FIDO2-PQC: Proposed Implementation of Passwordless Authentication with Post Quantum Cryptography

Aditya Mitra (adityamitra5102@gmail.com)

Abstract:

FIPS-204 has standardized Module Lattice Based Digital Signature Standard (ML-DSA) which is believed to be secure, even against adversaries in possession of a large-scale quantum computer.

It is to be noted that with the recent wide adoption of phishing resistant passwordless authentication standard like Security Keys, Passkeys and device attestation following the FIDO2 specifications, the adopted cryptographic standards for authentications have been primarily ES256 (Elliptic Curve Digital Signature Algorithm with SHA-256 on P-256 curve) and RS256 (RSA with SHA-256). Though most authenticators support other algorithms as well, the default algorithms are ES256 and RS256 when anything else is not mentioned explicitly. It is also be considered that neither of these algorithms can be deemed secure against adversaries with large-scale quantum computers.

This study proposes an implementation of ML-DSA for passwordless authentication with standard FIDO2 specifications like CTAP2 (Client to Authenticator Protocol v2) and WebAuthn (Web Authentication).

Introduction:

This proposed standard describes how to use ML-DSA keys and signatures as described in FIPS-204 for Passwordless Authentication with WebAuthn and CTAP2.

Algorithms:

This standard proposes the use of ML-DSA-44 and ML-DSA-65 in accordance with FIPS-204. It assumes the COSE values as represented in Table 1, which has been requested by IETF for IANA COSE assignment.

Table 1: COSE Values for algorithms

Name	Value
ML-DSA-44	-48
ML-DSA-65	-49

Secret keys:

FIPS-204 defines 2 expressions for private keys: a seed, and a private key that has been expanded from the seed. In this document, the authenticators are recommended to store the seed considering limited storage in HSMs, TPMs and SEs. The ML-DSA.KeyGen_internal(ξ) function as defined in FIPS-204 can be used to re-generate the signing key and verifying keys from this seed.

Key generation (Make credential):

Web Authentication defines the credential creation API. This takes a publicKey object which is of type PublicKeyCredentialCreationOptions

```
publicKey: {
        challenge: h'……',
        rp: {
                id: "example.com",
                name: "example"
        },
        user: {
                id: h'……',
                name: "johndoe",
                displayName: "John Doe"
        },
        pubKeyCredParams: [
                {type: "public-key", alg:-7},
                {type: "public-key", alg:-48},
                {type: "public-key", alg:-49}
        ]
}
```

The web browser or the client operating system is responsible for communicating with the Authenticator over a chosen mode of transport (as defined in the CTAP protocol) and send a CBOR encoded command to the Authenticator.
The CBOR Command for AuthenticatorMakeCredential function under the Authenticator API in CTAP is 0x01 and the payload is supposed to contain the publicKey data in CBOR encoded format.
The payload for the CBOR command can be represented as

```
{
```

1: h'…….' //clientDataHash

2: {'id': 'localhost', 'name': 'Demo server'}, //rp

3: {'id': h'……', 'name': 'a_user', 'displayName': 'A. User'}, //user

4: [{'alg': -48, 'type': 'public-key'}], //pubKeyCredParams

7: {'uv': True} //options

}

The same when encoded into CBOR string, can be represented as

A50158201637B26333915747DBDC6C630C0165405A64939AE8F6E4FC39414F853F702F1602A2626964696C6F63616C686F7374646E616D656B44656D6F2073657276657203A3626964504EC1D4219F294FB4A0BC0CD29D485AFC646E616D6566615F757365726B646973706C61794E616D6567412E20557365720481A263616C67382F64747970656A7075626C69632D6B657907A1627576F5

The authenticator should use ML-DSA-65 (-49), ML-DSA-44 (-48), ES256 (-7), RS256 (-257) in this order of preference if it is available in the Public Key Credential Parameters. Other behaviors of the authenticator to be used should be following the Web Authentication specifications.

When the authenticator receives the AuthenticatorMakeCredential request, it performs the steps as defined in the CTAP Specifications. It generates a keypair. The private key is to be stored in secure storage. Resident Key requirements should be followed according to the Web Authentication and CTAP specifications. The public key or verifying key will be COSE Encoded in the way defined in ML-DSA for JOSE and COSE Draft by IETF.

COSE Key for ML-DSA-44 would look like:

{

1: 7,

3: -48,

-1: h'.....'

}

It is then CBOR encoded. A CBOR encoded COSE Key for ML-DSA-44 looks like
A3010703382F205905200BE1BC2EE2929614D3046FA3FE8A4B486E06ED3785CDADB376C9DA86562838FBAC8D1B58389806367BEB1BC562A976A60ADE12D71E377EF4F9AC17CE1C2A5AF85F8F550269B5467A12BFCA1C361EA85DDD339760430ADB49A12A1702AB7F774536411FC4B1E9AA4D91E038B4290905D42522F5B7CC2B8B3015976852B39973874B2D3FD81918F053D413EFC4DC8852BB427AC16B1D9EFA8E0CB883B555CE94356882C0A0CEF3100CEFBF0127C08765B669E6A4CFDB297D667EB123629F136F7D34BCD017003CB4C0141BA21B6F77D

05C8FBDF749D592094B7DAD742902FF76BCFCB1C284C3970F82135227DA7798C764BA354
27DF01B43B26430E831390088E5993E273266BD168090F2B4F0582DDEE916C9036F7F5C54
5706D8C3B527E1729BB76BC6000543D22C9DF56C6F47B041770AA95C2E1BFB9B091F9C4E
B0BA419886F65E4888119551C1FFF3120BB430C3012AE3DF6C591D81D146C611DB70F3979
AE99F0E43939A611085D83783164F5D77982FEF8988F5118CF064A886931D0C2756821464
8E72CF1A5995B85A531B576F0EBE1096A460705F55C6F9A2D44BBFFA519ED0C4D9DE0BBB
6D09CAD230FACFA6BE88B4E929E9DC92A5BFCC349FBF4E182DF5508C98481CD293BD9296
45C5DC15FEBB46E66A05B123241BD3F5CD2FB17FB5008BC2BF8236D73323F1DA506AA578
9620912CF9853FA82C8B6CED2A5B2F565EF17B39F5679DF7D552A7AF5A2F8CD46B18FA685
5217AA6ADB5DBE8F45B73BAD10BEA4A26D948168795FCC2B74F3DEDCC8EE1BFEC73EB56
588917AAFEE09BF511C2C0BC32E901F33C0CC4DD0224FB4E4EBDA780AD11E9B184EC480A
B0377E8549078E393BA4AB9032F14081B3E6BB50B998D1F89641EC3F565BA8AD3BC5A3D9
635007FAC2879E2379820C9EE1E3DA760A555BA3B6A55138AD55F67FA9869BF26E50263D9
0AB58B4E1F61924BF6D3EF18759BBAC28281DA54B6F43BDFAFAB6811C0CB0F074B37254D
142615CA5D4021BB40075156EC2421B86ECC7A2BC2F1BDD078E893E35F44131277EE1CBF9
7F7EC4E00493ED23E32824F079A30F9808A87D8D79A5958654618E986B4983E7BF9E269A7
C48FB98C255A1CA4672C7F77E685118860EAF3423A00D7080B1053C30D7B804861004AFC5
3EEB98E63114AB5B9D77F22E3796A405D06B265DB7DC51C8C202655E1314A2174E3EECF1
5C0579DBC97BF8D2B1FC4B264E92A5A20C4AEF7291F983CB7605FE8A01F7413F5701E5166
EA863FC85BE9C1CFD880520A1B1E144AA9DCC3668275FF973F4F15634BB5D92F3EE407A6E
32CF717A925B9D4B9A9FA13D12DB088E6C53DDE00588885F1761938EB08C57F99CF85522
72B3554F557FA7BCEBC48144AB539A9E34063C3BD8DE9D59477B8574306FAA12834FEBBC
9BE00010A8138338B5061800AC7A682208EAC2713FDE393A9BBFE2996012EB4B8C064801E
7DFD0DDACE34D69BEA0E641BC7D8BD6C37BD12CF28BDF1394E149348BD0D90C66590697
2252836C3E9F90DD15A969E3678FC8A2E654BB1BDA9EE735FD6B2501A6C907ADF5137017
7A907C85C423F510CD1CBB4275154970FA6A7EDE91C9CEEAC63F3879D0FB8C92DB457D99
15C645539AA55216E215D861BD8A02703C63F8941EF966CE730525FB6B70A02709AE6296
A11CB74B937BEDBE20A7A28431F81FF0A0FF6166311C2F5764AE73B69EBB4944CE5498979
124393713CAC2247FC1DDFCB9ADB965CDA54E9618E2326771D46FAD88EEB6B534C4D4303
1CFFA876ED74882278342774495A5BD48A132154B48038A168BAA8A619A6D78D8960FE3A
89978FA4C0AE4498F93451F6C07189BCD5EAF8F04

To generate the attestation statement, the following is performed:

1. The RP ID is Hashed with SHA-256. This will be known as RP ID Hash
2. The credential (keypair) and credential ID is generated
3. AttestedCredemtilData is generated by aaguid+credentialIdLength+credentialId+credentialPublicKey (where credentialPublicKey is the COSE encoded public key.)
4. authData is generated as rpidhash+flags+signCount+attestedCredendialData (flags and sign count are defined in Web Authentication specifications)

5. authData and clientDataHash is concatenated and is signed with the private key. This is known as signature
6. Attestation statement is generated following the attestation statement format. An example for the same is {'alg': -48, 'sig': h'.....'}

The attestation object is generated as:

{
    1: 'packed', //Attestation Format
    2: h'.....', // Authenticator Data RP ID Hash (32 Bytes) + Flags (1 Byte) + Sign Count (4 Bytes) + attestedCredentialData => AAGUID (16 bytes) + credential ID Length (2 bytes) + credential ID + credential Public Key (COSE Encoded)
    3: {
        'alg': -48,
        'sig': h'.....' //Signature
    } //Attestation statement
}

The attestation object is returned in CBOR encoded format, completing the authenticatorMakeCredential request.

Authentication (Get Assertion)

Web Authentication defines the credential request API. This takes a publicKey object which is of type PublicKeyCredentialRequestOptions

publicKey: {
    allowCredentials: [{id: h'.....', type: 'public-key'}, ...]
    challenge: h'.....',
    rpId: "example.com",
}

The web browser or the client operating system is responsible for communicating with the Authenticator over a chosen mode of transport (as defined in the CTAP protocol) and send a CBOR encoded command to the Authenticator.
The CBOR Command for AuthenticatorGetAssertion function under the Authenticator API in CTAP is 0x02 and the payload is supposed to contain the publicKey data in CBOR encoded format.
The payload for the CBOR command can be represented as

{
    1: 'example.com', //rpId

```
        2: h'.....' //clientDataHash
}
```

When the authenticator receives the authenticatorGetAssertion command it performs the steps as defined in the CTAP Specifications. The private key(s) is/are fetched from the secure storage. The credential ID of this key(s) is/are denoted as credId. Resident Key requirements should be followed according to the Web Authentication and CTAP specifications.

The following step are followed to generate the assertion:

1. The RP ID is hashed with SHA-256. This is known as rpIdHash
2. authData is generated as rpidhash+flags+signCount (flags and sign count are defined in Web Authentication specifications)
3. authData and clientDataHash is concatenated and is signed with the private key. This is known as signature.
4. The credential descriptor is generated in the format {'id': b'…….', 'type': 'public-key'}, where the id is the credId
5. The user Entity associated with the key is retrieved from storage. It is of the format {'id': h'.....', 'name': 'a_user', 'displayName': 'A. User'},

The assertion object is generated as

```
{
        1: {
                'id': h'.....', //credId
                'type': 'public-key'
        }, //Credential descriptor
        2: h'.....', //authData
        3: h'.....', //signature
        4: {
                'id': h'.....', //User id
                'name': 'a_user',  //User name
                'displayName': 'A. User' //User display name
                }, //User entity descriptor
        5: 1 //numberOfCredentials
}
```

The numberOfCredentials field as shown here is optional and is generated according to the CTAP specifications for Resident keys.

The attestation object is returned in CBOR encoded format, completing the authenticatorGetAssertion request.

Experimental Setup and Performance Analysis

The Open Quantum Safe (OQS) implementation of ML-DSA algorithms have been used in a quad-core ARM Cortex-A76 processor-based microcontroller (Raspberry Pi 5 running Raspberry Pi OS Lite). The microcontroller has been configured to be able to communicate over USB HID and a custom implementation of CTAP-HID has been used. The custom security key is able to work with ES256, ML-DSA-44 and ML-DSA-65 algorithms. Further, it is to be noted that no changes were done to the Web Browser or the Client. The Client is running Windows 11 24H2. The RP Server is running Ubuntu 24.04 and the application is running on Flask.

A few credential creations and authentication have been attempted to benchmark the time taken for the process. Table 2 shows the time taken for the same.

Table 2: Average time taken for each function

Function	**Algorithm**	**Average time (µs or microseconds)**
authentication	ES-256	3192.7
authentication	ML-DSA-44	17800.6
authentication	ML-DSA-65	30675.2
registration	ES-256	12251.8
registration	ML-DSA-44	36069.2
registration	ML-DSA-65	68086.8

References:

- FIPS-204 https://doi.org/10.6028/NIST.FIPS.204
- WebAuthn https://www.w3.org/TR/webauthn-2/
- CTAP2 https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html
- OQS https://openquantumsafe.org/
- ML-DSA for JOSE and COSE draft by IETF https://www.ietf.org/archive/id/draft-ietf-cose-dilithium-05.html
- IANA COSE https://www.iana.org/assignments/cose/cose.xhtml
- Yubico/Python-FIDO2 https://github.com/Yubico/python-fido2
- RPi Security Key https://github.com/AdityaMitra5102/RPi-FIDO2-Security-Key
- RPi PQC Security Key https://github.com/AdityaMitra5102/RPi-FIDO2-PQC-Security-Key
- PQC FIDO2 RP Server https://github.com/AdityaMitra5102/python-fido2-PQC
- Demo video https://youtu.be/qAKDtAn4LVg

Appendix 1: Time taken for the operation multiple times

Table 3 shows the time taken for performing the operations multiple times.

function	algo	Time µs
registration	ES-256	37810
registration	ES-256	5601
registration	ES-256	5898
registration	ES-256	5871
registration	ES-256	6079
authentication	ES-256	3435
authentication	ES-256	3132
authentication	ES-256	3295
authentication	ES-256	3089
authentication	ES-256	3184
authentication	ES-256	3080
authentication	ES-256	3377
authentication	ES-256	3051
authentication	ES-256	3201
authentication	ES-256	3083
registration	ML-DSA-65	68796
registration	ML-DSA-65	67511
registration	ML-DSA-65	70420
registration	ML-DSA-65	64257
registration	ML-DSA-65	69450
authentication	ML-DSA-65	30142
authentication	ML-DSA-65	31431
authentication	ML-DSA-65	30696
authentication	ML-DSA-65	33001
authentication	ML-DSA-65	29139
authentication	ML-DSA-65	32220
authentication	ML-DSA-65	30723
authentication	ML-DSA-65	31537
authentication	ML-DSA-65	25272
authentication	ML-DSA-65	32591
registration	ML-DSA-44	36482
registration	ML-DSA-44	36288
registration	ML-DSA-44	36220
registration	ML-DSA-44	36003
registration	ML-DSA-44	35353
authentication	ML-DSA-44	16908
authentication	ML-DSA-44	18794

authentication	ML-DSA-44	17441
authentication	ML-DSA-44	18481
authentication	ML-DSA-44	17583
authentication	ML-DSA-44	18340
authentication	ML-DSA-44	17716
authentication	ML-DSA-44	18794
authentication	ML-DSA-44	16055
authentication	ML-DSA-44	17894

Appendix 2: Sample CBOR Inputs and outputs

It is to be noted that in the following CBOR examples, the first byte is NOT a part of the CBOR payload. In the input statements, the first byte is the CBOR command (0x01 for authenticatorCreateCredential and 0x02 for authenticatorGetAssertion). Similarly for the outputs, the first byte is 0x00 which signifies the execution was successful.

Credential Creation ES-256

Input:

01a5015820afedb91cf6971cecb8f26d2e066cb1333efa942420c254bc30235e5ce12eaa8a02a2626964696c6f63616c686f7374646e616d656b44656d6f2073657276657203a3626964505bf7dbad54524776be382d2376293742646e616d6566615f757365726b646973706c61794e616d6567412e20557365720481a263616c672664747970656a7075626c69632d6b657907a1627576f5

Output:

00a301667061636b656402589d49960de5880e8c687434170f6476605b8fe4aeb9a28632c7995cf3ba831d976345000000044d41190c7beb4a8018adf265a6352d0019f785d850be6b4bd7b241c30f69efd61f5f6372797074616e65a501020326200121582 0a58e44e07b296acfe3908846c7230b8887c790a19c0d75bb31d51b7a26dd1f225820225716514d192d4c5ba6496e2a66fb93e5afdf02118371099917423e88194a7103a263616c2663736967584630440220 45ecc72dc3103ec407e6a6e1cd40d9c11d69d12dd1df7ef2ef8a9e71d943de0902202bcf5b7c6f8c2620764d3a9f31e4711d55358e77187abd021a366a974fc41e

Credential Creation ML-DSA-44

Input:

01a5015820da8361bcb104b3e7cd4681cf80b6a96a2c788222b4b8218ef5311182c2ad7f0c02a2626964696c6f63616c686f7374646e616d656b44656d6f2073657276657203a36269645047787fd9fa0b4b6793cf7a75c388f919646e616d6566615f757365726b646973706c61794e616

d6567412e20557365720481a263616c67382f64747970656a7075626c69632d6b657907a1627576f5

Output:

00a301667061636b65640259057a49960de5880e8c687434170f6476605b8fe4aeb9a28632c7995cf3ba831d976345000000044d41190c7beb848018adf265a6352d001997e93509765f4a088d9f6a8d7f9314c55f6372797074616e65a3010703382f20590520bb2f031ef8a16176f0079737d9f5df04ea7b8954a899086212a8b859bb3cb1e38fa241a3a7dc90f25b2492031c1aea0f3ee3b91acdc167110dc68cc16d192a6d847f1149208bed109d9eb4b2d73343eb3ccb73f711c4cade91fc158e501cad07fe1d2730600e3615b2689b074662ac60b6964edaf20723cb2c43492415fc3931db0881e81fcedded9ba9140ac0ddb7e11ac748f003ff309fa0a4d845a3e56a9c786bd35e91b2c6ff62d6dfc50ec9719770d15c98578727cb99371e34f112615e2198d7820ca64bde86196ea352fe63a047e8d0b0a1a1810c368eab063f0e4115db8bf08b4abfb36cb87cc8577b7a44b0c65dc12fd17ce44ccc29b469ba45704cc4de8fa293f975ab1278850accbc70c7773d1e0995b876c3fc924b00b4357167544ffe712b66eebf6562d86a4585d43a8ba8c2e1564906d6a38fde232a658d5a7aea2f9871c40f1d5ebbdef5839478c029711bdd3c4e954c0c68c013361f5c29d373572c0e4cc770c4e996b7d39ac42eeb82cd28b056bfb337d60e89066a5e1d0faf04f274bb92465fc092e6efdb0026866cf9844f9bd7f3574204d9c90ceb3ad8f7b91d87179d2c8c096da05dd1d8a04760d7fafe56dc51a0c3d5b0b1b8c2deb5222a64da7f4fe5e1718d53b9901a24973bee90dc216d9065372b63eaa71ca611887752ccf9e2a2c0a2363d4145779caa61cbd0fcb963880396c25f15c109f9e246eb70e06b69605c488b92d312d70069037384d4e62c456ab4a54eae313e6efa3bd98f8a9914ad347c2dbe788ecfb3d73ab299ba593c563f9603d06719478ad1c6204ba88939378440a9dfef93bee6943626ca029c5143e66274f22ee9e251bb26b76193bfb604666043af8c709943563cc2558b75eccf5ce5d19e0a2b1a17713057bac1a3d39246d625ac74647180df31077537e0b5e40d1a4a270be6b7957da27562ea5d4918d3d86a717394d1c81ab5d34185e9ae22798046076763961896e842febc7fa718deffeee0e134d12a19ac5370fd09f4e5337e1175ee7528ce4ba6d97a030d02b25fbddde35df2e2af84fe6a9712b30c942c5818829e49085f5c2747b192a698f05d35eb21835eb6a6dc47cf2228423ec5051da5bf411f42327f3b09632ae19a062d394b7f73bc428068dc73195da660da1ed09a78fb10650142c127f6d24196d1ce6bcb7fe40a916557a48005ade487419e5d42c2f6bd7903cf7bdd6ee6b01a7f92da64b6328e65eb18d111e1a8c3ba1141c9ab8a181f7fd56561cc550e760ce682bc3ab97530194d5dfd9c990abc8671bd06785b334e55f82e369946e8b403f10642d93108365ccf471116230395c755bcfe2dbbb65a806543c00ed0c76376476ff10d9d2457710c253896688c4a4afca066e8064a91b3d465307e6bbd884f0bbb02daaed85b78065e382b9fbd16d8fc894eb453ee821b8b536d7e544950f86eb902e8e4ecbe12cfd4f3b05d22334b8f6b3837b61d7d1150243deb0ebb78dc4746690240a1427cb9af265c32c0c8b073b500857bd251dbcef13b6a2f34f6769d6d94e2c11db8bcaa9482dc5d4442a916f0c2ddb00f767817d9210b3fd3138d300e80b595dc2caba7c43eba93ed75790e3b06e25c352cce763f2c92de272e6fb0112d5d052dc59d7a8693a1ce5e93adf4d89930adf57d77055e667c6780fdf52083aa9370dd643a953fb36b31c844e19168ca3d681102069fd7398736cfa75d80d03b51fc4cfe11e3c2cc0943f7791bf1040f3349ef573ccc85f12ce66da0b981739da7ee4961287fd5639df851e2ac73419f8fb4c4928cbac1c64b2a349731c9c703a263616c67382f63736967590974

abc185658345af3ffb48f88450ee5ab012f705e7bf1d0da3bb31e7b536e31f269526dfbc09654
b02931ff6c7d2e295fe9019181ac39b8d01b864efa8837cebb6836e90569b684845cac715c1ff
29507eb0de608c2e08d43007e8ca09acfa1094df1b055267d72652d8928983aa25872aafd600
2dcbdfa849a0351344e752fbe7c10cc87bb679c25841bc4c981ba743e9d4583fed3007bc4e21
90a5632dfc243dff68a1d9a57390cd83865cd4b7a018e878c9bc2db1216eeb81fc7393c8c5d0f
76818a250ca69869498f331c44c16d4af32faef5993aab6d4061e1b169b6cf8202232d76bdc3d
a3e5265d763648f01a23f237205b609698c09926467ca8681b9b120d94fa437bc412433eba16
8b122aaacf246d9d58736a08a8acea668c94821a9476b3ff4b53a508b286e27756063e84adb6
2a85bb9c423e1c13b3f12b9e1fd533de58f2ed39668a5d82f86554135b6d1fb6ba0d14e704d7
5a8be090cc4f29d6bee2ee8090c659cec6a56a5a3ecc877e41230b210bd679bf2949d0855d51
cf0f174943be861676fdd3b712855d4c6c2d6df3e9de1d64fae2fae748cd77fd5c162df7ab7790
f45fb5edcce7262263b5a1390b7dfdd19999331226532b72aea0d473026acb31d0cfc2355968
42b097b972d894505b646362bccf27803cefe82d96e4ac8d442c0097b80717057071babf7ab1
0e610ebd450e64fd7fa94ea386ba638808a61c07626f9a8aaa3142e6fa6e4dae1b4985aba906
0927cd1e983fb52b17df2e5ede1c907f76d70eeb219179e11e1d7993566e40a256d60bb00c6
80734ce159452f6f670e18d2d36f9708fc66fac812418c3556569bd9360e7936839ee4f14a8b1
e32c69b702c6aef9f38af8b0aecf43f1487ece855207b6c6f07455faedf8b4be4bf5cdfeacee24f4
99df02737172c818ca284452644cd90f7f647b431a4c1cf92ed65af1a23bf9718dbafe7ea81a42
6ee3f8375a0654a60ad5451fe273642db6bf1c3aa6783739dda1cfb01ece752d872818a58938
c27356aff808f6c8563cd63d6e8afdb790ad05df51e8c7b243fec20f809d220093660b9e712c8c
791623dea3eabe887f09346c596cbb938d615431aa88fa176fc89e2a516e49acf43a67585757
6616b6eea9fa83b524b64bae70996a3fdf5753cc75b5b3ac5a9f4c5578cca120d064702fb4a2d
63820109f35ca1e17eac66b94684061e97ab4c78a9bc9770721ec4e10f66386d12f3dd37707b
8ee6aeaae7a44d21d3a114775769991bb7fe438bdb11098c385dec84f170135a2aaf0bb1d52
557a1a76dd2e0bfe945a0a42ca80ce66ed651af8fea89f3b6ae39362240804f4e8d746ad051d
9590ce6ebcb72f15cf54fd91051e830e6ec3993e7e10807ba0b16014898e3598da5f01f1e334
d8e8a578bdcfb69fa484a05ddc8c5c0006a904b492fbe56ad74cdbf28e4eb09f95008f25e21a6
9af7a3caed686a097793a0d16e4a27218cd7c21a7402876314e17547b28330f43f6015029625
1ee70637c8a99d2a82dae0177368caffb11752ff544e54d276f4af1a6f61c5c85e4cec29d199f9
b1365c0247e4e3a841150b85411b80d17ea0fd4156b8e18355d5c00bc29dc45deb673eadd27
1342e1eb56413d4c8f8485f1a322ccdbabefbc4f03975b8a463ef34beb4f2deeb613bcc43a2b7
b8573ec49973c16d17c7fe574de9397b38e8f639e0b9d4cf9bf89644fa36306ec1b75321b410
6d3aff5872948bff27482401cae784bce999e23ea495f006f3cab46c99dfae42942f3c399e05aff
d8e9573331c75eb75976acd62d0c82531c107fa21656a3e0aa6734b68439fe31e7d73c6e6412
9a70d9125f0ce15868d8abb2cfe44a9c0f111b31d9c7f700414d1ba3ba3812d73415494d1fc65
2bb0918b512cdb115265f652bdaf2e3aed365a86256affd5f803664ef92afe0146fadafe99416a
f0953615a4721c64693733274b481a57cd4ce1daf7fb84549795d47c95d0dbb91655fb19819f
52abbc16a275258784655a996b1187d9fed0713cf59a48aca3447cd56522ff76b52a87c6dbb9
9a65a20c11ed12679245e106289f19fca556cba3df0131d3e04c463cce4b4877136401874d08
7f452fd0b9d61d3422ef781d7210fd9f878eacf3980ae82b3aeaff3b09f9ae90281f629df71b0bf
b1e4e898b219a58e90769ecaa0d18db73318e20c204bc8424128058085ecf064282ea391d38

3157f453e7278b56d259702cf0c763d0d7421ea17e88776bd7579d190443672f30e6a9cb31f5
11bdd59b00e2e059cfa33289b867f0f8e599fd13eb2f621ae7bb812c8e981783a366ebbc2e5e
e611cf2dcfe5f95a6324357fb0d75d0c3573a5efdf87bbb2bc6dd0cad41be8c5df2bbddb4116c
a706a6c9c6884d7b22a10db228168beb5e83bb097983968178240ffc7de42e45d22826bf8f82
edba924b51b1a8dba61da2f2cc12511745a1647e0936b0d4734a162e63edbd3041f3f1daa4c
b5743e52b2b951694c0dba5a8bceecd1d6325e6476878c8f0024cb2994805258496c15da1f6
56f5844e1ffad3630045671768526c954a264917fc4d3683f3a5cc05458fb1b6d4fbfe49516fed
085b33b36ac7cb104cfd9566f09f2c3d8ebcdd2a635ce9127f2f393d946afd967e38e20e92517
2b0497bb218109654d14d14953617c3b60cf3ba11b9b5ea4b682682b05bd5b4bde89f8d414f
5e68fa0b9f0b8a5e61de62b956313618ecce25bb363be196cc1a563047e48c1fd13effb4abf8a
146650a89218e9232136dbc37a78125e89d8624fda75cb32ab1e4984d64baf17fa6567d30b1
ddc3a4268df14b477e7f19f5b7b3730a754850776054c69129937c48f920d1fcbdc78a6ea533
161ebaebd5dcfa6b422ea051b13ba2832fd08e3eb1d44c0ee5297d26455f23696c1ac3ae70a7
fc24e3873e4b992c838172dfb37a23c98917d2182c9d92e208efec9144d4238e3fc32769ab31
5e64a6cd2f1c8326eb98abef947c62982ede007345f25213ed7f6d1b523c503e70dcb05be8e4
8f55896a1bfaa34a83e2a5be12dfa1a70207ed22173deac0c17c2df90b733680e5c65ea133c3c
359449b13faf412c602075bd9a6e4531b77212afe3720194abb461d96bd96f6da80bc74f8f34
1893caeff3e673fc7ca2af04a528ab443d97b8d5b177044846f13ed0b0b40bacd9bc6082a35aa
49b52afbcd1c9578c59d85da4d5eaf794cd07035077d22b3f6d90530f83c0c2ed800e26a08a0f
146de0315253450677b93a7b5dbe6ff1b31484d686c718e8f92c8e8eaed0e18232d33434555
6f75818d909daab5bcbed4e0f2f7063145565d606280999aa8afc0d0ecf20000000000000000
00000000000e1c3243

Credential Creation ML-DSA-65

Input:

01a50158208c7b5feb215b52bb89e664e9ed1e7a4d722d72425dd88f19e61a073d5f01aab90
2a2626964696c6f63616c686f7374646e616d656b44656d6f2073657276657203a362696450
23eda4d83bac46d2b42fbe14ca248902646e616d6566615f757365726b646973706c61794e6
16d6567412e20557365720481a263616c67383064747970656a7075626c69632d6b657907a
1627576f5

Output:

00a301667061636b6564025907fa49960de5880e8c687434170f6476605b8fe4aeb9a28632c
7995cf3ba831d976345000000044d41190c7beb848018adf265a6352d001964f4c2ae87ab4e
9289ec16e4c26390265f6372797074616e65a30107033830205907a0d085c8bdbaff82088d9
d02570a280d390943560300f9db1fbe87e0b281dd34373b22af6e0ad0e6846748263146d0eb
f4cb6143ea70a8c35fa41e5f3c0fb09295599c863c77812a08964db261dfdf4a6a5687b00e0fde
ae25472ac2575690014bfb82279a0950437dbe22423ec131ac41d9302e22da60c2653a14d40
4dc4a650e8bf61a98bdd683461a4d2c9be8b2a0bebc47262ca8c3184818075ae28574607d02
13a43f38a753c00113066557f0c0dddb5c79ce6ae56f1db949906ccbdc7f7712eff0890996381

a682ff7c5fb47ca550607d711d3b6ba728a4ce21d67ee30de8052ba73d61d92c2b8f8aa49e64
a1ba39b8c81ef7e3d2626aa0169df2d4033b47d5eb1873fe9815220da63d8b47f0550842dea3
c809f9fc6164c7ae0ce69b6856b619aa54cefd83fbfa09f104a4da8e36bf60dfec6fc9fe69d89cae
7192c1c2a23206b7e9da0187bb83209ba7f49ef57c8074e7ca3e6ac7587802de5510d60c2a18
4ba250f26920541c3d790fd2ff95d1ce31b2da93960df20f1ae63efb8a18c5ccb39660538a69e
81414c25dcecc18f6cfe8a4cb8ecbe99a41e322255a3d39725a18e9c1574d6e8401c67e4c75a
4b7a0fe1bc949df6681b8ef0b8c01a4f7fa64970aeb273b4a2cac59321c97cfef9fa19e6535390
bb138a1eb964f6e8c3806f3ea5b7a3e71e1fd20bc59adf5842f48c131d8500d8232272a45c7e
28998a869149aa7429a4ece595b0404ed354c418bf5137528418ee92d725907f34e1e920cf3e
b53dcc8011c14238703546523be8ac6947a899efc448b4d1e50bd0f67a11563ecc53d0d1a7b7
153ceb58eb1aff06212e4ce76dbcb014af557e445b5652f22c0971f927a95bf4d1e5172d3d15b
ebd7722e03d253386df827dfbb7ddded64407afc2ad5824e09a8dd7df3f23b913caddae29b57
8c3a7e48423618f180e24528216614d838de527fe9d6e3218ee5f2fde059b586d5b0b331509
9805f37823415dddf8896459425f08e46181642aa6d0ddbd700a9fbc1cfe710069472301f957
74a73b8f37fdbdc32c734a54d898be5a09f52179942646b5b3544300832aa5fce24bc02f4b3bc
915d31fba9294a1c467fa57cc9d1d4c0cfb470e2661f79a6b1b85772620dbc6beef93b36a8a40
eeb352db061b15ea723fcd35cf6e50f8599f337ed7870791acac34195a025ba30c170ebfc9289
d7f447ea496718b04f5c9c2b5259219272bc0cab6357b883650026803615fe0866a154259ade
0e052ed8e7581750b2d026ef52d4cf268ab671f3e876a25a0fa31d2d68ae085207bbb22965e9
c2c4264bc51c4266c238ba592dea5c5822fbb42914c5dd429a6f85e01dce3d76f5287903ece8
c31cc3b73de1e2e45f83b2aa7236617dc056d6152b67b2edae81b4b7137f29d3208dd283037
3d81cf2c21d1dcd32b3ac6b5ea3f3cb6a79abdee0de1406ea8b88cb8ada2739a3abd5e00f228
94f1e1913d45d635c5b2274a64acb3cd152cfbe96568b73ffaea3bd6c7c4d2ec3756f61a3fe53
407bd68f3fdf41d591d8f09890cf694d1b39d0e8fe96de07bb33c419df3cda96f39a7f2c13c19a
ee976fd95da8c11d03faaee897faf9404c26cb7bdfaf6193338b32b822ae8742a58dfe915c1ffe
6a9fafb9c9f3a136d026673af9450772a0459a92396cd53521869c498e0ced2d7afead92ac333
e93ea1631c76f1005225e8a799c82678bc9d18f0cd63cfc163890c82325336c3b614927623ab
9a18a7ef8c94fddbd6827e84549ed276d45bb6ea0f141143df9c098014566f88d1431de45316
15d3d1fad48480ed09ac13ab475212670e16cee3614168ac34a8ebd95494aa88b892ec09161
1bd272100d29322a92eb19e4421c7a11300889c1ca618ed53cefe32d3fc1f7089ecd175bf5ccc
8bbd2ae66423edbc919ceaef45c12e82ef16341cf0901b72401a0a9bb46c21cfb66f3d50ef6f2c
5a6a29d35a5be9f2b063d8f2c8ff04d5b157b1bc9a4055872e893ba0fb40ca9881653448b354
5c75e228e54a44022edeca4186b316f4d647e09643d007f1ad8fd61647e740bd3ca4441d840
12758ca32c10c98a87d4f7c103cde536fa2d3d087659e753cae135eed7dffdd685a51247389a8
b9ec7c7a47cc5e7fe386de08ee4111708a76f2b049a80e56d0778e1569025054278befd60f10
0588e395a96e371761f8b77419f2c5440d2346d1beeb3141017f43729cb3ea3a36d4230e9f8f
3acaec1e2b0606f305152474f5cdeb52d6f44bf5df8bcb80f9d8b5ee6ff464b19b5c1ebf555111
7ac7af4971fd8d6ebb203b9902b0f6637876951bfc6d3e88f2579e6984a0afac8896754ca4e7a
989721201b250ae81dde62dd41337f08130fb713a96aeb2ad2b29a8f359527fe8699e1c1da6c
7182da4a38b540aba66cfd35d2c408e62e48c1e457f331bcaadff39347e3bfe7cabc4d9cf8cdc2
24f8316ac36e4422162e2f515bce56a280e68c2e0fdfdcd18b4587558bb3c40d67b2961d0c25

8992c397367dd37d94b4d1df82859c823ac35231723de65047fb5c0dde27417eed04eb4ac5a
5d9aa24435b67ecf68f098d1cd66d5e792a898727bdc71294b94ec8ff0f1df2befe64843ea2c3
6c40923fdd499539e3502688a491f65309023e6e1c819c5e1e7070ef0d0158d930ff5970fc7c9
792f0b9d76f8ca4b3e3881a3cb6d5dd167f01b6efd76ff8a58f13bed15cfeb529ad1d43203a26
3616c673863736967590ced54006c2f43a6fa47db38f5e5d2d94aa83ef5e7dced94487447d9c
e10cd697244532219435583d815fa512f848bd3ecdacc2d77cb844d11251a39ab458b70e5aa
a61ede8eb7045617533d52acd04228006d647e9738ad473e50a0c61e9a94b26dfe72940fc07
4646813d4394fce97b5594179218a20f2bd42115ebbad04036aff46664491662040ec1a6814a
dde32ec5424ec660a0469d894b3abf2e05c771a9ff0adb8490c43133dbbfa151ffe813695d658
fd9edf5d7fda1c25e27a5f6b619f012d6c9ae1ef961d92567ccad73ffc2bb523f5d2549bddad5fc
675305abb85b80fd2219b280705045a14589a6adf3ba62b2bda82327df6b4fcf4eb306c2b863
eea171a85d1f2ceb7dbdeaa7bc9201e69509694cab24adc5bd309d86e3abdd04017583668ed
1ce8a53b1c64c78078783b7a2368d53cf19aee13127a53c7a5ee6fb2926a18f837c11165be71
985c980c6de5e57bf805c5aff36c3eda431dceb0fbfb9fd3b03aefc6a698f5ceb94b31f51f00892
8c059c8f69c56417f3d46f328f4252919477080b1031e5705df2911f0c3c0efa5a5af6a764edb3
3e16b801a6d53dd4bea090f8c3d220b7f040a214319731fb9ec105e40db9d64fd4b4986e14e
6cdb4e0b14f3af8d366e774f31ac4d9ac7eb5d6d16bc41215261f7c56a8c0102f7ad7e18e1138
320f155b42c0e64d046a000318e28886d091e50a2b1df8f057e04a8df6c5889540810ea071ba
325346f39ade318364894c0740af3bf431d8c38123150a334b4a3787fc8a837cf3500a294e835
affe4e9a09ce31583c36ccafbf3cc62ad8f20e1228c83405a21a3a6d3682531a5904bed556c353
c0daf0f38e326c41da4912895e343fc34588aa3cfb795735b3b2211dd632f13030dfb8682e1ce
93762a668e25de69b79fc1d53ba671f789f06aa39d834a2366102db7782d3aca6090db68fc49
227355efe18165189df6bd97872a8f55068e0722faaa26dff5084b24b66073b6a74b024015bbf
15197163daa07c229596b6278113e48f672c3aadee5c6f5043c98445adb13485ea65682e69e
3927b9ded8493d9b0cf9810c401e9c2d7d1af452026cbcbc2bd9639bbffbd97b8b7ce78e6681
6cc25505e68190d993e5282a011fae1a4939504493568326fd64c9992387ef4c9196971b4e1f
394370d62c1c496cfcf1bf2b3dfe0904cbbcb02b1881cdeaa1bf7f0a3c9933c996324d26c6f97f
0d18b2a17fcaaa3596d70a95ace015c2fc286f680724682051a6a56212cef4ae41a928b255e24
d624b1d874e4c4efc052589ee81f6d507a1d09b30928a5df16426f7fd829eb8ada54ee0cabf76
1af18dbaacb418f1c295a46072c1ce9306bb1883b9a209f4c5109145f1e97c84179597c511302
fd77ed5909ea7ac0f2d60dc1adcacaa7e23bec4c2005159b125ed7d37fdd9bda21f25a0846dc6
b32f3eda35134058e950d1461c8629bbaefb9d5739fbdec504ed66a9298cd5220006039e4aa
04022b8a8c30680cca43d4df21bd7eb6edea7b0e5f96f005af22212264c001850cfde261e5140
9ff8e6e3eece85742c0f10143a389b4615cb382db2342e7a50d684a2ca65716618ce0c1ad1cb
eba0929fa4c5cfb938667018a1ba9bd692577e00f0d8739b6a1efad1f5d3c1b6cc49e6963471f
d771b224b025ec6ea45895142fceb955c20aea0833b1d4f428f13001dfb546050919b9dd2670
1079d80e8dd93dd37a97f9c2d98431abe314349f7cb4e7d605e4d97aaa07da3c2d1cd6d39ca
dbcd28724a2e2da77a03dfe93b5bff9a5f237d2e40ba263f183445923320c6869f999f92442a6
0fa612e4f220fcfbc816f985e7f6df8d6ece6a4f85e27fb6afe52750dc542104dc6dc63efcb066a1
fa48cfd11cea6554c951c229d733281877e6c662bd592a08eca842f67489d32b85808b85389d
d48ff50d305e1a70baea958f85d2dfe442c1c0f03e7e1a5abbebdc93ada1f4d89912861f4fcea7

728c365347cd87991494d271fae3cdc089236a45c53d3aa6c3226ce7b937dd542adb2204620
40d890bcaaf690e22f30200a8289c7e3da0438c68ff9089d300aeac1bed53a62025f1c012079a
af84f5d39f00fc57fa27fcdcd72625bd13731026eeea32c797fada98d7560ee8a4e5c93e1f226d2
b2f3b89d6aaab74596e70b56d99a5c115ec59bcbd582b0493d4094ae589fdee5b707646f53b
98025f4b5231751ae9dd7e419bc102fba2db5e97462724cc765d34210644e4570e9b09abb34
195054b50af434bc618a47a7e326bc57925646631aa4a86856f04f1d6cf8e07f3afbd22cd8ae2
f1d0bab6df83bb0498a000888fbf2d880ccc8d65ac24422af331f53df022630679efee4e936616
7af02b3af0e7fa33cf4e39e59b9dcf72905d5cac5532b2706dcf96db1380abf32efa561a34e781
65dd6197481c900654e24b4706a28491c52c3b3fb8fcf32ba847480d55b64cb9221dea21d098
b401d1bfe98cb70723cbff30ffeb96bafdc62a52de49f11dba7f10365deea16d9990134115a5ac
b647791f00a9cd37330d447eb519433d831917ef3086125f1d53914cd1558536ba58871cc78
91c4e75631f68152be3080b2553b3a441be25ded258eee47f30c8d125981264e5a774cdcc16
2b353644d3ce4d23ba7576d90ceb9ddf7834ec84f6ffa3c2c3c1e9ada3829183892624f0ff972b
40924fc9a6c8ac79a94c590bfd06919e30625be03fdd89fdae46dd50b760f12f82b1fe5956148
25b53bbf7aaa16c7d245a983c45df5391220dc7e2eadaecece6eb3d996b7dcb48e088998b04
587b51d2e7e52c6d01d6f277b1f1069dea2f62df32e15103cb631d1746ed9fe6c0f1a3a78d22e
b92113b2acc89bc37523d5873a5204021e263cfb308d7d4aeafe08ebd3d918c16778115894f1
76785ce39055d5bbb02ddaa0b1479128f763d241b20d7f7e32a2e3feb4518a8e3df03518024
7507ff0c8c37c76f47788b16e145c0744012964f627d8c1760b655d9de8095b2b1eef5c959761
0e7c75abe96412a81356148380f2574877e18a992eb2bc831e5537142d4e68e4f768256db12
965fde3c642ab12839dc3b9e1f37fe59321ad15eb94052d6df7689d1e06b26ee670d539cc694
52eeb92a9f156364b1f57242b00310ae887d00187ba6e7d0f984c84612a43c740d23f5b99f2e
5d6970c4e9feeef26cdec2e93811cb87da7b3bcdf48230c1bba3aa5d3425b01bf0a4ed86f2d6b
b195093e5753dd8b8536454bf6ed3237172751c91708bb90c316e0a10bc29417d3dfac46648
3f112aa3f5dbba8d1a6641d8ff48bbe44aeac135f926332666cf5fd9916c7168720a9100a1112
7252f647d3cd2d1a72fc854636cf96ef26ade808a212c27fe22234c3f93bef6f8e341f5828d0cc2
0afa58168eebcff5b0e04323147d521e574079714c5225992166ba61f1054de1d4899606b5e2
111a85ea106fdfe7776032db4d42d9cf75c8a421820b1f03290c951014677743c1bef216fdc15
de342f9d23d8fcb078105da4ac211329365c3f264a8377d2ee8377d80dc486480faf24956a15e
36841cca151b0442c0801e2b8ee258c6c7a3f968c7bd87d4599da3d5b8f9bcc3d02be135e996
ae012af494f0509887655c4fef7ccca5cfa77df92c4bf2a2679d502580e9e1371ea82c38fe3fee2
81486600cafa4c10ffb1074e08b91c038eb4edcdf50715c0d9b5c9db421293408e80e54b4ca6
1d1208e3347527425509f908cbeaf2cba24592d5bb5456f86e6dbffa5b39e631137960eda642
1ccab278ff279a0b0c74d2e1fd02e3c05a6785bb675654914bb27076d5debeaeb961bacade06
06d9e72ce14d54eb6f0e71bffc683aaeec24d56b6cba4d1fda0b61383ed6a8796edd05a0798b
b9101c9a51284d8cbc2a993ac88f9e7ba20808acefbd0a17114818400f4cad2308a3170f16e57
7abdfcef3564cbafee1f9475e9c023acc3a2d40c446b0ccd1e563a701191d33fbb122c8b284fc0
9275686314f110ede3f76bedbb3649363d221ac16e2e8ed79d5a3693962743be5059b451e39
76b8a6d58ee9b3257a2cc4275db420dc6c33bc22d9506da94cbd08285a85be7982bb477bd9
5b640520f2dbe7118b19d9483407b055ad82955448f50021b16f7aa8ec7d1349ca29bc465c1
10ca6a1643af40b76f32202c4482cc103f3c4e4a03b45096f0239f9a64b9de562ef36526b4f99f

2f38a63330605a6c40c5ff3bf68a6da1517fb95c64e02f98d59494406ba8491b1774d3b9af147
4d83e17ae4543d82b5ece41a58056f5739e99374851460c486fb22998217ba635571172bb2f
9f4a8d35cd1717bb617b2a05d282945c6d5f7cc7a772fe5f7cacbac20a3d710267a127bef1741
31ee2dec75027dd22c19166a0358eebd7bbd40d5a86e5705c0a1e59fba34ce37476e5fc9ae2
93b5ffc42e61d1d2710092609cf50e4612e194e4db5320af9587b3a0dca4b88a892784a56f21
748d76be226fe38eaddade367f75b6d45caefd2dd797edbe69d319f52e9ab2b47a7ade1e8f00
71a5052193a456f8c9cabc4d2fa005960851041797e99abb224353e6f809abed800000000000
0000000000000000000070b15192028

Get Assertion ES-256

Input:

02a401696c6f63616c686f7374025820262ae1aecf82e3fd33489a3a70a59d2a0db161e6a144
eef412518fe1fe3bd4460381a2626964581911402ef9ec5f449eb8ea1d5f645a0e585f6372797
074616e6564747970656a7075626c69632d6b657905a1627570f4

Output:

00a501a2626964581911402ef9ec5f449eb8ea1d5f645a0e585f6372797074616e6564747970
656a7075626c69632d6b657902582549960de50e8c687434170f6476605b8fe4aeb9a28632c
7995cf3ba831d976305000000040358473045022100aad84e3fddd28d95223a4c33f9424578
8f99f2bbfdd94c700109ffd336f2b6022062a8f2dab99c1945cfb03cab0a77fa8e4f591389aebfb
caae22d4af126f6d1c304a36269645065fd82a31143f78f40697a0938af90646e616d6566615f
757365726b646973706c61794e616d6567412e20557365720501

Get Assertion ML-DSA-44

Input:

02a401696c6f63616c686f7374025820b74ec47517bedcdf7b73a68a7b03ad5fbbdf1c6ce9507
05a0e7d49fcc998f76b0381a262696458192467a4d62c03439fa0441e4d829cf7cc5f63727970
74616e6564747970656a7075626c69632d6b657905a1627570f4

Output:

00a501a262696458192467a4d62c03439fa0441e4d829cf7cc5f6372797074616e6564747970
656a7075626c69632d6b657902582549960de50e8c687434170f6476605b8fe4aeb9a28632c
7995cf3ba831d976305000000040359097461 7dcce5f68e669552b905fcaee91a42a1b5cbf45
128cc740f03189cb4a376e39f7c7a855a6bdadcc2ec3a7c5ecdab897acbffd6d7aa623ed871c3
9da9ff4a62bf8307f764472560fac2e3871de88acb8e9d24ad6216c9cea70249271c6f53a73da
e85b76c5147872dc17455f9523f8d74f704d0d17bc329de220ab6c9668b6b0de122a0fd6386e
5bb9e5831fa9e018d78423763f2080e23796f4bce11fc843999d4cea7f9d038948532a78386a
0ba1ff118980c56b8942f5d9a7e59cc24e9cb1aad026d167aa03fe57c15740096b85149758d7
b3d649d9933e939737e1b74d20b4f20b85bab776cc52b237383749e8315a4bec77a08a4368
43c836b70c347958e4f445df1cf8854fb99ba7ffa2ca5fcdd2e455c18a557e899c51eab7be93ac

9cb5774512bfd15512e54a5b175e466fa4f01a7ae3e0b6c7cc4aa7696c4289b575f89229b3cb3
d4b73acbc4995fdfd3fbcd3b99d8230286e5bc02e4c970feb67533cec688bc83cf907ce49ebbb
96e9a14c7e7f39d0f4243b8f7006e486d79fb38a105e3bce6cac0dde583b8df9e0bec1a64a397
a77d50429e123954510a4bae86c440d4a5d973d2c0802b8952352d8ed30d1f3888c3bef9dd5
1cff6c86f56af3bda1ab5472042310c79897ce8eb255fb6a493fb90b25b8340706d275532eeaa
af4cba940239c442cb3b696d45e8eae5047818c8d61035f0b48ea18de904c184bea7cacc7858
8ce5ab7dd451bd2b069d4a74998e49aa3303f579dfc497a48f4e5df660638bb427b320975bed
5b3b7dfac54dc98d0be70d4c3fad61a3124d65860abe08f3d4e5c8215ce5bb296d5b129ef114
a21167af82718394ad538e872e103e1a5fd64b29696b4f2591f9b7226dd019a154f90cc63881
85cb0ed46a2b84fc421bde0d27262c4e752c50c166da8c0987641fb15ae9f0c9eaf8f4fe20498
48afb899a567938aee48aa76de37d25ca194efd1c082f451d51aa47a8e7cf05b0d68e4aba7d3
cb96cae9ac1e2efd518c6442c311bac8cecc08ec41678a15109785edaee2115a303576532d90
1d8efb518e7da46e69d54af5f3784987bed9ef701673b5b27315410bb62f0649c286ad6d7692
18cfc21995c0075aee8f3684ab4a30e5b269e0b79abb23d47732d666b93b3d930bdbcc944de
a16f7bc6c96d7208573024b35cbec32d1365b2f44a94718003368b0df2ebe3c0edcb5d483e9f
cb815be80d04f98a6ad8693f042af180cec17095433849535e8c918f5d94998f527fe5c56f13f7
5de633a568a827bda0f4fadc74fea664deae1cbad94c2bb22bf39e4e9d38ec7c1711d4fe92878
c5d124a4cdf8580c7356fd4f6c51184eff9dc8407d8e053d74c95e63e8b567c6b8e5124a235a4
ca831c8f2132715c20a13bb354433cdecf94301960f322d05c2125f5e25978e8c512386c21725
6548fe8496c41e62e5db59925deef2740b5e91ec6e4f185a036eafc20ec49bd43f942608266ab
ec0f006c28debb2e1186b88525a970844b476aad4c603834eb5255a402bc5b6156fee6295eef
700a591546e9d9294afc8e1c54f700a5a5f03d87808352e4e43ca6f7d1fb8d1c5332b89e04c8b
f6f6f67aa5e389b701ee612c8ab4397430c267a58e0c6c56f89a55d36e039124ee669a541762
9289e3c2b2d04ad3b18b59ccead6572f0c1ce9036fcbeed55a822e5d7b31887fee76dcebcecd
b4cd9d0aac43482cbd97a62777998b52da4cea11f343da2df1c9449f646c295d7f4656589a42
7f9198a9bd4b9eb48fb6fdb49325a0ea30a938fa243df72b59cfecf0be3d56e576b84a60c53f02
1388a044c3170a20d746f6ac9bc47526e1e18a98f98c287de6beba4ec69c722e9e8f7978fe3b1
bbf5b290e220dd46c40088b8bf4ddec0b7e582021ba2f877f4f47af692796081b0b85a6e9914
e2dadb6e6257ec9958e0f0921322271612bfdf0a06ca64501dcc12ccce059c58a8872f18f0966
1d24cacd5edbeea0796c99c6fd71bcde9a87f5f93ab11a4b53b04ee51d6a500f762935cf1add4
b0fd30aa4dfb26b7f43a057fcdd7933b5dbfb8b2e94f92a7ba3e0b963374bdb52d9fa6cbcca2a
b698baa49486e4a5760674e943e5af646652ffef8f939dfcf0b7c9559fb660bb9e58842449c697
7c079bbda9a8d086117cd07dd338a5fcfc3cc5c4d979ca7fde79d5daacbae49e41a90eb7c61d1
31b05a1b54a9aed3b791d7f3c17c5ee690027902a53e4f3f16cc65704c266c599cbe278ae662
7567efb6d83a9d3280c3281b6fa924545153df3411f1a974e7917a164aa416dd8602a907b294
6abd2a951a952b478239c23a364cdbc065fd7ad3d224f8033bc8124f3353b59a245e25fed45b
78bb968f0616c1f7015dd5d01f789f9744354dc447af19b3fe890a03bdc50dc5b8220cf74e5ac
eb468d0b233b691326024cea58a7aeed8692fc22c314fe27ac01633cd53eb48c1086b8973958
b25d86091c6b2653d84b4e2fb5c2b542dac0d37c003d0f83c005e3fcfb59d916f128f6014cc1a
43ddab8c0da2d76bad636e04bf6f15be8004eaf18855fc0a258cd9731eac2853ef290daa92409
034fcd91cb6e2119d5ecfea2748710c0b2ea2d45697cc678333fb3bba8106143657e173bb147

933048d6d900afa5a89f044de8bfceaf6daf115b4ca6f41ec1948d3096b881ef21746bc871a13
902ecfe97a5aee8b50a8a3018fc45dcd69ac4a2e8b0bc6896ed55728818e0146f929893e36bb
488770bef7a0191da6186205b32ceb103d75e4ceff5c8d95fd620426f00e593981473c61432b
28aba3553dd320ca4910b075413d1af28de703c86f293f5090c259c654bd39eee0f802b9d61a
8af5c74d2c0907ad2289d3e0ca9d7c7491b65bb37b82eebc08573eb38956f51d2c0119ed13b
b440c311dedd026d0a36a72d2cc2dc63f6986ea3c29fb58f7289899773fb55fd912ae89d83e3
3c83571c366e99e333d4b31e274b2adfba4ce2cf4bfcafa85b75a85be6f6002b8dbd1314d527c
0a648fbef00ef73e8cc841871480700968518 47ad892b8fe9a45234219c7d762b9e0ce4913e2
a981e4a11020e093116ba08f2429ca54bb2e13c196ee9c7323388e5c0c285ddc3f2e9bd8a13b
fc91dd568c85be1303493de4f65eeaff68174304f8531d5fed1f1a5bb6df8335bfd6abd49ab8af
520d753ad0e273627cd5968f68d174bac462929168b4b178e3388328c13d50c22b541608654
e005f59597cd03d225e88bcca81b580e68605d337020e0f121c242d32343d405f6393a6b0b9f
8112964666875899498a8b5c4f3f402123139616b7785969cc4e3ecfb0b0d171d22272f35585
c757679bdf5f70000000000000000000000000000000012202f3f04a362696450a7807134
18c545a38a6c664bba8cb0646e616d6566615f757365726b646973706c61794e616d6567412
e20557365720501

Get Assertion ML-DSA-65

Input:

02a401696c6f63616c686f73740258204d751eb7308061789efbea0ce788b6771eccceeb65c7
c4fa8a0e77470a4921d90381a26269645819622518ecb4dd41109f3a62008c269c085f637279
7074616e6564747970656a7075626c69632d6b657905a2627570f5627576f5

Output:

00a501a26269645819622518ecb4dd41109f3a62008c269c085f6372797074616e656474797
0656a7075626c69632d6b657902582549960de50e8c687434170f6476605b8fe4aeb9a28632
c7995cf3ba831d97630500000000403590ced403cf1952470b4d3c91ab18b1d5a711eb4fa528f
994254b6f88c3fd2a0bffc5e1137d4ef15cd6efb9037da9fb27f440ae17032dcc5af534a6e8d23
ac860a4a4174de3f1b000ee70dcca80f5f4cb3b014084a9d8832322f25e1cee758c372fab4c7a
36f440232279f14e1fda94f322beb14c0dfa41af651160785a02c6e723674da00818f29865b91
44c4a38ad21b9e3521cac8674c754dcc6b8024a1728a66ebf81b31160b89c7462d86a71344a
28dd1b2b7c64cfb3623a7e24e275e9ea5296020ec655d0e5a0ead28c676b0657a0076da87fd
7a0710f62a6f19f33e64056134189fedfc5f81b9d47ffefa4fa1a7d3ff0499cb1863c6091832203c
8e27f5954957f097b91be4606fe5e4eee8b1c25e911d24e50b3f9466ab4a05f3e32f660b9154
8c2c5516afff13e9e04b3f7f22b35694676a59acc92887e7be0874d7342c31ff25efb6dd2b9951
5b71ca7c7cd9baed44c8f79c82a9f5be231c0432f7b2a4bf5731b5cb397c78acc3b92e48ddaf6
8e134aba23a858d620199c330c19f387bc136bf11086361fa6365408ba3031f8f5e02d72a295
a81a90187b1a9b76874eb12d7ef938817db77bd8cd315a5918b4f8204f3e24e1bc16d84023a
e7fb41bfec52a6e030f497753d248cef86a670ff64c4fefecc1c01111339d963bdcb4a79ee6527
3bbfe2b639382405632e0a8c93576d2ee51b9534ef90db84490dd9ee2c2d5522eb35923f5f2

d07b82b9028cc21c6d31906ee65269f67324115d56af1e1728b3820a5de273b15a2483521acf
9bea3faed076530fee0f163e29e2877fa839b6d925278de7c944872f14232048c371204488c1
b8dd64aa9ee96da6c0d3163ae042893be616a84a26679a7c82933d4f072aa192be559ae4a3a
d06a75cec06bf40421404ac6d53f239fd3428763a58d0ae95015929e6ad0481db7813197db3
a5b83df7772d51622187e4e137cf53b2e97e2476d0f55a6c3339cb22b1ff99635806d5f95197f
d5e9743044d97d55033321eabaa563e6c9a0a526d4e9fe0d335113554fc58ec25e2cd2abdb9
e1a9e1810068b7a380e16302c3664f560799f75dc265af661d77f51e0f806c2108ecba6960d9
d95b5203f2470640af838c0a7567a9c2c84c52e43ed4ff73e8ecb0656f80fdda385a398c3c663
09147d1d4b9e3fe2e1459664981928a51607a32218fe424507f1b1a085fc6d8ba108541e9b6d
9cef885ca91ada134158ebe940c020558d3748322c3e476b43cb018f79531521418488a870ef
3824acc06d81c0e00396cdfbff7efbf9579ebedc1537a7da8f2cd3f92d92c1f6da991c7d69a7ce
35bac74ded90f146db7c1e9055cd6cd2ea833ee6a99839ade589dc5ab75e79b760ab8e3971f
82184bb910f137cdae25a4096e3da1b31edf398bde2031c9cb8089fd158f005410bcfdd66e86
4e5fcc6b1169f5555e1309e9f6bf22de1317837656420c6cce53782bc8dbf6726713f6d2a3078
5127155686371d9bdf4fe698ef38b53822fc831d47bb5ca5a47e6fe525859485747d6313207c
3e2ea87d052d8149f86e328332602679c93e65cfd05a1ca4ad7dc0873573dccccf09538797dc
2980667f1e8eaf56ce1fcebf3b0346a1b1f030b39b0cbcf0013ce21a3ff330b59e45685cf66f9df
4432ca4e53c97d71812b5b631aaf78e064f4bb088edb5be8cff77f86495bb00dad27aeca19d1
d68ff025b053ac38b7a6c6dc23c1b716537934354bc0d586179530529a25efb613bf89913ee9
e3ad19c42a0c6483d02425d94f06b1b3b4aaba341d22ec5496f4e1877dc9eeb76ad01da288e
cf9c091ffcc4c44c0cbf886d930e6c361ba204677eb2cf0339e936dcf17a055ef8215ce83061cb0
cb7fbde07f96724614ddbd53335adc72a9f2bebdd5ee786c417713cc2e486ffe6dc2028367de
d7f563f9be09594db18f22ae33eaa66e15056918fc71a12429e540a751d4ece33ce350dd2bc1
75732253b4ca1131d91c47b53f682c4fa95f5bde8bfd9f19a2e31fd5c33b63778d2ee71315261
95528044140b2797f178c4fadfe30b63c0f0b3f069c11a4261f9e1f4ad7cfde28e23906de077ed
b693cfbd0a4c2636000d781c485860d676e6432a102f5426d0df4cee44d619c4f3f6161e16b7
bc3702fc21a94818ba0807ef940b19e07b5a594ab7110a0456311e37b6013208e6c78e59bb2
3cf83430a593fff02caea51ca2df1ee5ebed67fa6cc53f3cc267ab532df57ed28b5edfacbf794be
7e7449fd677d10f79c883467761be61379283422e889197b01ac1774faa213f216752239a792
9146caa68e7073206349e40a066e3417a14f89c4212c95ce078489f60641f6f2087dc2208af55
4fc586579df88466d531d53d3d051d6894ca143ba73de4079efb3ec3f5a219ff440696ef3fa918
74f97393b29daadf4db98de6847a49f1541c888ade3813e294cfed313d91cbec45163889b7d0
b14bc29911f3cc23dc4020c8040dd95f1bf9659ac4973cfd58d0da2b942d78e20c92e5f1a3a3a
e8704e51b54d392bb1c1361275ffe6546cc3a7930dca286522d123fecdcb03c68b7bfe2be9e68
8c82416eb888c272d3b34d679acc0994a2d625fd5d89f8394f854d0dc3a17968abc6e021705c
cc4c267ca2ba4b0de5b95602f16f68e591507bc03f3c45687c32363641173267dfef783f34f050
75485af6877b4cb259e7bf7e8f2063eba8bb7a8c7f12723c02fe03f1435720720836d88a9fa63
1b4bcb0ab52db24519fff518e0884f21c4255780003969dd8af26c81405637e5921ddc745ba7
5039950fca41a4681dd56b4cc92a4c1c8e93911aea8f68dd9ee1bf017df9aeb925fbfdb3ce34d
5d872ef1bb8be6ff526dcf3c9e1b008d7889e64af809b8f8e967688d248bbeddfafc9987cec526
5150fcff743382ce53527782be165fd11d9694fdb26ad7c8d2a1e5b771edbf78faebaa90c3282

5cbeff0f2c2314f577d67711dc2f3bfc01ece09fd6aae0ec3dbcc722074b6212af25d8db165cb0
44ba0ecee17af617478493d5022b0738d6621d9f04b175a61cef36b8bc3a89e0773c9bfce5b1
413693b8e84dbcefb142062b037596ed22960735d02fffefb0de6233719afd741b2448337799
6d3cc0c8b183897f98c76c29190fe2c7baf72aa31a9f625fc72cf464055822924958895e19c918
3c212bed93bc165267ed487ca5bc9a9f5c797f69553cfed6522695e71c28442cfb4cebccc5175
eca798d9b5de549fbf4db04fed5850fe909661ef713dcaa1dd1318374132ee1dd79c02409dd5
ea1cb520b405e9fe0bc435f0a52fa18237e700465b78f1a9055a1a8f53467aeb4106c57000307
0d77d96b44b91e5ed2d48830f24ee79bc87ef2b3b798bfc3686f7497d5c299b43183920e3c46
0dfeb44bef353e11431200637c1eff799cd6fa34255ad1a5028fedd8284439caa9534e9029822
78f050b4e926281225525d9624d0c63e5734f9e9181a30f5f84aff0e9b26aa9876582e27dba9
26a3607faf4879e80c5b6b271ea06e653678e0f97a31b495df297cfad24ebf3b12a07a602270d
0b4dee04e99d3c7849ca27612b311e229498895a12d8e0981a4a72997ead4684427d6b5407
4c7db7436ee69b395272d0a71b11e6b15943d1cee0bfdc5dbd9308cdb0648fbc541fedbb8caf
2415f2a59bf8869eca504557c370d8d6d68ebd25d83a28ce1d223082e86e094f06f524631617
2cd1271231b88860bfaf58776937de002ecf375fea59a2b9095aecb498d814dcf590c6cbbde8c
f970bff542f5763db6207842ec65dc97e4381ce5f5d1732c0186b6a21d97b67a875400420c9a
d90882afa1ff4a5b34fe60ce21f5b7acd1cd84c46d393696c1f43773b1f30eddb76996afce912d
1d4411e61a8bb5a2c2cda6d6a9c5682e74058d503651dcde850adcd026f886b6085d45f5ec5
97e6fce6bbebfcf9b9c873b79902c174d1ccd7722f232b1b166ee065af450562975bd57777906
d11cd89052b8c3249c342af6bc91b33b4dd75e437d2b32ecbd54cc24f0758ba77f79adb2ed81
0ab56251ece25e21c74a147bcf96c2956257ef41ba47064cda71accdd83a14246335ad9c4c1fb
5a2e6fa8ab39336c99a121e10cf92a0325943595da12d994add28c9386ee23907eb1e52138a
42afc02a58c58c8066617b48798f6d25f9fb38d95fd9002fd0941088cad01aa2bd9b12396c3f7
7136def0e438b0436e2b56005d003e7b87d91208d015ad704027da38187c126b1ec4f36d1f1
e32721bf96d2b48c8ede7f747617f76d0c0e0015ece149856220819d8086f4ffb48be64fbd065
7f3fa9578c6a7ed1c826ec03ab6b54cc324be5e6e7d638c9c8839abed73ad08ed0bf9f96e91ba
9f73cc6ef91c80989a3398aefcdb47c3a9c32329ad3d5ba94ad25d5e345d86b1b92b986d2a67
9e679b0d9df958e2b81b9dfde1787afd208ba59526cd8373ac614f5789188bf3cbb20c5d0649
8574630ca18db7a154a7f4bb53842cd0cfbdd7f41ea02e5f60fcfeb6a5fa7e91a5dfb1a0483a2d
c0a385a8da6acb9d905090d5475d1d2226ce3e9ec16333666afd105314461e7f70000000000
0000000000000000000000000000040c13191f2504a36269645025919e6571314d93977a51fb5
0597c646e616d6566615f757365726b646973706c61794e616d6567412e20557365720501