac268b8030e60db20f9751794a4bc2fa71592f79de1b80520f9ecdabaee5dc33fab3e0ffdbd410d4af95de5bb1b26248ec0a2ee992ace4412ee87f74b5c3ea05da627d1a0e40b21ae0686c435c1c8ed7a45fd9c552cc8b744d070160b4465498cad0b219a103d80b6891e2135e53d3d4f153059acb31bed654be6cfd20a6098ccfb60322036b08d49bf09df4dfe7cfe391d7cde239e9f06f4337be4440487b4033f9c9b394a271d82614bd0d200cc3dfb11a5bffcd4200dbfddc81ed840ccdda0eab7c98a69a4cf4cbf4adf3ee0ccb0f8ae4091a34179399cbb0cac79e35be13cd2bb28bd5ea22f5c0556338294fbcffe3544168fc5ec4a6b7a1c6511146b61a840f4b94093646ccc4e6964b090010b9b6536eb8f2fd6f103c4f23c96a09bedff4b3081bb73bc615127b23f4bd7b3b41e3d2cb3a9ea63237355ec7df78382f337edb80d31e21faf5a7eeafba506a97e05be3dd482acbb7abc9d60a60d81e896e17b33969e26479219c5e1300b8713b2f09810410859856ea1a732b2ebd2e0653d1a0b3f77581f3704672ea763bd88c40715deb699d88d5ef91d144a265e600ad763bc2014dfc4c6be62b46c980a7420b8bd9bf8e534e97c30cab0ef2a49730b1251b3682a29716042dfe263fe67c0593e27f12456f49a95434c18cb476821173cfb201502cf5cd26cb5d9fe96b448c413f496ad026dacd66e4e7796910850f23cc988e9fa5c4b8866b6adbc5a203ea373c8d172dff49c3e573fc21824582e5c89441c1d944ee336daaee5f35754d920e213f3997ab97a90261735e3d7e9c6948be8389c8c85af44e99db7e576fdfe483bfbc4c73f627ce9613f6d265a1f2993557f2441f8fb513f1763dc092807a8d27ebc6d779baa9cca06741da204e001dc5c6d163cb083be6740c0c4d5994629f5dbd136301b1536bd170d545c035736d3c810b4d91dc1ba598502db07af85073342f5537b11675793611b2ab58deea4c4ebdc9d64622b47680e7e3f76d86b6fc2534532d7a8430d5707ed1f08d67fdca841f898933ec40d7430c4c38a2e574aa298f948b942e8b738b6ce263242d454d6556e4e4a965dd0b7555424a86e2217058139046e9dbba2f78b9bc4e690f94a6ccc63110754b1c9e377c3609109b54e1404c690545f965b4761bc289e60a943d626c241205fc922272579c3cea2d591c930c5edcd71fc9847d5bcf8e9ad8bb4382b9edff
```

```
f21690c85c233271e746b4b988a774de278adb2ef2e4a1409f2d6a2018ec53b6773f399177f682b07df1eaeec
c46cb55ba1ffc45f2e07f5d6952bc24db4845eca27e7ce790704ce9faab98bd2602bc094d1edf86990f95b423
374ca1f12d29c2bd78640ca386ee16caea4ae658380babfe60005172b2c30559698aac8e0e4e9ec0030355a80
818c9396acbfc6cee9f1f203050a10344b8ba0a9b5cfec18272e35474b54647682868ec7cef60000000000000
0000000000000000000000000000000000f1f2b3adc3252ce95af0c20c77fbd8308ffd1329e42a748ca64735a33
5af0c2664d1f9ad69c57ebb576072ed0c9c7d07dfac7ef79533a42f2199d5977e2a3d6b9b1b047",
  "raw_composite_public_key": "ba71f9f64e11baeb58fa9c6fbb6e14e61f18643dab495b47539a9166ca
0198131c44f826bbd56e34e55db5e5e2d733485e39ea260fc6000c5ea4ba80d3455cde53b46f34482aedfd545
0fc2e1ba4f25d15f9c144242fb39bb52287189030c50498e1717b7c758b190a6748ea9aa3f7acaaf2c7cb526e
d717c9f79aeb84214fa5cd8ded92a0c3fa1558810f12c7050a367708d196cd24e5af974904aed8e4ce8872e86
96b0b7bca50e452cd7d30ea9a4adac0311d672c6bde8496240b07431463708895cd9bafc31632d7397649388f
dafcbf7d305a3de9a495eca7433a8f83ba0f0b25c413c6e39c96eb7d691b34d37ce37f1eead1cf217e25ef34e
ecf3f7c60f84b8edfdde8405d4f832576c61ef98e0a2f28da187700953924f686b94614705bcf53d33fedd434
8edddbdf28b5065e1f20775043e85cf931f829179363a1a7e7404a838ec00086b0976386fe637c98244757e3f
769ddd4467471bfad670f9a05f8246ee50a7b1eaf87fc4069c3ae2aa2033258117792f0bcd49e083fd1bc7496
abff29cc94e4868b21214ed316525399a610fbdd4a80e7c80715f29578e2a84bb40bdddbd9f47a11b6e7da118
a1b658d359e8aef55eb46b5376b5b655979984a922beebfc59bcd600d5309dccd72dbf0787db8ba757b537c1e
afd5c0f50ea4bc9583549e2829a42c28cac248c96d78124c47159b18aedd754aba17b19d430fb78f633ea9d26
f54a9bd50f8d8f6b73594f828976e7ea09c53bbb9f11a56c9507fb89b9a5ebc037a37267a95f85b8d64ca9719
2b10a66f417b3f61fe9ca57130a48fd925eae2ab5502d571c8a51903c1d398f4c1f76a7e11743976afdbc697f
23094a3cd761ff9685de32e09fb3c28add453490300bc7c89dc0178009607172294577 5f264e1b0623bcf4619
c712c838761205d87691b75ef360196cbb9e9b92a0d4c4ed62326e5024d77510b8ee2c7426cc22eae209dc9f1
3bde6bf08f5e7181bd3b459450b451a51539a715c21d67dd330eb5970db00d9edbfb2822b036fa13bafeb86d8
dc78866e3f8d43e53d78cca5595a6faf886b5dc112f1cf4adcfa875800d90b48883af97316fe1506873fc157e
570eacbfd222868d14234101966afb6bf9940829253a953ada89fc756b6a849f70acb9838e69faa50bba75e3e
89c2adb57e86d088ab9b04a28e670709172243ec5e0008a5ceaf3f8722f487302596ffd755ad1b82a49c34b34
69515b46aa290cd86ee38ea7a9be3f103610335b531cca333ddfe32b14510f4b07ef95fc6684e8c454a92c10d
bb5d59c7a7c63fb305fe881967d99e669eb632840582560bb403431d40f75a4954908482278292821f4ea91e4
2e78fa48caee3c836146dcfd738d117e92e9a15137d28e8e6a4b4622650cb413504cb3a335d44beec5746c1c2
94b1e8cb99cb608d928f8ce3563632c521f23d13c61a8f61c01df8c96c7360db4f3c68aa5d2fdd342a62ff345
9c116389421ab43e8584c45882b50e6e4e96db6f0b8fde890d5dbfadcd88690b449e64240ddb2023747f30836
3e301aa77757169fc6150628d5920b5aa1ab1c8cbf44cb00e025d7879d72b479e3af5311c785725590da9c89b
9fc3b8450769554eb44d203eba2bbaef9cad2237011c2ea44eff00f299a48ffe28ca93ddf85f76608242ef8d6
cc24610a1e2078fcac4f9385c314905ecaa82e553916d94d1a7c1ec652aa08897083daa2ebb1775fbc471ae27
777d7904ea9f1b92bcac3d8a3158426087b645b1108f0d65fec93789c053743ca14fd63d05e98b652df2b9c2f
f9ce05f1940703ffb273f80e0e2732eca9960d981b4cfd3b7bb8045b3c3830546b9dd8db0dbf592d961641d2f
caddae18a8cdb7ac2728a01ac717f90e1d1f315dc29b07c1e7b7021e638508af4ecae2859c74927af35e86e03
d1e587fc5e472a2f10d856b7"
}
```


Figure 1: ML-DSA-44-ES256


```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "4cT9Q1VAUkl8mhuxioA9ZViGLsDoySnT0ZdDr4yHkyo",
    "kty": "AKP",
    "alg": "ML-DSA-65-ES256",
    "pub": "QksvJn5Y1bO0TXGs_Gpla7JpUNV8YdsciAvPof6rRD8JQquL2619cIq7w1YHj22ZolInH-YsdAkeu
Ur7m5JkxQqIjg3-2AzV-yy9NmfmDVOevkSTAhnNT67RXbs0VaJkgCufSbzkLudVD-_91GQqVa3mk4aKRgy-wD9PyZ
pOMLzP-opHXlOVOWZ067galJN1h4gPbb0nvxxPWp7kPN2LDlOzt_tJxzrfvC1PjFQwNSDCm_l-Ju5X2zQtlXyJOTZ
SLQlCtB2C7jdyoAVwrftUXBFDkisElvgmoKlwBks23fU0tfjhwc0LVWXqhGtFQx8GGBQ-zol3e7P2EXmtIClf4Kbg
Yq5u7Lwu848qwaItyTt7EmM2IjxVth64wHlVQruy3GXnIurcaGb_qWg764qZmteoPl5uAWwuTDX292Sa071S7GfsH
Fxue5lydxIYvpVUu6dyfwuExEubCovYMfz_LJd5zNTKMMatdbBJg-Qd6JPuXznqc1UYC3CccEXCLTOgg_auB6EUdG
0b_cy-5bkEOHm7Wi4SDipGNig_ShzUkkot5qSqPZnd2I9IqqToi_0ep2nYLBB3ny3teW21Qpccoom3aGPt5Zl7fpz
hg7Q8zsJ4sQ2SuHRCzgQ1uxYlFx21VUtHAjnFDSoMOkGyo4gH2wcLR7-z59EPPNl51pljyNefgCnMSkjrBPyz1wiE
T-uqi23f8Bq2TVk1jmUFxOwdfLsU7SIS30WOzvwD_gMDexUFpMlEQyL1-Y36kaTLjEWGCi2tx1FTULttQx5JpryPW
6lW5oKw5RMyGpfRliYCiRyQePYqipZGoxOHpvCWhCZIN4meDY7H0RxWWQEpiyCzRQgWkOtMViwao6Jb7wZWbLNMeb
wLJeQJXWunk-gTEeQaMykVJobwDUiX-E_E7fSybVRTZXherY1jrvZKh8C5Gi5VADg5Vs319uN8-dVILRyOOlvjjxc
lmsRcn6HEvTvxd9MS7lKm2gI8BXIqhzgnTdqNGwTpmDHPV8hygqJWxWXCltBSSgY6OkGkioMAmXjZjYq_Ya9o6AE7
WU_hUdm-wZmQLExwtJWEIBdDxrUxA9L9JL3weNyQtaGItPjXcheZiNBBbJTUxXwIYLnXtT1M0mHzMqGFFWXVKsN_A
IdHyv4yDzY9m-tuQRfbQ_2K7r5eDOL1Tj8DZ-s8yXG74MMBqOUvlglJNgNcbuPKLRPbSDoN0E3BYkfeDgiUrXy34a
5-vU-PkAWCsgAh539wJUUBxqw90V1Du7eTHFKDJEMSFYwusbPhEX4ZTwoeTHg--8Ysn4HCFWLQ00pfBCteqvMvMfl
cWwVfTnogcPsJb1bEFVSc3nTzhk6Ln8J-MplyS0Y5mGBEtVko_WlyeFsoDCWj4hqrgU7L-ww8vsCRSQfskH8lodiL
zj0xmugiKjWUXbYq98x1zSnB9dmPy5P3UNwwMQdpebtR38N9I-jup4Bzok0-JsaOe7EORZ8ld7kAgDWa4K7BAxjc2
eD540Apwxs-VLGFVkXbQgYYeDNG2tW1Xt20-XezJqZVUl6-IZXsqc7DijwNInO3fT5o8ZAcLKUUlzSlEXe8sIlHax
```

```
jLoJ-oubRtlKKUbzWOHeyxmYZSxYqQhSQj4sheedGXJEYWJ-Y5DRqB-xpy-cftxL10fdXIUhe1hWFBAoQU3b5xRY8
KCytYnfLhsFF4O49xhnax3vuumLpJbCqTXpLureoKg5PvWfnpFPB0P-ZWQN35mBzqbb3ZV6U0rU55DvyXTuiZOK2Z
1TxbaAd1OZMmg0cpuzewgueV-Nh_UubIqNto5RXCd7vqgqdXDUKAiWyYegYIkD4wbGMqIjxV8Oo2ggOcSj9UQPS1r
D5u0rLckAzsxyty9Q5JsmKa0w8Eh7Jwe4Yob4xPVWWbJfm916avRgzDxXo5gmY7txdGFYHhlolJKdhBU9h6f0gtKE
tbiUzhp4IWsqAR8riHQs7lLVEz6P537a4kL1r5FjfDf_yjJDBQmy_kdWMDqaNln-MlKK8eENjUO-qZGy0Ql4bMZtN
bHXjfJUuSzapA-RqYfkqSLKgQUOW8NTDKhUk73yqCU3TQqDEKaGAoTsPscyMm7u_8QrvUK8kbc-XnxrWZ0BZJBjdi
nzh2w-QvjbWQ5mqFp4OMgY94__tIU8vvCUNJiYA1RdyodlfPfH5-avpxOCvBD6C7ZIDyQ-6huGEQEAb6DP8ydWIZQ
8xY603DoEKKXkJWcP6CJo3nHFEdj_vcEbDQ-WESDpcQFa1fRIiGuALj-sEWcjGdSHyE8QATOcuWl4TLVzRPKAf4tC
Xx1zyvhJbXQu0jf0yfzVpOhPun4n-xqK4SxPBCeuJOkQ2VG9jDXWH4pnjbAcrqjveJqVti7huMXTLGuqU2uoihBw6
mGqu_WSlOP2-XTEyRyvxbv2t-z9V6GPt1V9ceBukA0oGwtJqgD-q7NXFK8zhw7desI5PZMXf3nuVgbJ3xdvAlzkmm
5f9RoqQS6_hqwPQEcclq1MEZ3yML5hc99TDtZWy9gGkhR0Hs3QJxxgP7bEqGFP-HjTPnJsrGaT6TjKP7qCxJlcFKL
Ur5AU_kxMULeUysWWtSGJ9mpxBvsyW1JuraxZ3SSYIXAV2pD29U-wpi-RrpF9EUGje3th-5QGywro6eU0ENNpl-hr
V-5Jm2kyEZPSxCCriRfcSqiRdyCnjR",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws": "eyJhbGciOiJNTC1EU0EtNjUtRVMyNTYiLCJraWQiOiI0Y1Q5UTFWQVVrbDhtaHV4aW9BOVpWaUdMc0R
veVNuVDBaZERyNHlIa3lvIn0.SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb3V0IHlv
dXIgZG9vci4.-g7hBwk8qVgbzmN6qPbmMrBy2nbZZRP0MmUMfRvSxpwSAi7p5jIwEQCNu4IT9K9AJWZHXzc2GQ0l5
iQG-1dTKxzM3Q-0Iaolk_YDHJA8ykPYWB03GvJoy1Xqw2BcMYysjVnh4IQrVxsEeTkB3OpaWiZRZ4fgqA4Q75gh01
iOvWwqM8kZVG1y4Eg06SwyZZ07Mvz77tPPWiLHRYsJyaX3T8M0H3ogpo4KDLUuEG8L-lfKFYgLRG0Y31yhMpNgDDZ
Cz9FgEudK4o6qcJm40u52ZS8i7fDGF1OQmL14v7pJdiSkxfMONV5wX_o98kiqhprPRk5D8GdxT0ZXHvRRaIhu_JHG
uLl3FsQHkqYBiEEAu8PNHkCpJmiou9kAMnriHftDzL-NBQLiN7VjgmUA6jolxzxRUMEzf4Q5IqUNW93si-rBCeY1O
O9KxYQwbSXhdbu5yo728WRNCuH4oN3NRbkiNKt-uN2dCgndjGa0XMG45sIdNUO4dphjmi_hhx-Ft0ZmSj6JltKm2u
cAt8RV133IGabhppCYnqtKyjo09SmK5kGXms4tpqxNM4LTjZxi1nwHvDc-9_1gg_6Z9rkhHBgnJELIw-tMgs2-FNx
X7bA6kayvqN_gcbR-f4OoqhpOJ2denpKJ5esX5lXLVKRy8K0TzlliO0QHM5eKAhfCD0PC2KdBT2C9La-KhDEhADMz
TlUGfMfRn6_mBY66UA1-A4QVIzr6Y4-QbuPDS0nrW2ECs0by1FNZ_fpNH5ROLFhEP3a2ZI3waWak9QIlxGkGijVfy
2YlOXLpsP1FQlw97NEPyinPwqSIuC32VEoApg6m3KLJrCM2HIK7AF9d_uYsM7i8gjJ4QySFZANJHf630SWufU0Hc0
A7HS52cCVachbOqzPci17U2jqcHrnr9eRWjKpCtFvuRlCsRGTd0B1fJ1awMw16ZvbhXX5BjyYq-ZlWOHA3k7pVbWl
eYtlWReB-vwmVwbT4oHdP-h3dfPvYlMB61uI3r3radi1ChFhKYT1wlhWtJ0aDPLacqO2gN-4sYqDbW23TnJKvh8Tf
8obxe1MbX-jl9sKtCMlID8r7whxvVXH_EYCAqFtRqqXR00pQzTxPnh58Unt3__qznbL4yN_YDACskeGliiBYosQg1
7bqSe6RWKZpYC0ATB_5VWu2mbU1kSqTkpFecrc-l4WOG1KD9QbkRBB3GOzGKABoUQXtxZzl_CZxZMqH9U7frZIZuy
JStcGKZr_AfQ_7l5NQ69bHxswhjvsfzdcY84CUdFmiqx73Rb3iBn0_xaCca3zkCNBcU3AxGErXbIUgAKW7Kd8GIPw
ZZhD6mQcT-CJD2Dj1zzzvzxFLLXjvai0CLB6HXOs0bYVQxtXIfqpfW9oOPab-M4JEAflREEO_tpGb5ysQtsLERrRX
jf1zhtRd4OMJcYlcB-k63n6qxNjIkY99xpOSTs1K2TKp9HYCgJUqxRwe3ESwAP9yImoHsRbfkZWBZ8LxLJYJiiJbC
utaDcKmsieOvUvudkv5g0e5RlBYVlm7tfleMs6QNTBL5TCHKlkg7DQ8hr1yesaI312KfDrHETPRUMoOK-dkAh7Od-
xBfnDsEFjgKLWOH56qQZxGMCHOdYPhq-Nzlo-nZaEiXAGKLsiFY2OGK9xwBZ8yoOG4X2thn54OuLbRtuF_O7zdqLb
IaEZWziUWWpW7PSXyGt8aZraaNbnGIpprUPkRObPCroL7d8m7-5CrJKtN6XMRddpvfepL09Dz6FarRlTbMB00cwjc
qwikixkU_A6usqve6SniF8WXLWUEMA_9i9iUTgII78HAU1E68E40VYgpC9DT2LB-5hu67jzlaW9iitEYxtgXnl_yc
h8oFiTphDRByMzVawJ7pkvrc-uMBZfxOEW62YK7dkrSRLqzUYPlUq2NLOHXZV5qpZilDbFBFj6wbluzONUl5NQF3N
8LgPpP4_5vfTp0L1MI-XmNG6KjI_7RxFxBSWw3XUHbdldL4cmw4PsZlbgLgLIibONa3QWzfdMo_Dv3BW1WsTlxUyV
_n50C8lhLrWVvmu32N2HQez_pEAFFhtn6OEOeZ7d8Kr8n8MzP4O8sLWQoUmjB6U9gsyO1HpEU54TH2j7DE4wd_69R
r79ebJ88zo7Z_Lv4dffULy1ogHstXldn6OCvuMm57n77ms7q89AST2HuSpWs4iKrG1bBxKdn-D9vkjC6nV-pCWzkn
WjMyHtTxFT7FcEVLxyWH_O09WJ_p5J_21IqkvA082OC_i15bXu63gO8a6vfd14Uc88ZIYYMyxZcC5M0fDwx6Cc8Fw
gZz5cEXJPzUvZf0v9NHdAQIBQoG-bK_68ccJNEVt1_jdNXHqMsnpafyjsXG0pRa2SmxhlhzkwXlSxLC0AgTXdmK6h
wwmk68VeUpMmPA2F-xnbkKlXeiFM7PG37oCyvAYuOg8WdHe_HqvneyENizqzES3qTqRRSm4pKJaeNe62WfjbUm0iD
c7qA7kwZineyq89SVMhmmdreDXFriEecu0Jski65R2SDya7HGMCbBTCtVczVR9DQidQWeO-_TbghhGfbUcdIv-m1z
-r95iam-DQD_eJ4FNasJB8QGqS3Om3u7elPrv2J7LuAW9M9zPs4K61HOvk8YzkAAlV3A9Dt0ULqWqCoDYafZu62RY
0OeuVziTOIGNR8LtfP-Mc3CLzWgQ0TIeMvZ2iba4Jp34DFIOrGCG9PNVJHaJRher1mXaxGGpDU1BlQPH531rXE6gW
llgCSW5kJ5JMPAyamSXMf28UKLULi1MCNIItNFBp_bByrnOdLie6SCz-zZJPXuVk_MuAtXMPigkiGNdV6aCtXXCo_
FbJw3uioA4wMPSZujqC3tQKBZxyl3-5muZBfsCElQQDABQ7rrnF0UGHBwtGd-gszeu5FzMFBBT5giUlpA4VNbNLHX
ISmgtHv8ImBMe1D6VK9X3-49WfTQ1p7mRR9gR24hHllTE0kyQ8_J6ojW1CcgoR_8RH9Lk6Au3hVDAJ1BcWpaL7jzY
C-4BV4AMPWr4kFumezxG8-u9FwlwP6W0SYyjQ_HR73oWuNR1SqS55mtGJCuctYEVnepiGlm0GpBXUKIIM2512XLcm
Yrg97iJEY-coOv0wGrjc-rj6zGZvhV3JCrbdVtf-dlZLy5tVTfdEv3Z1OZixKviSQjtbAzkJ9EtVcTZJUv1r8bv1f
eDfXqq01z-mb0iH-jSzSfIW7NLsGciKn2YMBkxR5cxRycaDo-IutvVYgHgM70fGMZ3e0VJVi9q9K8IU6jjMSZqxWl
6jNN8kM8vLsVswLzw_nQ4Axc9trFHiP_Xo0X7XqHtqVjQ_xUGQcWQbiePjzjfnAwxzZSEK54VCkDVtmPkIkCE8mYD
YWayM48LhmHGYhEP7m0c2-cLBe5ys9zkn06KUdqTcffl-ubqubg_QPIcXN_x61qXYc0zAmWk9scBMiR3oLn0VlhjA
ZyG-1TwW5arEouUNaVPA3T0_3PoheXc8vwoGdodu6xMF3-cB1fQiZMMT6TOwrKR-YggwZHs2gIyptcwiH8_jMpCgw
aThlw7z-F5b-Dka7NmAK2yYc7edqMZT9OWD62CUp6F-4Lqe8Qh6QaCaIowEx68EUYPyNlCcxa6TP3BFBQR0dzUeLf
arvm9ougr11v35Zzy9OswjgO0fe5gXYT4QuSZ5queY9tWJD9OvYSA2qOn9xzxJbTEToRiLMGfYSU7Y0L5LYsnpZRT
MCVu_vCWdDzo_Kp4qNU6ZheM8nBuAAKf8Lwqxgk20L8tTPPukiRdjNseMK6t9hex3dDLh5rG8NbldGsGsI_-wTOZW
n7BvULU7ZXNB_U0lPez-pQWXYgLC_uIT5JOL460i43otepJy2XJkI9X7aE6RGvpHwI6coPqGwq12iBWfQmfwAgYhN
DEzlD7L4DuQGIZu9d90saJ6JpFC21Gg2YL0Lvw49EzyH654fFwpC-Ff8JoITaZRyqh5bC31ufw6TYBnViuq1Z59Qz
R0DIY_IuNm_PXTfJaYRn0zACqJzKs0FYd2_QpM-PBTg35VM-U2322IGC3xWfJUQHZnAXYX4gEJootljHLTmnu1ocg
BHVfLZ7dxSLSMmpjiLYXyjxS2znZT5pocI9g2O_bSzuaxRgazjJG_HwrGifU88-1yND5ckuyIxOGvQgyodoL63dAo
OZ7E1fUIUBwc_RS31zKP6B18F6m0al0JK0COMxjvFVjKNZ9F1KvfzBu1rFeGrXfIFpo48NxT6u2YDwDc7cn6nAZfE
8sfMv9JjDF32DmXWaY7Ku_8NXcm3s-DNTGHa886e-TLjBZg4paWr58tUt5dRqJbQFTT6LXabHHOn7p9cy3H8fYdDL
```

```
EMF8cna0nkA_kFWExRHV3Oygg0TLlHhJUFmd5sbQ4C9zNJeyg4kW2PN0f4CGzjS0wAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAFChASGR4fu_nzDVvTr0ndl0cYMi4DuaUVyIaqN7Aw6wpmcS3SELIDnYZ4EyI_JjdblADcNUNCvjUtuOi
DtlrsUQCDMPRN",
  "raw_randomizer": "fa0ee107093ca9581bce637aa8f6e632b072da76d96513f432650c7d1bd2c69c",
  "raw_to_be_signed": "436f6d706f73697465416c676f726974686d5369676e617475726573323035060b6086480186fa6b5009010800fa0ee107093ca9581bce637aa8f6e632b072da76d96513f432650c7d1bd2c69caaff7641ad9cd7aa5fc022756f1b8b5dbd4404843ac970cfd871a441f293b34cc33bc00c1701a0ac62ac4879c018145eaa7158bb9ee052df5575e676c0dcf106",
  "raw_composite_signature": "fa0ee107093ca9581bce637aa8f6e632b072da76d96513f432650c7d1bd2c69c12022ee9e6323011008dbb8213f4af402566475f3736190d25e62406fb57532b1cccdd0fb421aa2593f6031c903cca43d8581d371af268cb55eac3605c318cac8d59e1e0842b571b04793901dcea5a5a26516787e0a80e10ef9821d3588ebd6c2a33c919546d72e04834e92c32659d3b32fcfbeed3cf5a22c7458b09c9a5f74fc3341f7a20a68e0a0cb52e106f0bfa57ca15880b446d18df5ca13293600c3642cfd16012e74ae28eaa7099b8d2ee76652f22edf0c617539098bd78bfba497624a4c5f30e355e705ffa3df248aa869acf464e43f067714f46571ef45168886efc91c6b8b97716c40792a601884100bbc3cd1e40a92668a8bbd900327ae21dfb43ccbf8d0502e237b563826500ea3a25c73c5150c1337f843922a50d5bddec8beac109e63538ef4ac584306d25e175bbb9ca8ef6f1644d0ae1f8a0ddcd45b92234ab7eb8dd9d0a09dd8c66b45cc1b8e6c21d3543b87698639a2fe1871f85b746664a3e8996d2a6dae700b7c455d77dc819a6e1a690989eab4aca3a34f5298ae641979ace2da6ac4d3382d38d9c62d67c07bc373ef7fd6083fe99f6b9211c18272442c8c3eb4c82cdbe14dc57edb03a91acafa8dfe071b47e7f83a8aa1a4e27675e9e9289e5eb17e655cb54a472f0ad13ce59623b440733978a0217c20f43c2d8a7414f60bd2daf8a8431210033334e55067cc7d19fafe6058eba500d7e038415233afa638f906ee3c34b49eb5b6102b346f2d45359fdfa4d1f944e2c58443f76b6648df06966a4f50225c469068a355fcb66253972e9b0fd45425c3decd10fca29cfc2a488b82df6544a00a60ea6dca2c9ac23361c82bb005f5dfee62c33b8bc8232784324856403491dfeb7d125ae7d4d0773403b1d2e7670255a7216ceab33dc8b5ed4da3a9c1eb9ebf5e4568caa42b45bee4650ac4464ddd01d5f2756b0330d7a66f6e15d7e418f262af9995638703793ba556d695e62d95645e07ebf0995c1b4f8a0774ffa1ddd7cfbd894c07ad6e237af7ada762d4284584a613d709615ad2746833cb69ca8eda037ee2c62a0db5b6dd39c92af87c4dff286f17b531b5fe8e5f6c2ad08c9480fcafbc21c6f5571ff118080a85b51aaa5d1d34a50cd3c4f9e1e7c527b77fffab39db2f8c8dfd80c00ac91e1a58a2058a2c420d7b6ea49ee9158a669602d004c1ff9556bb699b535912a9392915e72b73e97858e1b5283f506e444107718ecc62800685105edc59ce5fc267164ca87f54edfad9219bb2252b5c18a66bfc07d0ffb979350ebd6c7c6cc218efb1fcdd718f380947459a2ab1ef745bde2067d3fc5a09c6b7ce408d05c537031184ad76c852000a5bb29df0620fc196610fa990713f82243d838f5cf3cefcf114b2d78ef6a2d022c1e875ceb346d8550c6d5c87eaa5f5bda0e3da6fe33824401f9511043bfb6919be72b10b6c2c446b4578dfd7386d45de0e30971895c07e93ade7eaac4d8c8918f7dc693924ecd4ad932a9f4760280952ac51c1edc44b000ff72226a07b116df91958167c2f12c96098a225b0aeb5a0dc2a6b2278ebd4bee764bf98347b94650585659bbb5f95e32ce9035304be530872a5920ec343c86bd727ac688df5d8a7c3ac71133d150ca0e2be764021ece77ec417e70ec1058e028b58e1f9eaa419c463021ce7583e1abe373968fa765a1225c018a2ec8856363862bdc70059f32a0e1b85f6b619f9e0eb8b6d1b6e17f3bbcdda8b6c8684656ce25165a95bb3d25f21adf1a66b69a35b9c6229a6b50f91139b3c2ae82fb77c9bbfb90ab24ab4de9731175da6f7dea4bd3d0f3e856ab4654db301d347308dcab08a48b1914fc0eaeb2abdee929e217c5972d6504300ffd8bd8944e0208efc1c053513af04e345588290bd0d3d8b07ee61bbaee3ce5696f628ad118c6d8179e5ff2721f281624e9843441c8ccd56b027ba64beb73eb8c0597f13845bad982bb764ad244bab35183e552ad8d2ce1d7655e6aa598a50db141163eb06e5bb338d525e4d405dcdf0b80fa4fe3fe6f7d3a742f5308f9798d1ba2a323fed1c45c41496c375d41db76574be1c9b0e0fb1995b80b80b2226ce35add05b37dd328fc3bf7056d56b1397153257f9f9d02f2584bad656f9aedf63761d07b3fe910014586d9fa38439e67b77c2abf27f0cccfe0ef2c2d64285268c1e94f60b323b51e9114e784c7da3ec3138c1dffaf51afbf5e6c9f3cce8ed9fcbbf875f7d42f2d68807b2d5e5767e8e0afb8c9b9ee7efb9aceeaf3d0124f61ee4a95ace222ab1b56c1c4a767f83f6f9230ba9d5fa9096ce49d68ccc87b53c454fb15c1152f1c961ff3b4f5627fa7927fdb522a92f034f36382fe2d796d7bbade03bc6babdf775e1473cf1921860ccb165c0b93347c3c31e8273c170819cf97045c93f352f65fd2ff4d1dd0102014281be6caffaf1c70934456dd7f8dd3571ea32c9e969fca3b171b4a516b64a6c61961ce4c17952c4b0b40204d77662ba870c2693af15794a4c98f03617ec676e42a55de88533b3c6dfba02caf018b8e83c59d1defc7aaf9dec84362ceacc44b7a93a914529b8a4a25a78d7bad967e36d49b488373ba80ee4c198a77b2abcf5254c86699dade0d716b88479cbb426c922eb9476483c9aec718c09b0530ad55ccd547d0d089d41678efbf4db8218467db51c748bfe9b5cfeafde626a6f83403fde27814d6ac241f101aa4b73a6deeede94faefd89ecbb805bd33dccfb382bad473af93c63390002557703d0edd142ea5aa0a80d869f66eeb6458d0e7ae57389338818d47c2ed7cff8c73708bcd6810d1321e32f67689b6b8269df80c520eac6086f4f3552476894617abd665dac461a90d4d419503c7e77d6b5c4ea05a59600925b9909e4930f0326a649731fdbc50a2d42e2d4c08d208b4d141a7f6c1cab9ce74b89ee920b3fb36493d7b9593f32e02d5cc3e282488635d57a682b575c2a3f15b270dee8a8038c0c3d266e8ea0b7b50281671ca5dfee66b9905fb021254100c0050eebae71745061c1c2d19dfa0b337aee45ccc141053e6089496903854d6cd2c75c84a682d1eff0898131ed43e952bd5f7fb8f567d3435a7b99147d811db88479654c4d24c90f3f27aa235b509c82847ff111fd2e4e80bb78550c027505c5a968bee3cd80bee0157800c3d6af8905ba67b3c46f3ebbd1709703fa5b4498ca343f1d1ef7a16b8d4754aa4b9e66b46242b9cb581159dea621a59b41a905750a208336e75d972dc998ae0f7b889118f9ca0ebf4c06ae373eae3eb3199be1577242adb755b5ff9d9592f2e6d5537dd12fdd9d4e662c4abe24908ed6c0ce427d12d55c4d9254bf5afc6efd5f7837d7aaad35cfe99bd221fe8d2cd27c85bb34bb067222a7d9830193147973147271a0e8f88badbd56201e033bd1f18c6777b4549562f6af4af0853a8e331266ac5697a8cd37c90cf2f2ec56cc0bcf0fe743803173db6b14788ffd7a345fb5ea1eda958d0ff150641c5906e278f8f38df9c0c31cd94842b9e150a40d5b663e4224084f266036166b2338f0b8661c662110fee6d1cdbe70b05ee72b3dce49f4e8a51da9371f7e5fae6eab9b83
```

```
f40f21c5cdff1eb5a9761cd330265a4f6c701322477a0b9f4565863019c86fb54f05b96ab128b9435a54f0374
f4ff73e885e5dcf2fc2819da1dbbac4c177f9c0757d089930c4fa4cec2b291f98820c191ecda0232a6d730887
f3f8cca42830693865c3bcfe1796fe0e46bb36600adb261cede76a3194fd3960fad82529e85fb82ea7bc421e9
0682688a30131ebc11460fc8d9427316ba4cfdc1141411d1dcd478b7daaef9bda2e82bd75bf7e59cf2f4eb308
e03b47dee605d84f842e499e6ab9e63db56243f4ebd8480daa3a7f71cf125b4c44e84622cc19f61253b6342f9
2d8b27a5945330256efef096743ce8fcaa78a8d53a66178cf2706e00029ff0bc2ac60936d0bf2d4cf3ee92245
d8cdb1e30aeadf617b1ddd0cb879ac6f0d6e5746b06b08ffec133995a7ec1bd42d4ed95cd07f53494f7b3fa94
165d880b0bfb884f924e2f8eb48b8de8b5ea49cb65c9908f57eda13a446be91f023a7283ea1b0ab5da20567d0
99fc0081884d0c4ce50fb2f80ee406219bbd77dd2c689e89a450b6d4683660bd0bbf0e3d133c87eb9e1f170a4
2f857fc268213699472aa1e5b0b7d6e7f0e936019d58aeab5679f50cd1d03218fc8b8d9bf3d74df25a6119f4c
cc00aa2732acd0561ddbf42933e3c14e0df954cf94db7db62060b7c567c95101d99c05d85f8804268a2d9631cb
4e69eed6872004755f2d9eddc522d2326a6388b617ca3c52db39d94f9a68708f60d8efdb4b3b9ac5181ace324
6fc7c2b1a27d4f3cfb5c8d0f9724bb2231386bd0832a1da0beb7740a0e67b1357d421407073f452df5cca3fa0
75f05ea6d1a97424ad0238cc63bc556328d67d1752af7f306ed6b15e1ab5df205a68e3c3714fabb6603c0373b
727ea70197c4f2c7ccbfd2630c5df60e65d6698ecabbff0d5dc9b7b3e0cd4c61daf3ce9ef932e3059838a5a5a
be7cb54b79751a896d01534fa2d769b1c73a7ee9f5ccb71fc7d87432c4305f1c9dad27900fe41561314475773
b2820d132e51e1254166779b1b4380bdccd25eca0e245b63cdd1fe021b38d2d3000000000000000000000000
0000000000000000000000000050a1012191e1fbbf9f30d5bd3af49dd974718322e03b9a515c886aa37b030eb
0a66712dd210b2039d867813223f26375b9400dc354342be352db8e883b65aec51008330f44d",
  "raw_composite_public_key": "424b2f267e58d5b3b44d71acfc6a656bb26950d57c61db1c880bcfa1fe
ab443f0942ab8bdbad7d708abbc356078f6d99a252271fe62c74091eb94afb9b9264c50a888e0dfed80cd5fb2
cbd3667e60d539ebe44930219cd4faed15dbb3455a264802b9f49bce42ee7550feffdd4642a55ade693868a46
0cbec03f4fc99a4e30bccffa8a475e5395396674ebb81a94937587880f6dbd27bf1c4f5a9ee43cdd8b0e53b3b
7fb49c73adfbc2d4f8c54303520c29bf97e26ee57db342d957c893936522d0942b41d82ee3772a00570adfb54
5c1143922b0496f826a0a970064b36ddf534b5f8e1c1cd0b5565ea846b45431f0618143ece89777bb3f61179a
d20295fe0a6e062ae6eecbc2ef38f2ac1a22dc93b7b126336223c55b61eb8c0795542bbb2dc65e722eadc6866
ffa9683beb8a999ad7a83e5e6e016c2e4c35f6f7649ad3bd52ec67ec1c5c6e7b9972771218be9554bba7727f0
b84c44b9b0a8bd831fcff2c9779ccd4ca30c6ad75b04983e41de893ee5f39ea7355180b709c7045c22d33a083
f6ae07a114746d1bfdccbee5b9043879bb5a2e120e2a4636283f4a1cd4924a2de6a4aa3d99ddd88f48aaa4e88
bfd1ea769d82c10779f2ded796db542971ca289b76863ede5997b7e9ce183b43ccec278b10d92b87442ce0435
bb1625171db5554b470239c50d2a0c3a41b2a38807db070b47bfb3e7d10f3cd979d69963c8d79f8029cc4a48e
b04fcb3d708844febaa8b6ddff01ab64d59358e6505c4ec1d7cbb14ed2212df458ecefc03fe03037b1505a4c9
444322f5f98dfa91a4cb8c45860a2dadc7515350bb6d431e49a6bc8f5ba956e682b0e513321a97d1962602891
c9078f62a8a9646a31387a6f09684264837899e0d8ec7d11c565901298b20b345081690eb4c562c1aa3a25bef
06566cb34c79bc0b25e4095d6ba793e81311e41a3329152686f00d4897f84fc4edf4b26d545365785ead8d63a
ef64a87c0b91a2e5500383956cdf5f6e37cf9d5482d1c8e3a5be38f17259ac45c9fa1c4bd3bf177d312ee52a6
da023c05722a8738274dda8d1b04e99831cf57c87282a256c565c296d0524a063a3a41a48a83009978d98d8ab
f61af68e8013b594fe151d9bec199902c4c70b49584201743c6b53103d2fd24bdf078dc90b5a188b4f8d77217
9988d0416c94d4c57c0860b9d7b53d4cd261f332a1851565d52ac37f008747cafe320f363d9beb6e4117db43f
d8aeebe5e0ce2f54e3f0367eb3cc971bbe0c301a8e52f96094936035c6ee3ca2d13db483a0dd04dc16247de0e
0894ad7cb7e1ae7ebd4f8f900582b20021e77f70254501c6ac3dd15d43bbb7931c5283244312158c2eb1b3e11
17e194f0a1e4c783efbc62c9f81c21562d0d34a5f042b5eaaf32f31f95c5b055f4e7a2070fb096f56c415549c
de74f3864e8b9fc27e3299724b4639986044b55928fd6972785b280c25a3e21aab814ecbfb0c3cbec0914907e
c907f25a1d88bce3d319ae8222a35945db62af7cc75cd29c1f5d98fcb93f750dc3031076979bb51dfc37d23e8
eea78073a24d3e26c68e7bb10e459f2577b90080359ae0aec10318dcd9e0f9e34029c31b3e54b1855645db420
618783346dad5b55eddb4f977b326a655525ebe2195eca9cec38a3c0d2273b77d3e68f1901c2ca5149734a511
77bcb089476b18cba09fa8b9b46d94a2946f358e1decb1998652c58a90852423e2c85e79d19724461627e6390
d1a81fb1a72f9c7edc4bd747dd5c85217b5856141028414ddbe71458f0a0b2b589df2e1b051783b8f718676b1
defbae98ba496c2a935e92eeadea0a8393ef59f9e914f0743fe65640ddf9981cea6dbdd957a534ad4e790efc9
74ee89938ad99d53c5b68077539932683472 9bb37b082e795f8d87f52e6c8a8db68e515c277bbea82a7570d42
80896c987a0608903e306c632a223c55f0ea3682039c4a3f5440f4b5ac3e6ed2b2dc900cecc72b72f50e49b26
29ad30f0487b2707b86286f8c4f55659b25f9bdd7a6af460cc3c57a3982663bb717461581e196894929d84153
d87a7f482d284b5b894ce1a78216b2a011f2b88742cee52d5133e8fe77edae242f5af91637c37ffca32430509
b2fe4756303a9a3659fe32528af1e10d8d43bea991b2d109786cc66d35b1d78df254b92cdaa40f91a987e4a92
2ca81050e5bc3530ca85493bdf2a825374d0a8310a6860284ec3ec732326eeeffc42bbd42bc91b73e5e7c6b59
9d016490637629f3876c3e42f8db590e66a85a7838c818f78fffb4853cbef09434989803545dca87657cf7c7e
7e6afa71382bc10fa0bb6480f243eea1b861101006fa0cff3275621943cc58eb4dc3a0428a5e425670fe82268
de71c511d8ffbdc11b0d0f961120e971015ad5f448886b802e3fac11672319d487c84f1001339cb969784cb57
344f2807f8b425f1d73caf8496d742ed237f4c9fcd5a4e84fba7e27fb1a8ae12c4f0427ae24e910d951bd8c35
d61f8a678db01caea8ef789a95b62ee1b8c5d32c6baa536ba88a1070ea61aabbf59294e3f6f974c4c91cafc5b
bf6b7ecfd57a18fb7557d71e06e900d281b0b49aa00feabb35714af33870edd7ac2393d93177f79ee5606c9df
176f025ce49a6e5ff51a2a412ebf86ac0f40471c96ad4c119df230be6173df530ed656cbd8069214741ecdd02
71c603fb6c4a8614ff878d33e726cac6693e938ca3fba82c4995c14a2d4af9014fe4c4c50b794cac596b52189
f66a7106fb325b526eadac59dd2498217015da90f6f54fb0a62f91ae917d1141a37b7b61fb9406cb0ae8e9e53
410d36997e86b57ee499b69321193d2c420ab8917dc4aa8917720a78d1"
}
```

Figure 2: ML-DSA-65-ES256

```
{
  "priv": "0000000000000000000000000000000000000000000000000000000000000000",
  "jwk": {
    "kid": "p1MMg8xj6mCplHRRACr5Afj_-4etB4DQLeRyFOMG1cQ",
    "kty": "AKP",
    "alg": "ML-DSA-87-ES384",
    "pub": "5F_8jMc9uIXcZi5ioYzY44AylxF_pWWIFKmFtf8dt7Roz8gruSnx2Gt37RT1rhamU2h3LOUZEkEBB
eBFaXWukf22Q7US8STV5gvWi4x-Mf4Bx7DcZa5HBQHMVlpuHfz8_RJWVDPEr-3VEYIeLpYQxFJ14oNt7jXO1p1--m
cv0eQxi-9etuiX6LRRqiAt7QQrKq73envj9pkUbaIpqL2z_6SWRFln51IXv7yQSPmVZEPYcx-DPrMN4Q2slv_-fPZ
eoERcPjHoYB4TO-ahAHZP4xluJncmRB8xdR-_mm9YgGRPTnJ15X3isPEF5NsFXVDdHJyTT931NbjeKLDHTARJ8iLN
LtC7j7x3XM7oyUBmW0D3EvT34AdQ6eHkzZz_JdGUXD6bylPM1PEu7nWBhW69aPJoRZVuPnvrdh8P51vdMb_i-gGBE
zl7OHvVnWKmi4r3-iRauTLmn3eOLO79ITBPu4CZ6hPY6lfBgTGXovda4lEHW1Ha04-FNmnp1fmKNlUJiUGZOhWUhg
-6cf5TDuXCn1jyl4r2iMy3Wlg4o1nBEumOJahYOsjawfhh_Vjir7pd5aUuAgkE9bQrwIdONb788-YRloR2jzbgCPB
HEhd86-YnYHOB5W6q7hYcFym43lHb3kdNSMxoJJ6icWK4eZPmDITtbMZCPLNnbZ61CyyrWjoEnvExOB1iP6b7y8nb
HnzAJeoEGLna0sxszU6V-izsJP7spwMYp1Fxa3IT9j7b9lpjM4NX-Dj5TsBxgiwkhRJIiFEHs9HE6SRnjHYU6hrwO
BBGGfKuNylAvs-mninLtf9sPiCke-Sk90usNMEzwApqcGrMxv_T2OT71pqZcE4Sg8hQ2MWNHldTzZWHuDxMNGy5pY
E3IT7BCDTGat_iu1xQGo7y7K3Rtnej3xpt64br8HIsT1Aw4g-QGN1bb8U-6iT9kre1tAJf6umW0-SP1MZQ2C261-r
5NmOWmFEvJiU9LvaEfIUY6FZcyaVJXG__V83nMjiCxUp9tHCrLa-P_Sv3lPp8aS2ef71TLuzB14gOLKCzIWEovii0
qfHRUfrJeAiwvZi3tDphKprIZYEr_qxvR0YCd4QLUqOwh_kWynztwPdo6ivRnqIRVfhLSgTEAArSrgWHFU1WC8Ckd
6T5MpqJhN0x6x8qBePZGHAdYwz8qa9h7wiNLFWBrLRj5DmQLl1CVxnpVrjW33MFso4P8n060N4ghdKSSZsZozkNQ5
b7O6yajYy-rSp6QpD8msb8oEX5imFKRaOcviQ2D4TRT45HJxKs63Tb9FtT1JoORzfkdv_E1bL3zSR6oYbTt2Stnpz
-7kVqc8KR2N45EkFKxDkRw3IXOte0cq81xoU87S_ntf4KiVZaszuqb2XN2SgxnXBl4EDnpehPmqkD92SAlLrQcTax
aSe47G28K-8MwoVt4eeVkj4UEsSfJN7rbCH2yKl2XJx5huDaS0xn2ODQyNRmgk-5I9hXMUiZDNLvEzx4zuyrcu2d0
oXFo3ZoUtVFNCB__TQCf2x27ej9GjLXLDAEi7qnl9Xfb94n0IfeVyGte3-j6NP3DWv8OrLiUjNTaLv6Fay1yzfUaU
6LI86-Jd6ckloiGhg7kE0_hd-ZKakZxU1vh0Vzc6DW7MFAPky75iCZlDXoBpZjTNGo5HR-mCW_ozblu60U9zZA8bn
-voANuu_hYwxh-uY1sHTFZOqp2xicnnMChz_GTm1Je8XCkICYegeiHUryEHA6T6B_L9gW8S_R4ptMD0Sv6b1KHqqK
eubwKltCWPUsr2En9iYypnz06DEL5Wp8KMhrLid2AMPpLI0j1CWGJExXHpBWjfIC8vbYH4YKVl-euRo8eDcuKosb5
hxUGM9Jvy1siVXUpIKpkZt2YLP5pEBP_EVOoHPh5LJomrLMpORr1wBKbEkfom7npX1g817bK4IeYmZELI8zXUUtUk
x3LgNTckwjx90Vt6oVXpFEICIUDF_LAVMUftzz6JUvbwOZo8iAZqcnVslAmRXeY_ZPp5eEHFfHlsb8VQ73Rd_p8Xl
Ff5R1WuWiUGp2TzJ-VQvj3BTdQfOwSxR9RUk4xjqNabLqTFcQ7As246bHJXH6XVnd4DbEIDPfNa8FaWb_DNEgQAiX
Gqa6n7l7aFq5_6Kp0XeBBM0sOzJt4fy8JC6U0DEcMnWxKFDtMM7q06LubQYFCEEdQ5b1Qh2LbQZ898tegmeF--EZ4
F4hvYebZPV8sM0ZcsKBXyCr585qs00PRxr0S6rReekGRBIvXzMojmid3dxc6DPpdV3x5zxlxaIBxO3i_6axknSSdx
nS04_bemWqQ3CLf6mpSqfTIQJT1407GB4QINAAC9Ch3AXUR_n1jr64TGWzbIr8uDcnoVCJlOgmlXpmOwubigAzJat
tbWRi7k4QYBnA3_4QMjt73n2Co4-F_Qh4boYLpmwWG2SwcIw2PeXGr2LY2zwkPR4bcSyx1Z6UK5trQpWlpQCxgsvV
_RvGzpN22RtHoihPH74K0cBIzCz7tK-jqeuWl1A7af7KmQ66fpRBr5ykTLOsa17WblkcIB_jDvqKfEcdxhPWJUwmO
o4TIQS-xH8arLOy_NQFG2m14_yxwUemXC-QxLUYi6_FIcqwPBKjCdpQtadRdyftQSKO0SP-GxUvamMZzWI780rXuO
Bkq5kyYLy9QF9bf_-bL6QLpe1WMCQlOeXZaCPoncgYoT0WZ17jB52Xb2lPWsyXYK54npszkbKJ4OIqfvF8xqRXcVe
22VwJuqT9Uy4-4KKQgQ7TXla7Gdm2H7mKl8YXQlsGCT2Ypc8O4t0Sfw7qYAuaDGf752Hbm3fl1bupcB2huIPlIaDP
6IRR9XvTYIW2flbwYfhKLmoVKnG85uUi2qtqCjPOIuU3-peT0othfmwKQXaoOqO-V4r6wPL1VHxVFtIYmEdVt0Rcc
UOvpOVR_OAHG9uHOzTmueK5557Qxp0ojtZCHyN-hgoMZJLrvdKkTCxPNo2-mZQbHoVh2FnThZ9JbO49dB8lKXP4_M
U5xAnjXMgKXtbfI8w6ZWATE_XWgf2VQMUpGp4wpy44yWQTxHxh_4T9540BGwG0FU0bkgrwA_erseGZnepqdmz5_Sc
Cs84O5Xr5MbYhJLCGGxY6O5GqS-ooB2w0Mt87KbbE4bpYje9CAHH8FX3pDrJyLsyasA3zxmk4OmGpG7Z70ofONJtH
Re56R5287vFmuazEEutXn81kNzB-3aJT1ga3vnWZw4CSvFKoWYSA7auLgrHSHFZdITfOrgtmQmGbFhM9kSBdY1UCn
pzf65oos3PZWRa2twfUxxLAnPNtrxpRGyvtsapw7ljUagZmuyh3hLCjhAxYmnoE1dbyIWvpCqSlEtVjL1yb_nuLEz
gvmZuV02fHxGuWgHTOMVGXpf81Rce3eoBK3lapW1wkzezlk3tcA2bZOtA9qbxdsbVR37kemzQ9K1e3Y0OWhtSjRqQ
mtOnSvpya53Ryy2PbQ7cZXO5g_pA-gCiwb4wjVtPLXS9zt3a7nf1VB9h9BWpkajKzgra_MfK_LbjoheW_4M89DYXa
JANLwpuQ3-Xw3pYLBRkx5ugklwCgf9teGCjq",
    "priv": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
  },
  "jws": "eyJhbGciOiJNTC1EU0EtODctRVMzODQiLCJraWQiOiJwMU1NZzh4ajZtQ3BsSFJSQUNyNUFmal8tNGV
0QjREUUxlUnlGT01HMWNRIn0.SXTigJlzIGEgZGFuZ2Vyb3VzIGJ1c2luZXNzLCBGcm9kbywgZ29pbmcgb3V0IHlv
dXIgZG9vci4.aOoS-NltTuvx-1JRpIYwIWBn7ALi8rwxM0TfNtOBg04u0c1EcNpb-4BPoPYQGZ7jBtDucKoVAooiR
l0YgYvaqRscIC1KwMk-v-T0ZEvQ9cIa4G29SLMZZZy8aSlIW-GDhWSxLm5RLTJvygkQ2YEAWglIFvlZ9S1i336ZKO
lMv_AW9HNr88HbFp2TEYG1bzfwTVZ4V5AYNyBzisD3p8DHkDCld5jwzpv0Y4KyQBH4EffcUmvMwJcowVvNax0i5Zr
onpGHPYpFSSrLGLTZPiFOu5Mj-X9zVWqbxi_2VRMdEC7ItDNgye5fKgKvFQ44We_avKMD2X09WWuTnVcCRqNE1i5O
N-GGww4IqsvgbSy2rO9tbfzsUnR_0qPPqkhqtTY7Ls51_bxhPnC-8UTLVxfRwNOP1VGSJwQoAzIV0i4phV-UGPwVn
EihCKSDgsnA5mLzHmndHJy9iWDE_DygcvhMxuL2Wo31GSLC7ljNVp8zylSBqLVCoPuYPJzubypeNFXyGWsptNdpBD
y_b51rBZvApB-UL3Mng8KJsXcEj0kZAITxF5pfod5JPfJLothT2kF2h3v-LZzvsHcYCggLZu_qEAtZj7rrmkjjXAX
mPDLtli5pXUs34_GcWx3Ct6SYnvWkdotnAKiHIrJKwL9MjESvumOv6OUng3vxRzq54AIKwc3TvQc868csAOO7OujK
gX_k4usPdUgFliVTIVcpMk8XWtQu3xYAGBL1j9Zf6hrie-CBZjIL3ncPHPz308F1W5nCIsuVctozakKH03gi0baPo
O0zlakK5kUAWGQQ8Rp4QsN0HvvCFtzjXYKvPWT7Y8vVuW6VSn1KLKpo4JtUnqQURGTqm1jc8ZN37tFQoqSgfDpKC-
fChVUZvEWYlKTs3tYVLFnwGj6SfQwGyWiE3A6VsGDE_OuIrOY0RraJtCIjjGMZ1_G5BSIvUmLT1_7IHYoUW1pFe6B
```

```
DrOQPtZyCNZd9GsDuWfJ2zOLYrZlo1AGMoJ4eR3aBf_6N2Y0uemPdXyvxKxNlFkYxHFQHH1_JqR3FLDP-bdnnkY_y
KLerd51G8RFhV9WPecpz_-H8KxEfylgokxcSKISK7TfUSgVzQ3PYEJ8UNovFDov8wPMFLCFapgGvsUxf_ziXp7I-Q
exBpqwFA_4TMuDAVP3ziaxyl-zQC-MvtsQkb0nQPFRcHW7oCpHAxpG4f62d2AtlagUKzo-NnDwtPAEC8gvfzhuWIQ
FdnWaCK7T0QihUkTlN_ywCrGJleP9AIAAcgORio9WPjSZioB8OjTU-jFJcq51nYEVW-aNSjnhZLVTPDGDsZnbgWOv
b86rjNsiDi9PD-k2anLlvCS2Ea5L-i1Ph3T6Nq-9jlof5Embw4dvF7qGRg-jOYSCq0BhCn4qHChJvfg39UVT-YYjv
p0Abbod-lFaTog7X34Md5Jkpp02FC0-_U5HqcckD-ucw9YZjlblNoB-bGsGal_aLFMKUuS26S-VVRany9FV9V6-iF
p4tSngiNPqB6cRkGMG2IRBwAEzFdDA3iVbL9lptUpm4kEEfVNos-fXp2Mlfaf4NHkusFIijekocybe4l4T9axe_yV
XPP53VB5SkR2OWFHacCX03xjGT-F_zw871olFD1KxjoIeuXeLDJjovRVmWbKNX-666fYprXhHRNl2HQdnTs-xT7AE
kLHKJ9Vn0chUv9Ff0H_xrSWfEU8SoLgPNDMvhx2_rj-9OjaYW-0sfDsHZFYEWv1h3CEenyXwkJRoLwK_oejcsg1nR
rzjtC5rvg8TWBbm3mHu1zI8a6FH6yuZZ_OaXHjK3eWrgagpe-ZJQqNoW8Ater31L4g0roeO24WvS6m8HJoWje1izJ
6unXKaosIJda1snyaNRIRQl9r-9-nYsEp1CmhTMilgRrpnCOyWjDsZjaqpNINntNxrWblmWf73IJ5E9L6S373E2BU
0Cjro-ZibMzF8Ao7dbLimfoBgt5im6B8hFbP9fDcjMgOqOhu38bW5MYnCUIsnxYqOiroTly297SFLiR7WQdsAFoB8
JKdPn3YV22eeFXOk0viFT0KqTkjWw4jaCS3l3DTJysLDtlzJklCbOPEaJnXLlWvaF_rmjB-fkY6co4QFueDpD-QlJ
jp9eVk3cB-Phpw1-hiOSNIrqRccQqMJ6GozwTEKAHIg2QaKmVfsZmp8TKkZP2FlZ-cVWGT1NVytlP30hc1L0kreRP
HrbsPsYU-Gbw7nhw_5K4RjV21D-8whe7kbmW7E8TTAV5BXkjp4XQrB7YlcS2IZihLpQ_MaWhl13Gi7B-z_CSrZ1H4
YMY-1kmdzTQGZgZL4YH3PEQehSMb8HuOhX-flOSLDGHIbDChOKSTZbWkBfjZ4Q_s16jwDHMIcsMQKFOgIpTjyf3wb
Em1HVv8VpgYPwYvaYwtsJ8iLF6TV9213jZjYWMsLzRNf8cjTE0YKhiTNtz4mvmxjcDr_sdkbKRYN9M2cz0Mhyu-VZ
zWxKUsMadGlz4NZOCw4i0ha38JRRVAljunkDGSl99Gh8412s2Ve76FOOuRNiffu8vJMIrg--DTM2g0lryZlzxhIf9
trHNR1wWe1v0VATQVRs5vIBdKIJEAF-A0e1o5ZqgZ-ywEHcKqzcIjFl3wT1mk03fHGD0qTMbNnwOgJmH5MRhuD1c1
Y4tqakPI_S3ooKNYRKnGQY3SHx6Hjxeryf5uxbTiY-VGRipm2CQHg5j26ftNgaJYevLDsu233csDpXgELudozv4LU
Y-jilfJ7iTiYlpGYuSA17IQuRTeHWNl3H-bzHKFROhbRAIc_NGbxiVMukjdNQqADCe7OvjCx2yZr07gah1Bt8N0gI
Ljm83jX1sIBivT8H_NrzkxzjV7nYgPKjKK6bNuw8n1jClqOYSsqSTdbCqhGIaiuhiWXwjnQS-ZhD93Ct3m5r6wYo1
T4rwUd5QDwJPo1aGcCI3g2JXd4Jq5O_HRxICd-NaDXw_D2R4GlCj4RECcXIv54SfudYcli0phFOihi7U4mkNz6AHo
3sidOfX1iq5mtGVfmGfdguAPOAL3FHlJhGPESmDfnqt2sJ7UHJw2cHP5xGcY4ue6sKlDx2MtruC8r6XRf1TlHEIk-
BiLsBkl9GMsV9Kf9QT4ig3CBUr_v2MIxFK-iKKcK9rug9FSJMWgUEpGCuq3JuaUDHEH_AY54zYOt0Gra4rQw2r5Db
MGQnGF2g9y4d58pt8LFB-qnmNrwb9RarT605Ia1s847UwZ9Cgk3evjvXQHi6-EfBILdnqnZHKj42oEIKueA-qQjhb
OrWGRlPczbh-onal4QroTqo-rhftPQBAbyqB_RSyOwYAQ3gQs5ada8Eg7APmUEemlbI_HLFGEMEynzbVy-oMYZFVh
LCVlp_X-SefrmyeXkdoHVCPrK2OqVn6dKi1-vZIw-bxz7qAnL6xEQsxcl-A5bXhQMzBUmG5A0OggFpwloYUNcPbXP
GKWpIRaRjmdlRUahKC5iglBSkbdxoY-KE8LnzLYcZav8jG0WF6fnYFfAde5ADXA8dFVPiT7KVAp8G_C39XFs4ulyD
P9NUrYuscfMLUq1Auxh2MeG-21GV4pfGWpZxO7KxjtSd9nYkPlae2gb5WZJPNuyZJXn8pWd8wl2ykcFg8dATKLuad
gaNuwwoedcYC8Mn8L-lTpS95_Jp1eCqzJkhNfFX6w8g7yKVH_Ao33Ks1kxQA1SloMnuV02fxIXlm4UD-RP0cr0pX8
AvUWeXNATYfQJXKqEuTIVU5SkaTt87wXmtKSHdwXqnGRi6XTgVhHKWSWrzTXeMQJIbEIqnxtZqvW0s07Y8m0eKAkm
jadKDjLEY_UcYpxwBziN7vvM-2_unQPibkM3E-JAwTjWsiCIWCGhdmfozLB3TVD07fGTranFdhF2OJ2uZUjWQjnoM
n63-xVYzkidR73If5ifTfMBtDX-OOzsdhsk6jm9yeUn5pC_MIrpRsCMgWSvmdmmNSJuHDDv4a21zfk7UBU_fCWZ9_
ZVnadWD_PNY5Xadtan2yJXBER0OFqX1xroAJzRlBEHatkNk5C5ETSxgYCZl6Tz96usShCwyHz1m2bXEDxLA4Q_ey1
YjjLhqtZNPY8kuRPi1s7pwKrpu-Jnjmlbmv KJ8kA1ggwJfo_N5VchOYQAzx-7HDfYqO63cXrXv0yEmcqpOECzIFCv
2UJP2RWHt2Em5paJKhoFj_kUeuq_hteAekgOipm59zOe8y8cxuoneHciItK2aUxbWrSasTY7DtowWajw40BL7tz_T
D5psVnYkghyPqnONcdCmB9FWzGBkIFxZ-Mqwx2bH9ICZU7n4UTavoEhuMHv6rKuUdswMPBG11jPxr2TbW4-UgoM2L
Ibj4prjYW2N5uWN9TkO65pUZtvOysfeS-EEglwy3f1qu_nBXac0ATeAaOyxYf_CzHCmvZDgjV1EGalkyBZmymqDhm
zZ0Ia1o5dj9IfY7qsBR37QU9Miu0lxaA-pMBN3j401eMdm5sVkQb-Q9ZHmtqy-SLLznO8X0oD8oOodmDHeA3BTtl6
8budNuVBXlEP8SFkWgjY0ZHLORTXw97uV-Okez8LC4efewOu7dB-7F1lxoC-slPpatwqW2KOoeas145pdjt9Etv-3
LDpRh0KjBVgXbmRJoGG1BBjyqPmTuXL5UWwGo9CDQfRNJvES-pXVZ7shnBanFOrrBuNJAfWTo894I95HUjAXv2XxQ
KEJLrRoEB5YrY8F7p2Ag0maNtm1th1X6XzbadGKhnxCt5wVm8okt35vCUcugcSG7sFi1xszYFiCXGCwkDXg1AQsqY
k0KMPoKIOHFXgFQoGINTNVfzhRYXQNwxgGyePdZRXAOJtNGNW5_m-ofjMHoPZ0AzOALwms6FR6dtLkXtcZpIfCzzT
iF8S-Z7fQcU-l33P0SLcdEmHVrrKyrPW7rxS-6dF7oT-7Mb0zr83Reb6vUTgEH3y5NDX5YUA6NXkS_CncYx9aOhE7
dIkJwxLutmqBRld1e5HsCpXyOpv4MuQKqu8qykDj_dOzhrusOwGKom1TZ3sJqjNZ2VGLB2urPKsS3739HtBFmx25K
eWtkojz7o8p-dMokHA8x1Ae__dzPUs-HPNyKrCWLV553iDzPYPAoAOYUnbKywmo3qFiMUnHTt0RewAcpCprThCniv
_bfGLKhCWuSpp06V53f8jZHyvgZ_BfLNGvo_ziUSIlwxVYFztWXPKFTzTie1WldbijIvVkqvawaMny5Ch85lJiUFX
KCO8GhOXdZMMGgdW4PTI5-le849MVjmuBXpzrVdDH1XrD7Dxx_5NUB3rSgB0qYZ9pw-HlcQKnVWRHAPe4TU1ANq9K
I1kOlpIrsvhlkJ1x9mXFAZ0V8_OXmuyZWXcZslNCn8iOPcCPJEfto8-Im9Q8puBr8jh-PKIRuSJcDLMrlHzCmU1N1
6kYHp6zkxEItIImE5ydg7EsnRixmtqc7D9rdj3sEj9QnT4ekb1BPay-sHPMZcHp4AbCQY0pc16Gker3l984I3nSko
tZ_V27dE9pk9Aukbar_kr1krY3JAOv9p4sPh_-rQ6A6ONByLRIwqIGBVhiQ5Y2j5RUcaa6iUK2Sp_hZbgulCSqcXD
1AgtdRfhOc93heMCxh4PDRXw_AZT6Rgca-76WldzMgbHOkeLTEbTsI9LGQ5OhphUJgv7Ot1yhBUECZZtJ4OIltXQt
4QAP814VrBYS5t_ey-_QYhcuOsgc4jtFY5xJCjj9uwlGcJNSmOhpxmxifxD3-ALZ8fIgRZIn5I8aH9YWoMzx45cP9
-rnVHHM1h8KAJ0dmCCsOw_iS9_vssl4cvtBnmE2ekEWmAtaiYfoVb5BnHBN2smyzq1ognbdfUNOlnkHZGHLMDDtMg
yaRSQYoZopx2Pat7zY1P2mXrV3sI2EM8QURDkUSYN0HLAnNULcaKcqxkS6Hr_USWS4bTEDemXEXIE0opoIjl_k9ua
qk3mO2wcVOoFhX6EQD3sag4b6V3-ZPUxIAhlMpGN-1-5SNA5GxfU-_epDKa3eZKBDG0m3NkWPLPg8L0rLwu3o1dRe
JLQMjOBpWKkOFxQh-vVDLQSFxl66-AI0mhiqB3ZU88bqOeZbOCXpGjF5Tyc6lxEqVVnVJdDbAQYZMTU5VXKXmMDB1
e0eJShqePkXHkpzeHyEniFihsvN6xYlKzhBRYDT1ScpWFtdeH6FkpSgutf5AAAAAAAAAAAAAAAAUIFhwkKjNB_t3nor
ZhrM89RwpYQoTwibJgoDM_clR4PyeFlowh_HG37-AjU_TL-51SP3SI62Zmybm_X--2xFFJE5dmHx5vN5mNh9j-MIJ
wOqub2nnGyl5C_8e48vUAlv67hR5ZlskU",
  "raw_randomizer": "68ea12f8d96d4eebf1fb5251a48630216067ec02e2f2bc313344df36d381834e",
  "raw_to_be_signed": "436f6d706f73697465416c676f726974686d5369676e617475726573323035060b6086480186fa6b5009010c0068ea12f8d96d4eebf1fb5251a48630216067ec02e2f2bc313344df36d381834e231d75946b497b4e357fc0600956557acbceeae744710d8cb45dcded1d3921e9c8aeb971d04b1bee0f0ca5d5fe187b104858fb73220220bd6462d787c03b2017",
```

"raw_composite_signature": "68ea12f8d96d4eebf1fb5251a48630216067ec02e2f2bc313344df36d38
1834e2ed1cd4470da5bfb804fa0f610199ee306d0ee70aa15028a22465d18818bdaa91b1c202d4ac0c93ebfe4
f4644bd0f5c21ae06dbd48b319659cbc6929485be1838564b12e6e512d326fca0910d981005a094816f959f52
d62df7e9928e94cbff016f4736bf3c1db169d931181b56f37f04d56785790183720738ac0f7a7c0c79030a577
98f0ce9bf46382b24011f811f7dc526bccc09728c15bcd6b1d22e59ae89e91873d8a45492acb18b4d93e214eb
b9323f97f73556a9bc62ff655131d102ec8b43360c9ee5f2a02af150e3859efdabca303d97d3d596b939d5702
46a344d62e4e37e186c30e08aacbe06d2cb6acef6d6dfcec52747fd2a3cfaa486ab5363b2ece75fdbc613e70b
ef144cb5717d1c0d38fd55192270428033215d22e29855f9418fc159c48a108a48382c9c0e662f31e69dd1c9c
bd8960c4fc3ca072f84cc6e2f65a8df51922c2ee58cd569f33ca5481a8b542a0fb983c9cee6f2a5e3455f2196
b29b4d769043cbf6f9d6b059bc0a41f942f732783c289b177048f49190084f1179a5fa1de493df24ba2d853da
4176877bfe2d9cefb077180a080b66efea100b598fbaeb9a48e35c05e63c32ed962e695d4b37e3f19c5b1dc2b
7a4989ef5a4768b6700a88722b24ac0bf4c8c44afba63afe8e527837bf1473ab9e0020ac1cdd3bd073cebc72c
00e3bb3ae8ca817fe4e2eb0f5480596255321572932 4f175ad42edf16001812f58fd65fea1ae27be08166320
bde770f1cfcf7d3c1755b99c222cb9572da336a4287d37822d1b68fa0ed3395a90ae64500586410f11a7842c3
741efbc216dce35d82af3d64fb63cbd5b96e954a7d4a2caa68e09b549ea4144464ea9b58dcf19377eed150a2a
4a07c3a4a0be7c2855519bc459894a4ecded6152c59f01a3e927d0c06c96884dc0e95b060c4fceb88ace63446
b689b422238c6319d7f1b905222f5262d3d7fec81d8a145b5a457ba043ace40fb59c8235977d1ac0ee59f276c
ce2d8ad9968d4018ca09e1e4776817ffe8dd98d2e7a63dd5f2bf12b13651646311c54071f5fc9a91dc52c33fe
6dd9e7918ff228b7ab779d46f1116157d58f79ca73ffe1fc2b111fca582893171228848aed37d44a05734373d
8109f14368bc50e8bfcc0f3052c215aa601afb14c5fff3897a7b23e41ec41a6ac0503fe1332e0c054fdf389ac
7297ecd00be32fb6c4246f49d03c545c1d6ee80a91c0c691b87fad9dd80b656a050ace8f8d9c3c2d3c0102f20
bdfce1b9621015d9d66822bb4f442285491394dff2c02ac626578ff4020001c80e462a3d58f8d2662a01f0e8d
353e8c525cab9d67604556f9a3528e78592d54cf0c60ec6676e058ebdbf3aae336c8838bd3c3fa4d9a9cb96f0
92d846b92fe8b53e1dd3e8dabef639687f91266f0e1dbc5eea19183e8ce6120aad018429f8a870a126f7e0dfd
5154fe6188efa7401b6e877e945693a20ed7df831de49929a74d850b4fbf5391ea71c903fae730f5866395b94
da01f9b1ac19a97f68b14c294b92dba4be55545a9f2f4557d57afa2169e2d4a782234fa81e9c46418c1b62110
70004cc57430378956cbf65a6d5299b890411f54da2cf9f5e9d8c95f69fe0d1e4bac1488a37a4a1cc9b7b8978
4fd6b17bfc955cf3f9dd50794a447639614769c097d37c63193f85ff3c3cef5a25143d4ac63a087ae5de2c326
3a2f4559966ca357fbaeba7d8a6b5e11d1365d8741d9d3b3ec53ec01242c7289f559f472152ff457f41ffc6b4
967c453c4a82e03cd0ccbe1c76feb8fef4e8da616fb4b1f0ec1d9158116bf58770847a7c97c24251a0bc0afe8
7a372c8359d1af38ed0b9aef83c4d605b9b7987bb5cc8f1ae851facae659fce6971e32b7796ae06a0a5ef9925
0a8da16f00b5eaf7d4be20d2ba1e3b6e16bd2ea6f072685a37b58b327aba75ca6a8b0825d6b5b27c9a3512114
25f6bfbdfa762c129d429a14cc8a5811ae99c23b25a30ec6636aaa4d20d9ed371ad66e59967fbdc827913d2fa
4b7ef7136054d028eba3e6626cccc5f00a3b75b2e299fa0182de629ba07c8456cff5f0dc8cc80ea8e86edfc6d
6e4c62709422c9f162a3a2ae84e5cb6f7b4852e247b59076c005a01f0929d3e7dd8576d9e7855ce934be2153d
0aa939235b0e236824b79770d3272b0b0ed9732649426ce3c46899d72e55af685feb9a307e7e463a728e1016e
783a43f909498e9f5e564ddc07e3e1a70d7e862392348aea45c710a8c27a1a8cf04c42801c883641a2a655fb1
99a9f132a464fd85959f9c556193d4d572b653f7d217352f492b7913c7adbb0fb1853e19bc3b9e1c3fe4ae118
d5db50fef3085eee46e65bb13c4d3015e415e48e9e1742b07b625712d8866284ba50fcc696865d771a2ec1fb3
fc24ab6751f860c63ed6499dcd340666064be181f73c441e85231bf07b8e857f9f94e48b0c61c86c30a138a49
365b5a405f8d9e10fecd7a8f00c730872c3102853a02294e3c9fdf06c49b51d5bfc5698183f062f698c2db09f
222c5e9357ddb5de366361632c2f344d7fc7234c4d182a189336dcf89af9b18dc0ebfec7646ca45837d336733
d0c872bbe559cd6c4a52c31a746973e0d64e0b0e22d216b7f09451540963ba790319297df4687ce35dacd957b
be8538eb913627dfbbcbc9308ae0fbe0d333683496bc99973c6121ff6dac7351d7059ed6fd1501341546ce6f2
0174a20910017e0347b5a3966a819fb2c041dc2aacdc223165df04f59a4d377c7183d2a4cc6cd9f03a02661f9
31186e0f5735638b6a6a43c8fd2de8a0a35844a9c6418dd21f1e878f17abc9fe6ec5b4e263e546462a66d8240
78398f6e9fb4d81a2587af2c3b2edb7ddcb03a578042ee768cefe0b518fa38a57c9ee24e2625a4662e480d7b2
10b914de1d6365dc7f9bcc728544e85b44021cfcd19bc6254cba48dd350a800c27bb3af8c2c76c99af4ee06a1
d41b7c3748082e39bcde35f5b08062bd3f07fcdaf3931ce357b9d880f2a328ae9b36ec3c9f58c296a3984aca9
24dd6c2aa11886a2ba18965f08e7412f99843f770adde6e6beb0628d53e2bc14779403c093e8d5a19c088de0d
895dde09ab93bf1d1c4809df8d6835f0fc3d91e069428f844409c5c8bf9e127ee7587258b4a6114e8a18bb538
9a4373e801e8dec89d39f5f58aae66b4655f9867dd82e00f3802f71479498463c44a60df9eab76b09ed41c9c3
67073f9c46718e2e7bab0a943c7632daee0bcafa5d17f54e51c4224f8188bb01925f4632c57d29ff504f88a0d
c2054affbf6308c452be88a29c2bdaee83d15224c5a0504a460aeab726e6940c7107fc0639e3360eb741ab6b8
ad0c36af90db306427185da0f72e1de7ca6df0b141faa9e636bc1bf516ab4fad3921ad6cf38ed4c19f42824dd
ebe3bd74078baf847c120b767aa76472a3e36a0420ab9e03ea908e16cead619194f7336e1fa89da97842ba13a
a8fab85fb4f40101bcaa07f452c8ec18010de042ce5a75af0483b00f99411e9a56c8fc72c5184304ca7cdb572
fa83186455612c2565a7f5fe49e7eb9b279791da075423eb2b63aa567e9d2a2d7ebd9230f9bc73eea0272fac4
442cc5c97e0396d7850333054986e40d0e820169c25a1850d70f6d73c6296a4845a46399d95151a84a0b98a09
414a46ddc6863e284f0b9f32d87196aff231b4585e9f9d815f01d7b90035c0f1d1553e24fb295029f06fc2dfd
5c5b38ba5c833fd354ad8bac71f30b52ad40bb187631e1bedb5195e297c65a96713bb2b18ed49df676243e569
eda06f959924f36ec992579fca5677cc25db291c160f1d01328bb9a76068dbb0c2879d7180bc327f0bfa54e94
bde7f269d5e0aacc992135f157eb0f20ef22951ff028df72acd64c500354a5a0c9ee574d9fc485e59b8503f91
3f472bd295fc02f5167973404d87d02572aa12e4c8554e5291a4edf3bc179ad2921ddc17aa71918ba5d381584
7296496af34d778c40921b108aa7c6d66abd6d2cd3b63c9b478a0249a369d2838cb118fd4718a71c01ce237bb
ef33edbfba740f89b90cdc4f890304e35ac88221608685d99fa332c1dd3543d3b7c64eb6a715d845d8e276b99

5235908e7a0c9fadfec55633922751ef721fe627d37cc06d0d7f8e3b3b1d86c93a8e6f727949f9a42fcc22ba5
1b02320592be676698d489b870c3bf86b6d737e4ed4054fdf09667dfd956769d583fcf358e5769db5a9f6c895
c1111d0e16a5f5c6ba002734650441dab64364e42e444d2c60602665e93cfdeaeb12842c321f3d66d9b5c40f1
2c0e10fdecb56238cb86ab5934f63c92e44f8b5b3ba702aba6ef899e39a56e6bca27c900d6083025fa3f37955
c84e610033c7eec70df62a3baddc5eb5efd3212672aa4e102cc8142bf65093f64561edd849b9a5a24a868163f
e451ebaafe1b5e01e9203a2a66e7dcce7bccbc731ba89de1dc888b4ad9a5316d6ad26ac4d8ec3b68c166a3c38
d012fbb73fd30f9a6c567624821c8faa738d71d0a607d156cc6064205c59f8cab0c766c7f4809953b9f85136a
fa0486e307bfaacab9476cc0c3c11b5d633f1af64db5b8f948283362c86e3e29ae3616d8de6e58df5390eeb9a
5466dbcecac7de4be104825c32ddfd6abbf9c15da73401378068ecb161ffc2cc70a6bd90e08d5d4419a964c81
666ca6a83866cd9d086b5a39763f487d8eeab01477ed053d322bb4971680fa93013778f8d3578c766e6c56441
bf90f591e6b6acbe48b2f39cef17d280fca0ea1d9831de037053b65ebc6ee74db950579443fc4859168236346
472ce4535f0f7bb95f8e91ecfc2c2e1e7dec0ebbb741fbb175971a02fac94fa5ab70a96d8a3a879ab35e39a5d
8edf44b6ffb72c3a518742a30558176e6449a061b50418f2a8f993b972f9516c06a3d08341f44d26f112fa95d
567bb219c16a714eaeb06e34901f593a3cf7823de47523017bf65f140a1092eb468101e58ad8f05ee9d808349
9a36d9b5b61d57e97cdb69d18a867c42b79c159bca24b77e6f09472e81c486eec162d71b336058825c60b0903
5e0d4042ca9893428c3e828838715780542818835335 57f385161740dc31806c9e3dd6515c0389b4d18d5b9fe
6fa87e3307a0f6740333802f09ace8547a76d2e45ed719a487c2cf34e217c4be67b7d0714fa5df73f448b71d1
261d5aeb2b2acf5bbaf14bee9d17ba13fbb31bd33afcdd179beaf5138041f7cb93435f961403a357912fc29dc
631f5a3a113b748909c312eeb66a814657757b91ec0a95f23a9bf832e40aaaef2aca40e3fdd3b386bbac3b018
aa26d53677b09aa3359d9518b076bab3cab12dfbdfd1ed0459b1db929e5ad9288f3ee8f29f9d32890703cc750
1efff7733d4b3e1cf3722ab0962d5e79de20f33d83c0a003985276cacb09a8dea1623149c74edd117b001ca42
a6b4e10a78affdb7c62ca8425ae4a9a74e95e777fc8d91f2be067f05f2cd1afa3fce2512225c31558173b565c
f2854f34e27b55a575b8a322f564aaf6b068c9f2e4287ce652625055ca08ef0684e5dd64c30681d5b83d3239f
a57bce3d3158e6b815e9ceb55d0c7d57ac3ec3c71ff9354077ad2801d2a619f69c3e1e57102a755644700f7b8
4d4d4036af4a23590e96922bb2f865909d71f665c5019d15f3f3979aec99597719b253429fc88e3dc08f2447e
da3cf889bd43ca6e06bf2387e3ca211b9225c0cb32b947cc2994d4dd7a9181e9eb3931108b48226139c9d83b1
2c9d18b19ada9cec3f6b763dec123f509d3e1e91bd413dacbeb073cc65c1e9e006c2418d29735e8691eaf797d
f382379d2928b59fd5dbb744f6993d02e91b6abfe4af592b6372403aff69e2c3e1ffead0e80e8e341c8b448c2
a2060558624396368f945471a6ba8942b64a9fe165b82e9424aa7170f5020b5d45f84e73dde178c0b18783c34
57c3f0194fa46071afbbe9695dccc81b1ce91e2d311b4ec23d2c64393a1a6150982feceb75ca1054102659b49
e0e225b5742de1000ff35e15ac1612e6dfdecbefd062172e3ac81ce23b45639c490a38fdbb094670935298e86
9c66c627f10f7f802d9f1f220459227e48f1a1fd616a0ccf1e3970ff7eae75471ccd61f0a009d1d9820ac3b0f
e24bdfefb2c97872fb419e61367a4116980b5a8987e855be419c704ddac9b2cead688276dd7d434e967907646
1cb3030ed320c9a452418a19a29c763dab7bcd8d4fda65eb577b08d8433c4144439144983741cb0273542dc68
a72ac644ba1ebfd44964b86d31037a65c45c8134a29a088e5fe4f6e6aa93798edb07153a81615fa1100f7b1a8
386fa577f993d4c4802194ca4637ed7ee52340e46c5f53efdea4329adde64a0431b49b736458f2cf83c2f4acb
c2ede8d5d45e24b40c8ce06958a90e171421faf5432d0485c65ebaf802349a18aa077654f3c6ea39e65b3825e
91a31794f273a97112a5559d525d0db010619313539557297 98c0c1d5ed1e25286a78f9171e4a73787c849e21
6286cbcdeb16252b38414580d3d52729585b5d787e859294a0bad7f900000000000000000000000508161c242a3
341fedde7a2b661accf3d470a584284f089b260a0333f7254783f2785968c21fc71b7efe02353f4cbfb9d523f
7488eb6666c9b9bf5fefb6c451491397661f1e6f37998d87d8fe3082703aab9bda79c6ca5e42ffc7b8f2f5009
6febb851e5996c914",
  "raw_composite_public_key": "e45ffc8cc73db885dc662e62a18cd8e3803297117fa5658814a985b5ff
1db7b468cfc82bb929f1d86b77ed14f5ae16a65368772ce51912410105e0456975ae91fdb643b512f124d5e60
bd68b8c7e31fe01c7b0dc65ae470501cc565a6e1dfcfcfd12565433c4afedd511821e2e9610c45275e2836dee
35ced69d7efa672fd1e4318bef5eb6e897e8b451aa202ded042b2aaef77a7be3f699146da229a8bdb3ffa4964
45967e75217bfbc9048f9956443d8731f833eb30de10dac96fffe7cf65ea0445c3e31e8601e133be6a100764f
e3196e267726441f31751fbf9a6f5880644f4e7275e57de2b0f105e4db055d50dd1c9c934fddf535b8de28b0c
74c0449f222cd2ed0bb8fbc775ccee8c940665b40f712f4f7e00750e9e1e4cd9cff25d1945c3e9bca53ccd4f1
2eee7581856ebd68f26845956e3e7beb761f0fe75bdd31bfe2fa018113397b387bd59d62a68b8af7fa245ab93
2e69f778e2ceefd21304fbb8099ea13d8ea57c1813197a2f75ae251075b51dad38f853669e9d5f98a36550989
41993a1594860fba71fe530ee5c29f58f2978af688ccb75a5838a359c112e98e25a8583ac8dac1f861fd58e2a
fba5de5a52e020904f5b42bc0874e35befcf3e6119684768f36e008f04712177cebe627607381e56eaaee161c
1729b8de51dbde474d48cc68249ea27162b87993e60c84ed6cc6423cb3676d9eb50b2cab5a3a049ef131381d6
23fa6fbcbc9db1e7cc025ea0418b9dad2cc6ccd4e95fa2cec24feeca70318a751716b7213f63edbf65a633383
57f838f94ec071822c24851248885107b3d1c4e924678c7614ea1af038104619f2ae372940becfa69e29cbb5f
f6c3e20a47be4a4f74bac34c133c00a6a706accc6ffd3d8e4fbd69a99704e1283c850d8c58d1e5753cd9587b8
3c4c346cb9a58137213ec10834c66adfe2bb5c501a8ef2ecadd1b677a3df1a6deb86ebf0722c4f5030e20f901
8dd5b6fc53eea24fd92b7b5b4025feae996d3e48fd4c650d82dbad7eaf936639698512f26253d2ef6847c8518
e8565cc9a5495c6fff57cde7323882c54a7db470ab2daf8ffd2bf794fa7c692d9e7fbd532eecc1d7880e2ca0b
3216128be28b4a9f1d151fac97808b0bd98b7b43a612a9ac865812bfeac6f47460277840b52a3b087f916ca7c
edc0f768ea2bd19ea21155f84b4a04c4000ad2ae0587154d560bc0a477a4f9329a8984dd31eb1f2a05e3d9187
01d630cfca9af61ef088d2c5581acb463e439902e5d425719e956b8d6df7305b28e0ff27d3ad0de2085d29249
9b19a3390d4396fb3bac9a8d8cbead2a7a4290fc9ac6fca045f98a614a45a39cbe24360f84d14f8e472712ace
b74dbf45b53d49a0e4737e476ffc4d5b2f7cd247aa186d3b764ad9e9cfeee456a73c291d8de3912414ac43911
c372173ad7b472af35c6853ced2fe7b5fe0a89565ab33baa6f65cdd928319d7065e040e7a5e84f9aa903f7648

094bad07136b16927b8ec6dbc2bef0cc2856de1e795923e1412c49f24deeb6c21f6c8a9765c9c7986e0da4b4c
67d8e0d0c8d466824fb923d8573148990cd2ef133c78ceecab72ed9dd285c5a3766852d54534207ffd34027f6
c76ede8fd1a32d72c30048bbaa797d5df6fde27d087de5721ad7b7fa3e8d3f70d6bfc3ab2e252335368bbfa15
acb5cb37d4694e8b23cebe25de9c925a221a183b904d3f85df9929a919c54d6f87457373a0d6ecc1403e4cbbe
620999435e80696634cd1a8e4747e9825bfa336e5bbad14f73640f1b9febe800dbaefe1630c61fae635b074c5
64eaa9db189c9e7302873fc64e6d497bc5c29080987a07a21d4af210703a4fa07f2fd816f12fd1e29b4c0f44a
fe9bd4a1eaa8a7ae6f02a5b4258f52caf6127f62632a67cf4e8310be56a7c28c86b2e277600c3e92c8d23d425
86244c571e90568df202f2f6d81f860a565f9eb91a3c78372e2a8b1be61c5418cf49bf2d6c8955d4a482a9919
b7660b3f9a4404ffc454ea073e1e4b2689ab2cca4e46bd7004a6c491fa26ee7a57d60f35edb2b821e6266442c
8f335d452d524c772e0353724c23c7dd15b7aa155e91442022140c5fcb0153147edcf3e8952f6f0399a3c8806
6a72756c9409915de63f64fa797841c57c796c6fc550ef745dfe9f179457f94755ae5a2506a764f327e550be3
dc14dd41f3b04b147d454938c63a8d69b2ea4c5710ec0b36e3a6c72571fa5d59dde036c42033df35af056966f
f0cd1204008971aa6ba9fb97b685ab9ffa2a9d1778104cd2c3b326de1fcbc242e94d0311c3275b12850ed30ce
ead3a2ee6d060508411d4396f5421d8b6d067cf7cb5e826785fbe119e05e21bd879b64f57cb0cd1972c2815f2
0abe7ce6ab34d0f471af44baad179e90644122f5f33288e689dddc5ce833e9755df1e73c65c5a201c4ede2ff
a6b19274927719d2d38fdb7a65aa43708b7fa9a94aa7d3210253d78d3b181e1020d0000bd0a1dc05d447f9f58
ebeb84c65b36c8afcb83727a1508994e826957a663b0b9b8a003325ab6d6d6462ee4e106019c0dffe10323b7b
de7d82a38f85fd08786e860ba66c161b64b0708c363de5c6af62d8db3c243d1e1b712cb1d59e942b9b6b4295a
5a500b182cbd5fd1bc6ce9376d91b47a2284f1fbe0ad1c048cc2cfbb4afa3a9eb9697503b69feca990eba7e94
41af9ca44cb3ac6b5ed66e591c201fe30efa8a7c471dc613d6254c263a8e132104bec47f1aacb3b2fcd4051b6
9b5e3fcb1c147a65c2f90c4b5188bafc521cab03c12a309da50b5a7517727ed41228ed123fe1b152f6a6319cd
623bf34ad7b8e064ab993260bcbd405f5b7fff9b2fa40ba5ed5630242539e5d96823e89dc818a13d16675ee30
79d976f694f5acc9760ae789e9b3391b289e0e22a7ef17cc6a4577157b6d95c09baa4fd532e3ee0a290810ed3
5e56bb19d9b61fb98a97c617425b06093d98a5cf0ee2dd127f0eea600b9a0c67fbe761db9b77e5d5bba9701da
1b883e521a0cfe88451f57bd36085b67e56f061f84a2e6a152a71bce6e522daab6a0a33ce22e537fa9793d28b
617e6c0a4176a83aa3be578afac0f2f5547c5516d218984755b7445c7143afa4e551fce0071bdb873b34e6b9e
2b9e79ed0c69d288ed6421f237e860a0c6492ebbdd2a44c2c4f368dbe99941b1e8561d859d3859f496cee3d74
1f252973f8fcc539c409e35cc80a5ed6df23cc3a65601313f5d681fd9540c5291a9e30a72e38c96413c47c61f
f84fde78d011b01b4154d1b920af003f7abb1e1999dea6a766cf9fd2702b3ce0ee57af931b62124b0861b163a
3b91aa4bea28076c3432df3b29b6c4e1ba588def420071fc157de90eb2722ecc9ab00df3c669383a61a91bb67
bd287ce349b4745ee7a479dbceef166b9acc412eb579fcd6437307edda253d606b7be7599c38092bc52a85984
80edab8b82b1d21c565d2137ceae0b6642619b16133d91205d6355029e9cdfeb9a28b373d95916b6b707d4c71
2c09cf36daf1a511b2bedb1aa70ee58d46a0666bb287784b0a3840c589a7a04d5d6f2216be90aa4a512d5632f
5c9bfe7b8b13382f999b95d367c7c46b968074ce315197a5ff3545c7b77a804ade56a95b5c24cdece5937b5c0
366d93ad03da9bc5db1b551dfb91e9b343d2b57b763439686d4a346a426b4e9d2be9c9ae77472cb63db43b719
5cee60fe903e8028b06f8c2356d3cb5d2f73b776bb9dfd5507d87d056a646a32b382b6bf31f2bf2db8e885e5b
fe0cf3d0d85da24034bc29b90dfe5f0de960b051931e6e8249700a07fdb5e1828ea"
}
```

Figure 3: ML-DSA-87-ES384

## A.2. COSE

Will be completed in later versions.

# Appendix B. Acknowledgments

We thank Orie Steele for his valuable comments on this document.

# Authors' Addresses

Lucas Prabel
Huawei
Email: lucas.prabel@huawei.com

Sun Shuzhou
Huawei
Email: sunshuzhou@huawei.com

John Gray
Entrust Limited
Email: john.gray@entrust.com
```