Stream:	Internet Engineering Task Force (IETF)			
RFC:	9935			
Category:	Standards Track			
Published:	March 2026			
ISSN:	2070-1721			
Authors:	S. Turner *sn3rd*	P. Kampanakis *AWS*	J. Massimo *AWS*	B. E. Westerbaan *Cloudflare*

RFC 9935
Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

Abstract

The Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) is a quantum-resistant Key Encapsulation Mechanism. This document specifies the conventions for using the ML-KEM in X.509 Public Key Infrastructure. The conventions for the subject public keys and private keys are also specified.

Status of This Memo

This is an Internet Standards Track document.

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

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9935.

Copyright Notice

Table of Contents

1. Introduction

The Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standardized in [FIPS203] is a quantum-resistant Key Encapsulation Mechanism (KEM) standardized by the US National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) Project [NIST-PQC]. Prior to standardization, versions of the mechanism were known as Kyber. ML-KEM and Kyber are not compatible. This document specifies the use of ML-KEM in Public Key Infrastructure using X.509 (PKIX) certificates [RFC5280] at three security levels: ML-KEM-512, ML-KEM-768, and ML-KEM-1024, using object identifiers (OIDs) assigned by NIST. The private key format is also specified.

1.1. Applicability Statement

ML-KEM certificates are used in protocols where the public key is used to generate and encapsulate a shared secret used to derive a symmetric key used to encrypt a payload; see [RFC9936]. To be used in TLS, ML-KEM certificates could only be used as end-entity identity certificates and would require significant updates to the protocol; for example, see [KEM-TLS].

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.

3. Algorithm Identifiers

The `AlgorithmIdentifier` type is defined in [RFC5912] as follows:

```
AlgorithmIdentifier{ALGORITHM-TYPE, ALGORITHM-TYPE:AlgorithmSet} ::=
  SEQUENCE {
    algorithm   ALGORITHM-TYPE.&id({AlgorithmSet}),
    parameters  ALGORITHM-TYPE.
                  &Params({AlgorithmSet}{@algorithm}) OPTIONAL
  }
```

> NOTE: The above syntax is from [RFC5912] and is compatible with the 2021 ASN.1 syntax [X680]. See [RFC5280] for the 1988 ASN.1 syntax.

The fields in `AlgorithmIdentifier` have the following meanings:

- `algorithm` identifies the cryptographic algorithm with an OID.
- `parameters`, which are optional, are the associated parameters for the algorithm identifier in the `algorithm` field.

The `AlgorithmIdentifier` for an ML-KEM public key **MUST** use one of the `id-alg-ml-kem` OIDs from NIST [CSOR] listed below, based on the security level. The `parameters` field of the `AlgorithmIdentifier` for the ML-KEM public key **MUST** be absent.

```
nistAlgorithms OBJECT IDENTIFIER ::= { joint-iso-ccitt(2)
  country(16) us(840) organization(1) gov(101) csor(3)
  nistAlgorithm(4) }

kems OBJECT IDENTIFIER ::= { nistAlgorithms 4 }

id-alg-ml-kem-512 OBJECT IDENTIFIER ::= { kems 1 }

id-alg-ml-kem-768 OBJECT IDENTIFIER ::= { kems 2 }

id-alg-ml-kem-1024 OBJECT IDENTIFIER ::= { kems 3 }
```

4. Subject Public Key Fields

In the X.509 certificate, the `subjectPublicKeyInfo` field has the `SubjectPublicKeyInfo` type, which has the following ASN.1 syntax:

```
SubjectPublicKeyInfo {PUBLIC-KEY: IOSet} ::= SEQUENCE {
    algorithm        AlgorithmIdentifier {PUBLIC-KEY, {IOSet}},
    subjectPublicKey BIT STRING
}
```

The fields in `SubjectPublicKeyInfo` have the following meaning:

- `algorithm` is the algorithm identifier and parameters for the public key (see above).
- `subjectPublicKey` contains the byte stream of the public key.

For each ML-KEM parameter set (see Table 1), we define a `PUBLIC-KEY` ASN.1 type as follows:

```
pk-ml-kem-512 PUBLIC-KEY ::= {
  IDENTIFIER id-alg-ml-kem-512
  -- KEY no ASN.1 wrapping; 800 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { keyEncipherment }
  PRIVATE-KEY ML-KEM-512-PrivateKey -- defined in Section 6
  }

pk-ml-kem-768 PUBLIC-KEY ::= {
  IDENTIFIER id-alg-ml-kem-768
  -- KEY no ASN.1 wrapping; 1184 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { keyEncipherment }
  PRIVATE-KEY ML-KEM-768-PrivateKey -- defined in Section 6
  }

pk-ml-kem-1024 PUBLIC-KEY ::= {
  IDENTIFIER id-alg-ml-kem-1024
  -- KEY no ASN.1 wrapping; 1568 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { keyEncipherment }
  PRIVATE-KEY ML-KEM-1024-PrivateKey -- defined in Section 6
  }

ML-KEM-512-PublicKey ::= OCTET STRING (SIZE (800))

ML-KEM-768-PublicKey ::= OCTET STRING (SIZE (1184))

ML-KEM-1024-PublicKey ::= OCTET STRING (SIZE (1568))
```

When an ML-KEM public key appears outside of a `SubjectPublicKeyInfo` type in an environment that uses ASN.1 encoding, it can be encoded as an OCTET STRING by using the `ML-KEM-512-PublicKey`, `ML-KEM-768-PublicKey`, and `ML-KEM-1024-PublicKey` types corresponding to the correct key size.

[RFC5958] describes the Asymmetric Key Package's `OneAsymmetricKey` type for encoding asymmetric key pairs. When an ML-KEM private key or key pair is encoded as a `OneAsymmetricKey`, it follows the description in Section 6.

When the ML-KEM private key appears outside of an Asymmetric Key Package in an environment that uses ASN.1 encoding, it can be encoded using one of the `ML-KEM-PrivateKey` `CHOICE` formats defined in Section 6. The `seed` format is **RECOMMENDED**, as it efficiently stores both the private and public key.

Appendix C.2 contains examples for ML-KEM public keys encoded using the textual encoding defined in [RFC7468].

5. Key Usage Bits

The intended application for the key is indicated in the keyUsage certificate extension; see Section 4.2.1.3 of [RFC5280]. If the `keyUsage` extension is present in certificates, then `keyEncipherement` **MUST** be the only key usage set for certificates that indicate `id-alg-ml-kem-*` in `SubjectPublicKeyInfo`, (with `*` being one of 512, 768, or 1024.)

6. Private Key Format

[FIPS203] specifies two formats for an ML-KEM private key: a 64-octet seed and an (expanded) private key, which is referred to as the decapsulation key. The expanded private key (and public key) is computed from the seed using `ML-KEM.KeyGen_internal(d,z)` (algorithm 16) using the first 32 octets as *d* and the remaining 32 octets as *z*. If the expanded private key is generated without exporting the seed, `ML-KEM.KeyGen()` (algorithm 19) is used; it combines seed generation with `ML-KEM.KeyGen_internal(d,z)`.

A key pair is generated by sampling 64 octets uniformly at random for the seed (private key) from a cryptographically secure pseudorandom number generator (CSPRNG). The public key can then be computed using `ML-KEM.KeyGen_internal(d,z)` as described earlier.

"Asymmetric Key Packages" [RFC5958] describes how to encode a private key in a structure that both identifies which algorithm the private key is for and allows for the public key and additional attributes about the key to be included as well. For illustration, the ASN.1 structure `OneAsymmetricKey` is replicated below.

```
OneAsymmetricKey ::= SEQUENCE {
  version                   Version,
  privateKeyAlgorithm       SEQUENCE {
  algorithm                 PUBLIC-KEY.&id({PublicKeySet}),
  parameters                PUBLIC-KEY.&Params({PublicKeySet}
                              {@privateKeyAlgorithm.algorithm})
                                 OPTIONAL}
  privateKey                OCTET STRING (CONTAINING
                              PUBLIC-KEY.&PrivateKey({PublicKeySet}
                                {@privateKeyAlgorithm.algorithm})),
  attributes           [0] Attributes OPTIONAL,
  ...,
  [[2: publicKey       [1] BIT STRING (CONTAINING
                              PUBLIC-KEY.&Params({PublicKeySet}
                                {@privateKeyAlgorithm.algorithm})
                                OPTIONAL ]],
  ...
}
```

For ML-KEM private keys, the privateKey field in `OneAsymmetricKey` contains one of the following DER-encoded `CHOICE` structures. The `seed` format is a fixed 64-byte `OCTET STRING` (66 bytes total with the `0x8040` tag and length) for all security levels, while the `expandedKey` and `both` formats vary in size by security level:

```
ML-KEM-512-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (64)),
  expandedKey OCTET STRING (SIZE (1632)),
  both SEQUENCE {
    seed OCTET STRING (SIZE (64)),
    expandedKey OCTET STRING (SIZE (1632))
    }
  }

ML-KEM-768-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (64)),
  expandedKey OCTET STRING (SIZE (2400)),
  both SEQUENCE {
    seed OCTET STRING (SIZE (64)),
    expandedKey OCTET STRING (SIZE (2400))
    }
  }

ML-KEM-1024-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (64)),
  expandedKey OCTET STRING (SIZE (3168)),
  both SEQUENCE {
    seed OCTET STRING (SIZE (64)),
    expandedKey OCTET STRING (SIZE (3168))
    }
  }
```

The `CHOICE` allows three representations of the private key:

- The `seed` format (tag [0]) contains just the 64-byte seed value from which both the expanded private key and public key can be derived using `ML-KEM.KeyGen_internal(d,z)` (algorithm 16) using the first 32 octets as *d* and the remaining 32 octets as *z*.
- The `expandedKey` format contains the expanded private key that was derived from the seed. If the seed is not exported, both the expanded private key and public key can be derived using `ML-KEM.KeyGen()` (algorithm 16).
- The `both` format contains both the seed and expanded private key, allowing for interoperability; some may want to use and retain the seed and others may only support expanded private keys.

The `privateKeyAlgorithm` field uses the `AlgorithmIdentifier` structure with the appropriate OID as defined in Section 3.

The publicKey field contains the byte stream of the public key. If present, the `publicKey` field will hold the encoded public key as defined in Section 4.

Note that while the private key can be stored in multiple formats, the seed-only format is **RECOMMENDED**, as it is the most compact representation. Both the expanded private key and the public key can be deterministically derived from the seed using `ML-KEM.KeyGen_internal(d,z)` (algorithm 16) using the first 32 octets as *d* and the remaining 32 octets as *z*. Alternatively, the public key can be extracted from the expanded private key. While the `publicKey` field and `expandedKey` format are technically redundant when using the seed-only format, they **MAY** be included to enable key pair consistency checks during import operations.

When parsing the private key, the ASN.1 tag explicitly indicates which variant of `CHOICE` is present. Implementations should use the context-specific tag `IMPLICIT [0]` (raw value `0x80`) for `seed`, `OCTET STRING` (`0x04`) for `expandedKey`, and `SEQUENCE` (`0x30`) for `both` to parse the private key, rather than any other heuristic like length of the enclosing `OCTET STRING`.

Appendix C.1 contains examples for ML-KEM private keys encoded using the textual encoding defined in [RFC7468].

7. Implementation Considerations

Though Section 7.1 of [FIPS203] mentions the potential to save seed values for future expansion, Algorithm 19 does not make the seed values available to a caller for serialization. Similarly, the algorithm that expands seed values is not listed as one of the "main algorithms" and features "internal" in the name even though it is clear that it is allowed to be exposed externally for the purposes of expanding a key from a seed. Below are possible ways to extend the APIs defined in [FIPS203] to support serialization of seed values as private keys.

To support serialization of seed values as private keys, let Algorithm 19b denote the same procedure as Algorithm 19 in [FIPS203], except it returns (ek, dk, d, z) on line 7. Additionally, Algorithm 16 should be promoted to be a "main algorithm" for external use in expanding seed values.

Note also that unlike other private key compression methods in other algorithms, expanding a private key from a seed is a one-way function, meaning that once a full key is expanded from a seed and the seed discarded, the seed cannot be recreated even if the full expanded private key is available. For this reason, it is **RECOMMENDED** that implementations retain and export the seed, even when also exporting the expanded private key.

8. Private Key Consistency Testing

When receiving a private key that contains both the seed and the expandedKey, the recipient **SHOULD** perform a seed consistency check to ensure that the sender properly generated the private key. Recipients that do not perform this seed consistency check avoid keygen and compare operations, but they are unable to ensure that the `seed` and `expandedKey` match.

If the check is done and the `seed` and the `expandedKey` are not consistent, the recipient **MUST** reject the private key as malformed.

When receiving a private key that contains an `expandedKey`, [FIPS203] stipulates in Section 7.3 that before use, a "hash check" **MUST** be performed. That section stipulates two other checks on the type and length of the `expandedKey`, which are ensured by this standard.

The seed consistency check consists of regenerating the expanded form from the seed via `ML-KEM.KeyGen_internal(d,z)` (algorithm 16) using the first 32 octets as *d* and the remaining 32 octets as *z* and ensuring it is bytewise equal to the value presented in the private key.

Appendix C.4 includes some examples of inconsistent seeds and expanded private keys.

9. Security Considerations

The Security Considerations section of [RFC5280] applies to this specification as well.

Protection of the private key information, i.e., the seed, is vital to public key cryptography. Disclosure of the private key material to another entity can lead to masquerades.

The generation of private keys relies on random numbers. The use of inadequate pseudorandom number generators (PRNGs) to generate these values can result in little or no security. An attacker may find it much easier to reproduce the PRNG environment that produced the keys, searching the resulting small set of possibilities, rather than brute force searching the whole key space. The generation of quality random numbers is difficult. ML-KEM key generation has specific requirements around randomness generation as described in Section 3.3 of [FIPS203].

Many protocols only rely on the IND-CCA security of a KEM. Some (implicitly) require further binding properties, formalized in [CDM23]. The private key format influences these binding properties. Per [KEMMY24], ML-KEM is LEAK-BIND-K-PK-secure and LEAK-BIND-K-CT-secure when using the expanded private key format, but not MAL-BIND-K-CT nor MAL-BIND-K-PK secure. Using the 64-byte seed format provides a step up in binding security, and additionally provides MAL-BIND-K-CT security (but still does not provide security for MAL-BIND-K-PK).

For more detailed ML-KEM specific security considerations regarding this, randomness, misbinding properties, decapsulation failures, key reuse, and key checks, refer to [ML-KEM-SEC-CONS].

10. IANA Considerations

For the ASN.1 module in Appendix A, IANA has assigned an OID for the module identifier (121) with a description of "id-mod-x509-ml-kem-2025" in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

11. References

11.1. Normative References

[CSOR]

NIST, "Computer Security Objects Register (CSOR)", 13 June 2025, <https://csrc.nist.gov/projects/computer-security-objects-register/algorithm-registration>.

[FIPS203] NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard", NIST FIPS 203, DOI 10.6028/NIST.FIPS.203, August 2024, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <https://www.rfc-editor.org/info/rfc5958>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9629] Housley, R., Gray, J., and T. Okubo, "Using Key Encapsulation Mechanism (KEM) Algorithms in the Cryptographic Message Syntax (CMS)", RFC 9629, DOI 10.17487/RFC9629, August 2024, <https://www.rfc-editor.org/info/rfc9629>.

[X680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

[X690] ITU-T, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.690>.

11.2. Informative References

[CDM23] Cremers, C., Dax, A., and N. Medinger, "Keeping Up with the KEMs: Stronger Security Notions for KEMs and automated analysis of KEM-based protocols", Cryptology ePrint Archive, Paper 2023/1933, 2023, <https://eprint.iacr.org/2023/1933.pdf>.

[KEM-TLS] Wiggers, T., Celi, S., Schwabe, P., Stebila, D., and N. Sullivan, "KEM-based Authentication for TLS 1.3", Work in Progress, Internet-Draft, draft-celi-wiggers-tls-authkem-06, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-celi-wiggers-tls-authkem-06>.

[KEMMY24] Schmieg, S., "Unbindable Kemmy Schmidt: ML-KEM is neither MAL-BIND-K-CT nor MAL-BIND-K-PK", Cryptology ePrint Archive, Paper 2024/523, 2024, <https://eprint.iacr.org/2024/523.pdf>.

[ML-KEM-SEC-CONS] Fluhrer, S., Dang, Q., Mattsson, J. P., Milner, K., and D. Shiu, "ML-KEM Security Considerations", Work in Progress, Internet-Draft, draft-sfluhrer-cfrg-ml-kem-security-considerations-04, 17 November 2025, <https://datatracker.ietf.org/doc/html/draft-sfluhrer-cfrg-ml-kem-security-considerations-04>.

[NIST-PQC] NIST, "Post-Quantum Cryptography (PQC)", 28 July 2025, <https://csrc.nist.gov/projects/post-quantum-cryptography>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <https://www.rfc-editor.org/info/rfc7468>.

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

[RFC9936] Prat, J., Ounsworth, M., and D. Van Geest, "Use of ML-KEM in the Cryptographic Message Syntax (CMS)", RFC 9936, DOI 10.17487/RFC9936, February 2026, <https://www.rfc-editor.org/info/rfc9936>.

Appendix A. ASN.1 Module

This appendix includes the ASN.1 module [X680] for the ML-KEM. Note that as per [RFC5280], certificates use the Distinguished Encoding Rules; see [X690]. This module imports objects from [RFC5912] and [RFC9629].

```
<CODE BEGINS>
X509-ML-KEM-2025
{ iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-x509-ml-kem-2025(121) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS

 PUBLIC-KEY
```

```
   FROM AlgorithmInformation-2009  -- [RFC 5912]
     { iso(1) identified-organization(3) dod(6) internet(1)
       security(5) mechanisms(5) pkix(7) id-mod(0)
       id-mod-algorithmInformation-02(58) }

 KEM-ALGORITHM
   FROM KEMAlgorithmInformation-2023  -- [RFC 9629]
     { iso(1) identified-organization(3) dod(6) internet(1)
       security(5) mechanisms(5) pkix(7) id-mod(0)
       id-mod-kemAlgorithmInformation-2023(109) };

--
-- ML-KEM Identifiers
--

nistAlgorithms OBJECT IDENTIFIER ::= { joint-iso-ccitt(2)
  country(16) us(840) organization(1) gov(101) csor(3)
  nistAlgorithm(4) }

kems OBJECT IDENTIFIER ::= { nistAlgorithms 4 }

id-alg-ml-kem-512 OBJECT IDENTIFIER ::= { kems 1 }

id-alg-ml-kem-768 OBJECT IDENTIFIER ::= { kems 2 }

id-alg-ml-kem-1024 OBJECT IDENTIFIER ::= { kems 3 }

--
-- Public Key Algorithms
--

PublicKeys PUBLIC-KEY ::= {
  -- This expands PublicKeys from [RFC 5912]
  pk-ml-kem-512 |
  pk-ml-kem-768 |
  pk-ml-kem-1024,
  ...
  }

--
-- ML-KEM Public Keys
--

pk-ml-kem-512 PUBLIC-KEY ::= {
  IDENTIFIER id-alg-ml-kem-512
  -- KEY no ASN.1 wrapping; 800 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { keyEncipherment }
  PRIVATE-KEY ML-KEM-512-PrivateKey
  }

ML-KEM-512-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (64)),
  expandedKey OCTET STRING (SIZE (1632)),
  both SEQUENCE {
      seed OCTET STRING (SIZE (64)),
      expandedKey OCTET STRING (SIZE (1632))
      }
```

```
  }

pk-ml-kem-768 PUBLIC-KEY ::= {
  IDENTIFIER id-alg-ml-kem-768
  -- KEY no ASN.1 wrapping; 1184 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { keyEncipherment }
  PRIVATE-KEY ML-KEM-768-PrivateKey
  }

ML-KEM-768-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (64)),
  expandedKey OCTET STRING (SIZE (2400)),
  both SEQUENCE {
      seed OCTET STRING (SIZE (64)),
      expandedKey OCTET STRING (SIZE (2400))
      }
  }

pk-ml-kem-1024 PUBLIC-KEY ::= {
  IDENTIFIER id-alg-ml-kem-1024
  -- KEY no ASN.1 wrapping; 1568 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { keyEncipherment }
  PRIVATE-KEY ML-KEM-1024-PrivateKey
  }

ML-KEM-1024-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (64)),
  expandedKey OCTET STRING (SIZE (3168)),
  both SEQUENCE {
      seed OCTET STRING (SIZE (64)),
      expandedKey OCTET STRING (SIZE (3168))
      }
  }

ML-KEM-512-PublicKey ::= OCTET STRING (SIZE (800))

ML-KEM-768-PublicKey ::= OCTET STRING (SIZE (1184))

ML-KEM-1024-PublicKey ::= OCTET STRING (SIZE (1568))

END
<CODE ENDS>
```

Appendix B. Parameter Set Security and Sizes

Instead of defining the strength of a quantum algorithm in a typical manner using the imprecise notion of bits of security, NIST has defined security levels by picking a reference scheme, which is expected to offer notable levels of resistance to both quantum and classical attacks. To wit, a KEM algorithm that achieves NIST PQC security must require computational resources to break IND-CCA security comparable or greater than that required for key search on AES-128, AES-192, and AES-256 for Levels 1, 3, and 5, respectively. Levels 2 and 4 use collision search for SHA-256 and SHA-384 as reference.

Level	Parameter Set	Encap. Key	Decap. Key	Ciphertext	Secret
1	ML-KEM-512	800	1632	768	32
3	ML-KEM-768	1184	2400	1088	32
5	ML-KEM-1024	1568	3168	1568	32

Table 1: Mapping Between NIST Security Level, ML-KEM Parameter Sets, and Sizes in Bytes

Appendix C. Examples

This appendix contains examples of ML-KEM public keys, private keys, certificates, and inconsistent seed and expanded private keys.

C.1. Example Private Keys

The following examples show ML-KEM private keys in different formats, all derived from the same seed `000102...1e1f`. For each security level, we show the seed-only format (using a context-specific `[0]` primitive tag with an implicit encoding of `OCTET STRING`), the expanded format, and both formats together.

> NOTE: All examples use the same seed value, showing how the same seed produces different expanded private keys for each security level.

C.1.1. ML-KEM-512 Private Key Examples

Each of the examples includes the textual encoding [RFC7468] followed by the so-called "pretty print"; the private keys are the same.

C.1.1.1. Seed Format

```
-----BEGIN PRIVATE KEY-----
MFQCAQAwCwYJYIZIAWUDBAQBBEKAQAABAgMEBQYHCAkKCwwNDg8QERITFBUWFxgZ
GhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9Pj8=
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.1 }
  }
  OCTET_STRING {
    [0 PRIMITIVE] { `000102030405060708090a0b0c0d0e0f10111213141
5161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f30313233343
5363738393a3b3c3d3e3f` }
  }
}
```

C.1.1.2. Expanded Format

```
-----BEGIN PRIVATE KEY-----
MIIGeAIBADALBglghkgBZQMEBAEEggZkBIIGYHBVT9Q2NE8nhbGzsbrBhLZnkAMz
bCbxWn3oeMSCXGvgPzxKSA91t0hqrTHToAUYYj/SB6tSjdYnIUlYNa4AYsNnt0px
uvEKrQ6KKQIHa+MTSL6xXMwJV83rtK/yJnVrvGAbZWireErLrrNHAvD4aiYgIRiy
KyP4NVh3bHnBTbqYM3nIA+DcwxYKEXVwMOacaRl5jYHraYqaRIOpnlpcssMcmmYX
mfPMiceQcG6gQWKQRdQqg67YiGDjlMaRh+IQXSjMFOw5NZLWfdAKpD/otOrkQUAC
hmtccTxqjX0Wz3i4GdbxLp5adCM5CPCxXjxLqDKcXN2lXISSjjqoBj5aqWdkA/kX
NbEQEMf1kwkTZNyGRFvIBIQKmiFyQhJGn4p7DOCsaY64bK05p/SCTZpRY6rCHuaA
iwU8ij+ssLZ0S1Jiu8smpD9mTIcytkz8es8JlgX0HHlgYJdqxDODP+ADQ/sYKDAK
QkdBEW5LRbsnbqgRKaDbTG5gvOYREB6MYlR0kl4CImeTCKPncI0Zcqe0I+sjKFHD
bS7VPT7Tu3UAY3BhpdwikvocRmwHNUaDMovsLB7Sy1yZt47KCWkDjPfDTdEYck4x
yuCGIGs0MCtSD10Xet7Vs8zgKszoCOomvMByYl/bk/F0WKX8HU2jlDgKH1fpzGYQ
lDigdfDSgT/MShmcx22zgj8nCwBhWUGSlAQRo3/7r64sFQFlzsXGv3PFlfuSzRUx
JgfaBwd4ZSvZlEvEi8fRpTQzi60LrWZWxdUCznhQqxWHJE7rWPQ5q14IV0pxjIqs
PXfHmLuhVCczvnNEjyP7cMDlNTonyIMixSGEk6+7OAhkNNbWCla6iH3UmMOrJqCH
CZOBWqakCXXyGK3KFYLWT/yGUvuzqab7wwT5GUX6Sq7yh4/XFd9wET0jefRIhvgS
yD/ytxmmnh7HSuSxWszTrtWlPOdqewmCRxYzuXPLQKGgAV0KQk+hGkecAjAXQ20q
KQDpk+taCgZ0AMf0qt8gH8T6MSZKY7rpXMjWXDmVgV5ZfRBDVc8pqlMzyTJRhp1b
zb5IcST2Ari2pmwWxHYWSK12XPXYAGtRXpBafwrAdrDGLvoygVPnylcBaZ8TBfHm
vG+QsOSbaTUSts6ZKouAFt38GmYsfj+WGcvYad13GvMIlszVkYrGy3dGbF53mZbW
f/mqvJdQPyx7fi0ADYZFD7GAfKTKvaRlgloxx4mht6SRqzhydl0yDQtxkg+iE8lA
k0Frg7gSTmn2XmLLUADcw3qpoP/3OXDEdy81fSQYnKb1MFVowOI3ajdipoxgXlY8
XSCVcuD8dTLKKUcpU1VntfxBPF6HktJGRTbMgI+YrddGZPFBVm+QFqkKVBgpqYoE
ZM5BqLtEwtT6PCwglGByjvFKGnxMm5jRIgO0zDUpFgqasteDj3/2tTrgWqMafWRr
evpsRZMlJqPDdVYZvplMIRwqMcBbNEeDbLIVC+GCna5rBMVTXP9Ubjkrp5dBFyD5
JPSQpaxUlfITVtVQt4KmTBaItrZVvMeEIZekNML2Vjtbfwmni8xIgjJ4NWHRb0y6
tnVUAAUHgVcMZmBLgXrRJSKUc26LAYYaS1p0UZuLb+UUiaUHI5Llh2JscTd2V10z
gGocjicyr5fCaA9RZmMxxOuLvAQxxPloMtrxs8RVKPuhU/bHixwZhwKUfM0zdyek
b7U7oR3ly0GRNGhZUWy2rXJADzzyCbI2rvNaWArIfrPjD6/WaXPKin3SZ1r0H3oX
thQzzRr4D3cIhp9mVIhJeYCxrBCgzctjagDthoGzXkKRJMqANQcluF+DperDpKPM
FgCQPmUpNWC5szblrw1SnawaBIEZMCy3qbzBELlIUb8CEX8ZncSFqFK3Rz8JuDGm
gx1bVMC3kNIlz2u5LZRiomzbM92lEjx6rw4moLg2Ve6ii/OoB0clAY/WuuS2Ac9h
uqtxp6PTUZejQ+dLSicsEl1UCJZCbYW3lY07OKa6mH7DciXHtEzbEt3kU5tKsII2
NoPwS/egnMXEHf6DChsWLgsyQzQ2LwhKFEZ3IzRLrdAA+NjFN8SPmY8FMHzr0e3g
uBw7xZoGWhttY7JsgvEB/2SAY7N24rtsW3RV9lWlDC/q2t4VDvoODm82WuogISIj
JCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+Pw==
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.1 }
  }
  OCTET_STRING {
    OCTET_STRING { `70554fd436344f2785b1b3b1bac184b6679003336c26
f15a7de878c4825c6be03f3c4a480f75b7486aad31d3a00518623fd207ab528d
d62721495835ae0062c367b74a71baf10aad0e8a2902076be31348beb15ccc09
57cdebb4aff226756bbc601b6568ab784acbaeb34702f0f86a26202118b22b23
f83558776c79c14dba983379c803e0dcc3160a11757030e69c6919798d81eb69
8a9a4483a99e5a5cb2c31c9a661799f3cc89c790706ea041629045d42a83aed8
8860e394c69187e2105d28cc14ec393592d67dd00aa43fe8b4eae4414002866b
5c713c6a8d7d16cf78b819d6f12e9e5a74233908f0b15e3c4ba8329c5cdda55c
84928e3aa8063e5aa9676403f91735b11010c7f593091364dc86445bc804840a
9a21724212469f8a7b0ce0ac698eb86cad39a7f4824d9a5163aac21ee6808b05
3c8a3facb0b6744b5262bbcb26a43f664c8732b64cfc7acf099605f41c796060
976ac433833fe00343fb1828300a424741116e4b45bb276ea81129a0db4c6e60
bce611101e8c625474925e0222679308a3e7708d1972a7b423eb232851c36d2e
d53d3ed3bb7500637061a5dc2292fa1c466c07354683328bec2c1ed2cb5c99b7
8eca0969038cf7c34dd118724e31cae086206b34302b520f5d177aded5b3cce0
2acce808ea26bcc072625fdb93f17458a5fc1d4da394380a1f57e9cc66109438
a075f0d2813fcc4a199cc76db3823f270b0061594192940411a37ffbafae2c15
0165cec5c6bf73c595fb92cd15312607da070778652bd9944bc48bc7d1a53433
8bad0bad6656c5d502ce7850ab1587244eeb58f439ab5e08574a718c8aac3d77
c798bba1542733be73448f23fb70c0e5353a27c88322c5218493afbb38086434
d6d60a56ba887dd498c3ab26a0870993815aa6a40975f218adca1582d64ffc86
52fbb3a9a6fbc304f91945fa4aaef2878fd715df70113d2379f44886f812c83f
f2b719a69e1ec74ae4b15accd3aed5a53ce76a7b0982471633b973cb40a1a001
5d0a424fa11a479c023017436d2a2900e993eb5a0a067400c7f4aadf201fc4fa
31264a63bae95cc8d65c3995815e597d104355cf29aa5333c93251869d5bcdbe
487124f602b8b6a66c16c4761648ad765cf5d8006b515e905a7f0ac076b0c62e
fa328153e7ca5701699f1305f1e6bc6f90b0e49b693512b6ce992a8b8016ddfc
1a662c7e3f9619cbd869dd771af30896ccd5918ac6cb77466c5e779996d67ff9
aabc97503f2c7b7e2d000d86450fb1807ca4cabda465825a31c789a1b7a491ab
3872765d320d0b71920fa213c94093416b83b8124e69f65e62cb5000dcc37aa9
a0fff73970c4772f357d24189ca6f5305568c0e2376a3762a68c605e563c5d20
9572e0fc7532ca294729535567b5fc413c5e8792d2464536cc808f98add74664
f141566f9016a90a541829a98a0464ce41a8bb44c2d4fa3c2c209460728ef14a
1a7c4c9b98d12203b4cc3529160a9ab2d7838f7ff6b53ae05aa31a7d646b7afa
6c45932526a3c3755619be994c211c2a31c05b3447836cb2150be1829dae6b04
c5535cff546e392ba797411720f924f490a5ac5495f21356d550b782a64c1688
b6b655bcc7842197a434c2f6563b5b7f09a78bcc488232783561d16f4cbab675
5400050781570c66604b817ad1252294736e8b01861a4b5a74519b8b6fe51489
a5072392e587626c713776575d33806a1c8e2732af97c2680f51666331c4eb8b
bc0431c4f96832daf1b3c45528fba153f6c78b1c198702947ccd337727a46fb5
3ba11de5cb4191346859516cb6ad72400f3cf209b236aef35a580ac87eb3e30f
afd66973ca8a7dd2675af41f7a17b61433cd1af80f7708869f665488497980b1
ac10a0cdcb636a00ed8681b35e429124ca80350725b85f83a5eac3a4a3cc1600
903e65293560b9b336e5af0d529dac1a048119302cb7a9bcc110b94851bf0211
7f199dc485a852b7473f09b831a6831d5b54c0b790d225cf6bb92d9462a26cdb
33dda5123c7aaf0e26a0b83655eea28bf3a8074725018fd6bae4b601cf61baab
71a7a3d35197a343e74b4a272c125d540896426d85b7958d3b38a6ba987ec372
25c7b44cdb12dde4539b4ab082363683f04bf7a09cc5c41dfe830a1b162e0b32
4334362f084a14467723344badd000f8d8c537c48f998f05307cebd1ede0b81c
3bc59a065a1b6d63b26c82f101ff648063b376e2bb6c5b7455f655a50c2feada
de150efa0e0e6f365aea2021222324252627282 92a2b2c2d2e2f303132333435
```

```
363738393a3b3c3d3e3f` }
  }
}
```

C.1.1.3. Both Format

```
-----BEGIN PRIVATE KEY-----
MIIGvgIBADALBglghkgBZQMEBAEEggaqMIIGpgRAAAECAwQFBgcICQoLDA0ODxAR
EhMUFRYXGBkaGxwdHh8gISIjJCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+PwSC
BmBwVU/UNjRPJ4Wxs7G6wYS2Z5ADM2wm8Vp96HjEglxr4D88SkgPdbdIaq0x06AF
GGI/0gerUo3WJyFJWDWuAGLDZ7dKcbrxCq0OiikCB2vjE0i+sVzMCVfN67Sv8iZ1
a7xgG2Voq3hKy66zRwLw+GomICEYsisj+DVYd2x5wU26mDN5yAPg3MMWChF1cDDm
nGkZeY2B62mKmkSDqZ5aXLLDHJpmF5nzzInHkHBuoEFikEXUKoOu2Ihg45TGkYfi
EF0ozBTsOTWS1n3QCqQ/6LTq5EFAAoZrXHE8ao19Fs94uBnW8S6eWnQjOQjwsV48
S6gynFzdpVyEko46qAY+WqlnZAP5FzWxEBDH9ZMJE2TchkRbyASECpohckISRp+K
ewzgrGmOuGytOaf0gk2aUWOqwh7mgIsFPIo/rLC2dEtSYrvLJqQ/ZkyHMrZM/HrP
CZYF9Bx5YGCXasQzgz/gA0P7GCgwCkJHQRFuS0W7J26oESmg20xuYLzmERAejGJU
dJJeAiJnkwij53CNGXKntCPrIyhRw20u1T0+07t1AGNwYaXcIpL6HEZsBzVGgzKL
7Cwe0stcmbeOyglpA4z3w03RGHJOMcrghiBrNDArUg9dF3re1bPM4CrM6AjqJrzA
cmJf25PxdFil/B1No5Q4Ch9X6cxmEJQ4oHXw0oE/zEoZnMdts4I/JwsAYVlBkpQE
EaN/+6+uLBUBZc7Fxr9zxZX7ks0VMSYH2gcHeGUr2ZRLxIvH0aU0M4utC61mVsXV
As54UKsVhyRO61j0OateCFdKcYyKrD13x5i7oVQnM75zRI8j+3DA5TU6J8iDIsUh
hJOvuzgIZDTW1gpWuoh91JjDqyaghwmTgVqmpAl18hityhWC1k/8hlL7s6mm+8ME
+RlF+kqu8oeP1xXfcBE9I3n0SIb4Esg/8rcZpp4ex0rksVrM067VpTznansJgkcW
M7lzy0ChoAFdCkJPoRpHnAIwF0NtKikA6ZPrWgoGdADH9KrfIB/E+jEmSmO66VzI
1lw5lYFeWX0QQ1XPKapTM8kyUYadW82+SHEk9gK4tqZsFsR2Fkitdlz12ABrUV6Q
Wn8KwHawxi76MoFT58pXAWmfEwXx5rxvkLDkm2k1ErbOmSqLgBbd/BpmLH4/lhnL
2GnddxrzCJbM1ZGKxst3Rmxed5mW1n/5qryXUD8se34tAA2GRQ+xgHykyr2kZYJa
MceJobekkas4cnZdMg0LcZIPohPJQJNBa4O4Ek5p9l5iy1AA3MN6qaD/9zlwxHcv
NX0kGJym9TBVaMDiN2o3YqaMYF5WPF0glXLg/HUyyilHKVNVZ7X8QTxeh5LSRkU2
zICPmK3XRmTxQVZvkBapClQYKamKBGTOQai7RMLU+jwsIJRgco7xShp8TJuY0SID
tMw1KRYKmrLXg49/9rU64FqjGn1ka3r6bEWTJSajw3VWGb6ZTCEcKjHAWzRHg2yy
FQvhgp2uawTFU1z/VG45K6eXQRcg+ST0kKWsVJXyE1bVULeCpkwWiLa2VbzHhCGX
pDTC9lY7W38Jp4vMSIIyeDVh0W9MurZ1VAAFB4FXDGZgS4F60SUilHNuiwGGGkta
dFGbi2/lFImlByOS5YdibHE3dlddM4BqHI4nMq+XwmgPUWZjMcTri7wEMcT5aDLa
8bPEVSj7oVP2x4scGYcClHzNM3cnpG+1O6Ed5ctBkTRoWVFstq1yQA888gmyNq7z
WlgKyH6z4w+v1mlzyop90mda9B96F7YUM80a+A93CIafZlSISXmAsawQoM3LY2oA
7YaBs15CkSTKgDUHJbhfg6Xqw6SjzBYAkD5lKTVgubM25a8NUp2sGgSBGTAst6m8
wRC5SFG/AhF/GZ3EhahSt0c/CbgxpoMdW1TAt5DSJc9ruS2UYqJs2zPdpRI8eq8O
JqC4NlXuoovzqAdHJQGP1rrktgHPYbqrcaej01GXo0PnS0onLBJdVAiWQm2Ft5WN
Ozimuph+w3Ilx7RM2xLd5FObSrCCNjaD8Ev3oJzFxB3+gwobFi4LMkM0Ni8IShRG
dyM0S63QAPjYxTfEj5mPBTB869Ht4LgcO8WaBlobbWOybILxAf9kgGOzduK7bFt0
VfZVpQwv6treFQ76Dg5vNlrqICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9
Pj8=
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.1 }
  }
  OCTET_STRING {
    SEQUENCE {
      OCTET_STRING { `000102030405060708090a0b0c0d0e0f1011121314
15161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334
35363738393a3b3c3d3e3f` }
      OCTET_STRING { `70554fd436344f2785b1b3b1bac184b6679003336c
26f15a7de878c4825c6be03f3c4a480f75b7486aad31d3a00518623fd207ab52
8dd62721495835ae0062c367b74a71baf10aad0e8a2902076be31348beb15ccc
0957cdebb4aff226756bbc601b6568ab784acbaeb34702f0f86a26202118b22b
23f83558776c79c14dba983379c803e0dcc3160a11757030e69c6919798d81eb
698a9a4483a99e5a5cb2c31c9a661799f3cc89c790706ea041629045d42a83ae
d88860e394c69187e2105d28cc14ec393592d67dd00aa43fe8b4eae441400286
6b5c713c6a8d7d16cf78b819d6f12e9e5a74233908f0b15e3c4ba8329c5cdda5
5c84928e3aa8063e5aa9676403f91735b11010c7f593091364dc86445bc80484
0a9a21724212469f8a7b0ce0ac698eb86cad39a7f4824d9a5163aac21ee6808b
053c8a3facb0b6744b5262bbcb26a43f664c8732b64cfc7acf099605f41c7960
60976ac433833fe00343fb1828300a424741116e4b45bb276ea81129a0db4c6e
60bce611101e8c625474925e0222679308a3e7708d1972a7b423eb232851c36d
2ed53d3ed3bb7500637061a5dc2292fa1c466c07354683328bec2c1ed2cb5c99
b78eca0969038cf7c34dd118724e31cae086206b34302b520f5d177aded5b3cc
e02acce808ea26bcc072625fdb93f17458a5fc1d4da394380a1f57e9cc661094
38a075f0d2813fcc4a199cc76db3823f270b0061594192940411a37ffbafae2c
150165cec5c6bf73c595fb92cd15312607da070778652bd9944bc48bc7d1a534
338bad0bad6656c5d502ce7850ab1587244eeb58f439ab5e08574a718c8aac3d
77c798bba1542733be73448f23fb70c0e5353a27c88322c5218493afbb380864
34d6d60a56ba887dd498c3ab26a0870993815aa6a40975f218adca1582d64ffc
8652fbb3a9a6fbc304f91945fa4aaef2878fd715df70113d2379f44886f812c8
3ff2b719a69e1ec74ae4b15accd3aed5a53ce76a7b0982471633b973cb40a1a0
015d0a424fa11a479c023017436d2a2900e993eb5a0a067400c7f4aadf201fc4
fa31264a63bae95cc8d65c3995815e597d104355cf29aa5333c93251869d5bcd
be487124f602b8b6a66c16c4761648ad765cf5d8006b515e905a7f0ac076b0c6
2efa328153e7ca5701699f1305f1e6bc6f90b0e49b693512b6ce992a8b8016dd
fc1a662c7e3f9619cbd869dd771af30896ccd5918ac6cb77466c5e779996d67f
f9aabc97503f2c7b7e2d000d86450fb1807ca4cabda465825a31c789a1b7a491
ab3872765d320d0b71920fa213c94093416b83b8124e69f65e62cb5000dcc37a
a9a0fff73970c4772f357d24189ca6f5305568c0e2376a3762a68c605e563c5d
209572e0fc7532ca294729535567b5fc413c5e8792d2464536cc808f98add746
64f141566f9016a90a541829a98a0464ce41a8bb44c2d4fa3c2c209460728ef1
4a1a7c4c9b98d12203b4cc3529160a9ab2d7838f7ff6b53ae05aa31a7d646b7a
fa6c45932526a3c3755619be994c211c2a31c05b3447836cb2150be1829dae6b
04c5535cff546e392ba797411720f924f490a5ac5495f21356d550b782a64c16
88b6b655bcc7842197a434c2f6563b5b7f09a78bcc488232783561d16f4cbab6
755400050781570c66604b817ad1252294736e8b01861a4b5a74519b8b6fe514
89a5072392e587626c713776575d33806a1c8e2732af97c2680f51666331c4eb
8bbc0431c4f96832daf1b3c45528fba153f6c78b1c198702947ccd337727a46f
b53ba11de5cb4191346859516cb6ad72400f3cf209b236aef35a580ac87eb3e3
0fafd66973ca8a7dd2675af41f7a17b61433cd1af80f7708869f665488497980
b1ac10a0cdcb636a00ed8681b35e429124ca80350725b85f83a5eac3a4a3cc16
00903e65293560b9b336e5af0d529dac1a048119302cb7a9bcc110b94851bf02
117f199dc485a852b7473f09b831a6831d5b54c0b790d225cf6bb92d9462a26c
db33dda5123c7aaf0e26a0b83655eea28bf3a8074725018fd6bae4b601cf61ba
ab71a7a3d35197a343e74b4a272c125d540896426d85b7958d3b38a6ba987ec3
```

```
7225c7b44cdb12dde4539b4ab082363683f04bf7a09cc5c41dfe830a1b162e0b
324334362f084a14467723344badd000f8d8c537c48f998f05307cebd1ede0b8
1c3bc59a065a1b6d63b26c82f101ff648063b376e2bb6c5b7455f655a50c2fea
dade150efa0e0e6f365aea20212223242526272829 2a2b2c2d2e2f3031323334
35363738393a3b3c3d3e3f` }
    }
  }
}
```

C.1.2. ML-KEM-768 Private Key Examples

Each of the examples includes the textual encoding [RFC7468] followed by the so-called "pretty print"; the private keys are the same.

C.1.2.1. Seed Format

```
-----BEGIN PRIVATE KEY-----
MFQCAQAwCwYJYIZIAWUDBAQCBEKAQAABAgMEBQYHCAkKCwwNDg8QERITFBUWFxgZ
GhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9Pj8=
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.2 }
  }
  OCTET_STRING {
    [0 PRIMITIVE] { `000102030405060708090a0b0c0d0e0f10111213141
5161718191a1b1c1d1e1f20212223242526272829 2a2b2c2d2e2f30313233343
5363738393a3b3c3d3e3f` }
  }
}
```

C.1.2.2. Expanded Format

```
-----BEGIN PRIVATE KEY-----
MIIJeAIBADALBglghkgBZQMEBAIEgglkBIIJYCfSp38zdW9hII7xE6voJZWHPUq8
cw5bXWeVKb9qTOtjg0JyMahhL0FVBRWsulLkjq2LlCgzu+aGXRPRSnnSxcPgfwoF
bY3nqt/KugWMSTyAs3yrjFYnU7s7prbsgpf4heqnVA1TABWoRAblWxNmtXfiNs5Y
om2KHrWkTVQjI8IWfZv0pH+YVpnKBbrkO43sYX8COAo4kK/UuMfsft4mVToCXzzl
vF16YhMDBCNcsa1INrVmtbhjvZvbRaKESnBHtsjTg+RIUl4EC03IorSMbDfJbWLU
Pz/YjiiBxAogXJ4kj2UrWSeBp3n4aIDyoUe2eGPzkcwaWpCMAJXgchIpHi74o265
qcDGBzIls0cDpK8Ek4LEdXPaaP3pJFrUROMbH721IfH2Hze8DO8pIGfmcNKKH/2Q
T28RkKmWkYoTA3psq/PDc7+Cls03qzO6d0aAnMP4reGzY5vVe/zGllCqrx3hmPxM
BGMpnlLEYXgMxCj8XQSlxRhQy6bCpSdDQGdXk92gm+RMKeY5XGX4XSoKfG30EeaR
Gx8stsNRzS6HX1G2OL53YJfpPi8rL4PaC+70qoW6nnY6tkUCoMpSIunqtbO3CI7V
IGDoyCablDpxqwrhxbG2h9LgGc+ANrz5v257rDqqNuQWYPqkVA8mSM2ToYnsXC3q
cLrKqk/8kG+QgQ6htnvyTyx4z2uogarqYcBlK/+VsbrkQm0Xc7nMLKgsIeOMY247
HFIyRJhrC+ioP13Vzy1Udi+zxev1m46IUwKxzkcDPt92D04Cm+QLbVZrGd11is1c
dBKHgTEkT5AXLFPyZmPCHZBTAdSLr5HJF8x3eenYgCzBDYmjcFCZoq06OoiWdDwR
RGmAk74lfay2bceFIouRLI2WXRSqKDQsOsSpP++lMrIJRd3BAgE5wU1ji5CMTd3p
oGRblbLkQU1Au3nwRBODDxWoc8KLtwWcJ0EAIBXyBAjwWOcVsL+ZW1OAt90yWgVq
uX5lmivgzfbDNzHGg6Y0t3HoySoTmu5LsOSccHcyHUL8GZ98HymMpiXSI6XCY6A8
xIFZt4EmZbeGN+ThhyCywpprmfQnZqTLxNxQi6lLqDuJw6XHj4uya72beb64yBgk
kPV5PuW5YBO3S34WninRYvExVGTqfXJDbYm3VRYRksgcwt0ci4u6eV70Ju4cwBw3
qqN7LP+LCjeLR8vQtNSTmM/CcSlZaZ+gvYzYRmasxh9UG4T6lrnIVOTnXpFErdtE
uFZqV9+7VFzkI8AzRvKywakXgNFSqN4aTUycrN5zksmWiIzCOZwCw4szU634rKso
OSTaAKBbduc4xyyTDWy6Ca4WiZD6of7yIm54CGHUFu/0AvT3WfxkirH5cQAQkIf5
bksUjSyzHkgFMU6gzZX7Aj6sDZiUdLpCAde0HSb1OUshfupbNLcaizeTHA5ZQnHg
t8czJXJAIz57pzVgPkJah97ncHnjfLKKIXZFlM5TUNjaK2KgcXSUMDLsicmICcc7
ZCPTDB0oOnZqZNiXA8PWKbSXgo1IMgw0YhB5eimKoQ1CPI3aBp0CvFnmzfA6CWuL
PaTKubgMpKFJB2cszvHsT68jSgvFt+nUc/KzEzs7JqHRdctnp4BZGWmcAvdlMbmc
X4kYBwS7TKRTXFuJcmecZgoHxeUUuHAJyGLrj1FXaV77P8QKne9rgcHMAqJJrk8J
StDZvTSFwcHGgIBSCnyMYyAyzuc4FU5cUXbAfaVgJHdqQw/nbqz2ZaP3uDIQIhW8
gvEJOcg1VwQzao+sHYHkuwSFql18dNa1m75cXpcqDYusQRtVtdVVfNaAoaj3G064
a8SMmgUJcxpUvZ1ykLJ5Y+Q3Lcmxmc/crAsBrNKKYjlREuTENkjWIsSMgjTQFEDo
zDdskn8jpa/JrAR0xmInTkJFJchVLs47P+JlFt6QG8fVFb3olVjmJslcgLkzQvgB
AATznmxslIccXjRMqzlmyDX5qWpZr9McQChrOLHBp4RwurlHUYk0RTzoZzapGfH1
ptUQqG9UVPw5gMtcdlvSvV97NrFBDWY1yM60fE3aDXaijqyTnHHDAkgEhmxxYmZY
RCFjwsIhF+UKzvzmN4qYVlIwKk7wws4Mxxa3eW4ray43d9+hrD2iWaMbWptTD4y2
OKgaYqwwGEmrr5WnMBvaMAaJCb/bfmfbzLs4pVUaJbGjoPaFdIrVdT2IgPABbGJ0
hhZjhMVXH+I2WQA2TQODEeLYdds2ZoaTK17GAkMKNp6Hpu9cM4eGZXglvUwFes65
I+sJNeaQXmO0ztf4CFenc91ksVDSZhLqmsEgUtsgF78YQ8y0sygbaQ3HKK36hcAC
gbjjwJKHM1+Fa0/CiS9povV5Ia2gGRTECYhmLVd2lmKnhjUbm2ZJPat5WU2YbeIQ
DWW6D/TqWLgVONJKRDWiWPrCVASqf0H2WLE4UGXhWNy2ARVzJyD0BFmqrBXkBpU6
kKxSmX0czQcAYO/GXbnmUzVEZ/rVbscTyG51QMQjrPJmn1L6b0rGiI2HHvPoR8Ap
qKr7uS4XskqgebH0GbphdbRCr7EZCdSla3CgM1soc5IYqnyTSOLDwvPrPRWkHmQX
wN2Uv+shQZsxGnuxOhgLvoMyGKmmsXRHzIXyJYWVh6cwdwSay8/UTQ8CVDjhXRU4
Jw1Ybhv4MZKpRZz2PA6XL4UpdnmDHs8SFQmFHLg0D28Qew+hoO/Rs2qBibwIXE9c
t4TlU/QbkY+AOXzhlW94W+43fKmqi+aZitowwmt8PYxrVSVMyWIDsgxCruCsTh67
QI5JqeP4edCrB4XrcCVCXRMFoimcAV4SDRY7DhlJTOVyU9AkbRgnRcuBl6t0OLPB
u3lyvsWjBuujVnhVwBRpn+9lrlTHcKDYXBhADPZCrtxmB3e6SxOFAr1aeBL2IfhK
SClrmN1DIrbxWCi4qPDgCoukSlPDqLFDVxsHQKvVZ9rxzenHnCBLbV4lnRdmoxu7
y05qBc9FAhdrMBwcL0Ekd1AVe87IXoCbMKTWDXdHzdD1uZqoyCaYdRd5OqqAgKCx
JKhVjfcrvje3X07btr6CFtbGM/srIoDiURPYaV5DSBw+6zl+sZJQUim2eiAeqJPD
4ssy2ovDQvpN6gV4ok4W2Pj5ODqVt3BQ9Nn9L1cz7sHWPvPCPr+ZGBc2aacgISIj
JCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+Pw==
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.2 }
  }
  OCTET_STRING {
    OCTET_STRING { `27d2a77f33756f61208ef113abe82595873d4abc730e
5b5d679529bf6a4ceb6383427231a8612f41550515acba52e48ead8b942833bb
e6865d13d14a79d2c5c3e07f0a056d8de7aadfcaba058c493c80b37cab8c5627
53bb3ba6b6ec8297f885eaa7540d530015a84406e55b1366b577e236ce58a26d
8a1eb5a44d542323c2167d9bf4a47f985699ca05bae43b8dec617f02380a3890
afd4b8c7ec7ede26553a025f3ce5bc5d7a62130304235cb1ad4836b566b5b863
bd9bdb45a2844a7047b6c8d383e448525e040b4dc8a2b48c6c37c96d62d43f3f
d88e2881c40a205c9e248f652b592781a779f86880f2a147b67863f391cc1a5a
908c0095e07212291e2ef8a36eb9a9c0c6073225b34703a4af049382c47573da
68fde9245ad444e31b1fbdb521f1f61f37bc0cef292067e670d28a1ffd904f6f
1190a996918a13037a6cabf3c373bf8296cd37ab33ba7746809cc3f8ade1b363
9bd57bfcc69650aaaf1de198fc4c0463299e52c461780cc428fc5d04a5c51850
cba6c2a5274340675793dda09be44c29e6395c65f85d2a0a7c6df411e6911b1f
2cb6c351cd2e875f51b638be776097e93e2f2b2f83da0beef4aa85ba9e763ab6
4502a0ca5222e9eab5b3b7088ed52060e8c8269b943a71ab0ae1c5b1b687d2e0
19cf8036bcf9bf6e7bac3aaa36e41660faa4540f2648cd93a189ec5c2dea70ba
caaa4ffc906f90810ea1b67bf24f2c78cf6ba881aaea61c0652bff95b1bae442
6d1773b9cc2ca82c21e38c636e3b1c523244986b0be8a83f5dd5cf2d54762fb3
c5ebf59b8e885302b1ce47033edf760f4e029be40b6d566b19dd758acd5c7412
878131244f90172c53f26663c21d905301d48baf91c917cc7779e9d8802cc10d
89a3705099a2ad3a3a8896743c1144698093be257dacb66dc785228b912c8d96
5d14aa28342c3ac4a93fefa532b20945ddc1020139c14d638b908c4ddde9a064
5b95b2e4414d40bb79f04413830f15a873c28bb7059c2741002015f20408f058
e715b0bf995b5380b7dd325a056ab97e659a2be0cdf6c33731c683a634b771e8
c92a139aee4bb0e49c7077321d42fc199f7c1f298ca625d223a5c263a03cc481
59b7812665b78637e4e18720b2c29a6b99f42766a4cbc4dc508ba94ba83b89c3
a5c78f8bb26bbd9b79beb8c8182490f5793ee5b96013b74b7e169e29d162f131
5464ea7d72436d89b755161192c81cc2dd1c8b8bba795ef426ee1cc01c37aaa3
7b2cff8b0a378b47cbd0b4d49398cfc2712959699fa0bd8cd84666acc61f541b
84fa96b9c854e4e75e9144addb44b8566a57dfbb545ce423c03346f2b2c1a917
80d152a8de1a4d4c9cacde7392c996888cc2399c02c38b3353adf8acab283924
da00a05b76e738c72c930d6cba09ae168990faa1fef2226e780861d416eff402
f4f759fc648ab1f97100109087f96e4b148d2cb31e4805314ea0cd95fb023eac
0d989474ba4201d7b41d26f5394b217eea5b34b71a8b37931c0e594271e0b7c7
33257240233e7ba735603e425a87dee77079e37cb28a21764594ce5350d8da2b
62a07174943032ec89c98809c73b6423d30c1d283a766a64d89703c3d629b497
828d48320c346210797a298aa10d423c8dda069d02bc59e6cdf03a096b8b3da4
cab9b80ca4a14907672ccef1ec4faf234a0bc5b7e9d473f2b3133b3b26a1d175
cb67a7805919699c02f76531b99c5f89180704bb4ca4535c5b8972679c660a07
c5e514b87009c862eb8f5157695efb3fc40a9def6b81c1cc02a249ae4f094ad0
d9bd3485c1c1c68080520a7c8c632032cee738154e5c5176c07da56024776a43
0fe76eacf665a3f7b832102215bc82f10939c8355704336a8fac1d81e4bb0485
aa5d7c74d6b59bbe5c5e972a0d8bac411b55b5d5557cd680a1a8f71b4eb86bc4
8c9a0509731a54bd9d7290b27963e4372dc9b199cfdcac0b01acd28a62395112
e4c43648d622c48c8234d01440e8cc376c927f23a5afc9ac0474c662274e4245
25c8552ece3b3fe26516de901bc7d515bde89558e626c95c80b93342f8010004
f39e6c6c94871c5e344cab3966c835f9a96a59afd31c40286b38b1c1a78470ba
b947518934453ce86736a919f1f5a6d510a86f5454fc3980cb5c765bd2bd5f7b
36b1410d6635c8ceb47c4dda0d76a28eac939c71c3024804866c716266584421
63c2c22117e50acefce6378a985652302a4ef0c2ce0cc716b7796e2b6b2e3777
dfa1ac3da259a31b5a9b530f8cb638a81a62ac301849abaf95a7301bda300689
```

```
09bfdb7e67dbccbb38a5551a25b1a3a0f685748ad5753d8880f0016c62748616
6384c5571fe2365900364d038311e2d875db366686932b5ec602430a369e87a6
ef5c338786657825bd4c057aceb923eb0935e6905e63b4ced7f80857a773dd64
b150d26612ea9ac12052db2017bf1843ccb4b3281b690dc728adfa85c00281b8
e3c09287335f856b4fc2892f69a2f57921ada01914c40988662d57769662a786
351b9b66493dab79594d986de2100d65ba0ff4ea58b81538d24a4435a258fac2
5404aa7f41f658b1385065e158dcb60115732720f40459aaac15e406953a90ac
52997d1ccd070060efc65db9e653354467fad56ec713c86e7540c423acf2669f
52fa6f4ac6888d871ef3e847c029a8aafbb92e17b24aa079b1f419ba6175b442
afb11909d4a56b70a0335b28739218aa7c9348e2c3c2f3eb3d15a41e6417c0dd
94bfeb21419b311a7bb13a180bbe833218a9a6b17447cc85f225859587a73077
049acbcfd44d0f025438e15d1538270d586e1bf83192a9459cf63c0e972f8529
7679831ecf121509851cb8340f6f107b0fa1a0efd1b36a8189bc085c4f5cb784
e553f41b918f80397ce1956f785bee377ca9aa8be6998ada30c26b7c3d8c6b55
254cc96203b20c42aee0ac4e1ebb408e49a9e3f879d0ab0785eb7025425d1305
a2299c015e120d163b0e19494ce57253d0246d182745cb8197ab7438b3c1bb79
72bec5a306eba3567855c014699fef65ae54c770a0d85c18400cf642aedc6607
77ba4b138502bd5a7812f621f84a48296b98dd4322b6f15828b8a8f0e00a8ba4
4a53c3a8b143571b0740abd567daf1cde9c79c204b6d5e259d1766a31bbbcb4e
6a05cf4502176b301c1c2f41247750157bcec85e809b30a4d60d7747cdd0f5b9
9aa8c826987517793aaa8080a0b124a8558df72bbe37b75f4edbb6be8216d6c6
33fb2b2280e25113d8695e43481c3eeb397eb192505229b67a201ea893c3e2cb
32da8bc342fa4dea0578a24e16d8f8f9383a95b77050f4d9fd2f5733eec1d63e
f3c23ebf9918173669a720212223242526272829 2a2b2c2d2e2f303132333435
363738393a3b3c3d3e3f` }
  }
}
```

C.1.2.3. Both Format

```
-----BEGIN PRIVATE KEY-----
MIIJvgIBADALBglghkgBZQMEBAIEggmqMIIJpgRAAAECAwQFBgcICQoLDA0ODxAR
EhMUFRYXGBkaGxwdHh8gISIjJCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+PwSC
CWAn0qd/M3VvYSCO8ROr6CWVhz1KvHMOW11nlSm/akzrY4NCcjGoYS9BVQUVrLpS
5I6ti5QoM7vmhl0T0Up50sXD4H8KBW2N56rfyroFjEk8gLN8q4xWJ1O7O6a27IKX
+IXqp1QNUwAVqEQG5VsTZrV34jbOWKJtih61pE1UIyPCFn2b9KR/mFaZygW65DuN
7GF/AjgKOJCv1LjH7H7eJlU6Al885bxdemITAwQjXLGtSDa1ZrW4Y72b20WihEpw
R7bI04PkSFJeBAtNyKK0jGw3yW1i1D8/2I4ogcQKIFyeJI9lK1kngad5+GiA8qFH
tnhj85HMGlqQjACV4HISKR4u+KNuuanAxgcyJbNHA6SvBJOCxHVz2mj96SRa1ETj
Gx+9tSHx9h83vAzvKSBn5nDSih/9kE9vEZCplpGKEwN6bKvzw3O/gpbNN6szundG
gJzD+K3hs2Ob1Xv8xpZQqq8d4Zj8TARjKZ5SxGF4DMQo/F0EpcUYUMumwqUnQ0Bn
V5PdoJvkTCnmOVxl+F0qCnxt9BHmkRsfLLbDUc0uh19Rtji+d2CX6T4vKy+D2gvu
9KqFup52OrZFAqDKUiLp6rWztwiO1SBg6Mgmm5Q6casK4cWxtofS4BnPgDa8+b9u
e6w6qjbkFmD6pFQPJkjNk6GJ7Fwt6nC6yqpP/JBvkIEOobZ78k8seM9rqIGq6mHA
ZSv/lbG65EJtF3O5zCyoLCHjjGNuOxxSMkSYawvoqD9d1c8tVHYvs8Xr9ZuOiFMC
sc5HAz7fdg9OApvkC21WaxnddYrNXHQSh4ExJE+QFyxT8mZjwh2QUwHUi6+RyRfM
d3np2IAswQ2Jo3BQmaKtOjqIlnQ8EURpgJO+JX2stm3HhSKLkSyNll0Uqig0LDrE
qT/vpTKyCUXdwQIBOcFNY4uQjE3d6aBkW5Wy5EFNQLt58EQTgw8VqHPCi7cFnCdB
ACAV8gQI8FjnFbC/mVtTgLfdMloFarl+ZZor4M32wzcxxoOmNLdx6MkqE5ruS7Dk
nHB3Mh1C/BmffB8pjKYl0iOlwmOgPMSBWbeBJmW3hjfk4YcgssKaa5n0J2aky8Tc
UIupS6g7icOlx4+Lsmu9m3m+uMgYJJD1eT7luWATt0t+Fp4p0WLxMVRk6n1yQ22J
t1UWEZLIHMLdHIuLunle9CbuHMAcN6qjeyz/iwo3i0fL0LTUk5jPwnEpWWmfoL2M
2EZmrMYfVBuE+pa5yFTk516RRK3bRLhWalffu1Rc5CPAM0byssGpF4DRUqjeGk1M
nKzec5LJloiMwjmcAsOLM1Ot+KyrKDkk2gCgW3bnOMcskw1sugmuFomQ+qH+8iJu
eAhh1Bbv9AL091n8ZIqx+XEAEJCH+W5LFI0ssx5IBTFOoM2V+wI+rA2YlHS6QgHX
tB0m9TlLIX7qWzS3Gos3kxwOWUJx4LfHMyVyQCM+e6c1YD5CWofe53B543yyiiF2
RZTOU1DY2itioHF0lDAy7InJiAnHO2Qj0wwdKDp2amTYlwPD1im0l4KNSDIMNGIQ
eXopiqENQjyN2gadArxZ5s3wOglriz2kyrm4DKShSQdnLM7x7E+vI0oLxbfp1HPy
sxM7Oyah0XXLZ6eAWRlpnAL3ZTG5nF+JGAcEu0ykU1xbiXJnnGYKB8XlFLhwCchi
649RV2le+z/ECp3va4HBzAKiSa5PCUrQ2b00hcHBxoCAUgp8jGMgMs7nOBVOXFF2
wH2lYCR3akMP526s9mWj97gyECIVvILxCTnINVcEM2qPrB2B5LsEhapdfHTWtZu+
XF6XKg2LrEEbVbXVVXzWgKGo9xtOuGvEjJoFCXMaVL2dcpCyeWPkNy3JsZnP3KwL
AazSimI5URLkxDZI1iLEjII00BRA6Mw3bJJ/I6WvyawEdMZiJ05CRSXIVS7OOz/i
ZRbekBvH1RW96JVY5ibJXIC5M0L4AQAE855sbJSHHF40TKs5Zsg1+alqWa/THEAo
azixwaeEcLq5R1GJNEU86Gc2qRnx9abVEKhvVFT8OYDLXHZb0r1fezaxQQ1mNcjO
tHxN2g12oo6sk5xxwwJIBIZscWJmWEQhY8LCIRflCs785jeKmFZSMCpO8MLODMcW
t3luK2suN3ffoaw9olmjG1qbUw+MtjioGmKsMBhJq6+VpzAb2jAGiQm/235n28y7
OKVVGiWxo6D2hXSK1XU9iIDwAWxidIYWY4TFVx/iNlkANk0DgxHi2HXbNmaGkyte
xgJDCjaeh6bvXDOHhmV4Jb1MBXrOuSPrCTXmkF5jtM7X+AhXp3PdZLFQ0mYS6prB
IFLbIBe/GEPMtLMoG2kNxyit+oXAAoG448CShzNfhWtPwokvaaL1eSGtoBkUxAmI
Zi1XdpZip4Y1G5tmST2reVlNmG3iEA1lug/06li4FTjSSkQ1olj6wlQEqn9B9lix
OFBl4VjctgEVcycg9ARZqqwV5AaVOpCsUpl9HM0HAGDvxl255lM1RGf61W7HE8hu
dUDEI6zyZp9S+m9KxoiNhx7z6EfAKaiq+7kuF7JKoHmx9Bm6YXW0Qq+xGQnUpWtw
oDNbKHOSGKp8k0jiw8Lz6z0VpB5kF8DdlL/rIUGbMRp7sToYC76DMhipprF0R8yF
8iWFlYenMHcEmsvP1E0PAlQ44V0VOCcNWG4b+DGSqUWc9jwOly+FKXZ5gx7PEhUJ
hRy4NA9vEHsPoaDv0bNqgYm8CFxPXLeE5VP0G5GPgDl84ZVveFvuN3ypqovmmYra
MMJrfD2Ma1UlTMliA7IMQq7grE4eu0COSanj+HnQqweF63AlQl0TBaIpnAFeEg0W
Ow4ZSUzlclPQJG0YJ0XLgZerdDizwbt5cr7Fowbro1Z4VcAUaZ/vZa5Ux3Cg2FwY
QAz2Qq7cZgd3uksThQK9WngS9iH4Skgpa5jdQyK28VgouKjw4AqLpEpTw6ixQ1cb
B0Cr1Wfa8c3px5wgS21eJZ0XZqMbu8tOagXPRQIXazAcHC9BJHdQFXvOyF6AmzCk
1g13R83Q9bmaqMgmmHUXeTqqgICgsSSoVY33K743t19O27a+ghbWxjP7KyKA4lET
2GleQ0gcPus5frGSUFIptnogHqiTw+LLMtqLw0L6TeoFeKJOFtj4+Tg6lbdwUPTZ
/S9XM+7B1j7zwj6/mRgXNmmnICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9
Pj8=
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.2 }
  }
  OCTET_STRING {
    SEQUENCE {
      OCTET_STRING { `000102030405060708090a0b0c0d0e0f1011121314
15161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334
35363738393a3b3c3d3e3f` }
      OCTET_STRING { `27d2a77f33756f61208ef113abe82595873d4abc73
0e5b5d679529bf6a4ceb6383427231a8612f41550515acba52e48ead8b942833
bbe6865d13d14a79d2c5c3e07f0a056d8de7aadfcaba058c493c80b37cab8c56
2753bb3ba6b6ec8297f885eaa7540d530015a84406e55b1366b577e236ce58a2
6d8a1eb5a44d542323c2167d9bf4a47f985699ca05bae43b8dec617f02380a38
90afd4b8c7ec7ede26553a025f3ce5bc5d7a62130304235cb1ad4836b566b5b8
63bd9bdb45a2844a7047b6c8d383e448525e040b4dc8a2b48c6c37c96d62d43f
3fd88e2881c40a205c9e248f652b592781a779f86880f2a147b67863f391cc1a
5a908c0095e07212291e2ef8a36eb9a9c0c6073225b34703a4af049382c47573
da68fde9245ad444e31b1fbdb521f1f61f37bc0cef292067e670d28a1ffd904f
6f1190a996918a13037a6cabf3c373bf8296cd37ab33ba7746809cc3f8ade1b3
639bd57bfcc69650aaaf1de198fc4c0463299e52c461780cc428fc5d04a5c518
50cba6c2a5274340675793dda09be44c29e6395c65f85d2a0a7c6df411e6911b
1f2cb6c351cd2e875f51b638be776097e93e2f2b2f83da0beef4aa85ba9e763a
b64502a0ca5222e9eab5b3b7088ed52060e8c8269b943a71ab0ae1c5b1b687d2
e019cf8036bcf9bf6e7bac3aaa36e41660faa4540f2648cd93a189ec5c2dea70
bacaaa4ffc906f90810ea1b67bf24f2c78cf6ba881aaea61c0652bff95b1bae4
426d1773b9cc2ca82c21e38c636e3b1c523244986b0be8a83f5dd5cf2d54762f
b3c5ebf59b8e885302b1ce47033edf760f4e029be40b6d566b19dd758acd5c74
12878131244f90172c53f26663c21d905301d48baf91c917cc7779e9d8802cc1
0d89a3705099a2ad3a3a8896743c1144698093be257dacb66dc785228b912c8d
965d14aa28342c3ac4a93fefa532b20945ddc1020139c14d638b908c4ddde9a0
645b95b2e4414d40bb79f04413830f15a873c28bb7059c2741002015f20408f0
58e715b0bf995b5380b7dd325a056ab97e659a2be0cdf6c33731c683a634b771
e8c92a139aee4bb0e49c7077321d42fc199f7c1f298ca625d223a5c263a03cc4
8159b7812665b78637e4e18720b2c29a6b99f42766a4cbc4dc508ba94ba83b89
c3a5c78f8bb26bbd9b79beb8c8182490f5793ee5b96013b74b7e169e29d162f1
315464ea7d72436d89b755161192c81cc2dd1c8b8bba795ef426ee1cc01c37aa
a37b2cff8b0a378b47cbd0b4d49398cfc2712959699fa0bd8cd84666acc61f54
1b84fa96b9c854e4e75e9144addb44b8566a57dfbb545ce423c03346f2b2c1a9
1780d152a8de1a4d4c9cacde7392c996888cc2399c02c38b3353adf8acab2839
24da00a05b76e738c72c930d6cba09ae168990faa1fef2226e780861d416eff4
02f4f759fc648ab1f97100109087f96e4b148d2cb31e4805314ea0cd95fb023e
ac0d989474ba4201d7b41d26f5394b217eea5b34b71a8b37931c0e594271e0b7
c733257240233e7ba735603e425a87dee77079e37cb28a21764594ce5350d8da
2b62a07174943032ec89c98809c73b6423d30c1d283a766a64d89703c3d629b4
97828d48320c346210797a298aa10d423c8dda069d02bc59e6cdf03a096b8b3d
a4cab9b80ca4a14907672ccef1ec4faf234a0bc5b7e9d473f2b3133b3b26a1d1
75cb67a7805919699c02f76531b99c5f89180704bb4ca4535c5b8972679c660a
07c5e514b87009c862eb8f5157695efb3fc40a9def6b81c1cc02a249ae4f094a
d0d9bd3485c1c1c68080520a7c8c632032cee738154e5c5176c07da56024776a
430fe76eacf665a3f7b832102215bc82f10939c8355704336a8fac1d81e4bb04
85aa5d7c74d6b59bbe5c5e972a0d8bac411b55b5d5557cd680a1a8f71b4eb86b
c48c9a0509731a54bd9d7290b27963e4372dc9b199cfdcac0b01acd28a623951
12e4c43648d622c48c8234d01440e8cc376c927f23a5afc9ac0474c662274e42
4525c8552ece3b3fe26516de901bc7d515bde89558e626c95c80b93342f80100
04f39e6c6c94871c5e344cab3966c835f9a96a59afd31c40286b38b1c1a78470
```

```
bab947518934453ce86736a919f1f5a6d510a86f5454fc3980cb5c765bd2bd5f
7b36b1410d6635c8ceb47c4dda0d76a28eac939c71c3024804866c7162665844
2163c2c22117e50acefce6378a985652302a4ef0c2ce0cc716b7796e2b6b2e37
77dfa1ac3da259a31b5a9b530f8cb638a81a62ac301849abaf95a7301bda3006
8909bfdb7e67dbccbb38a5551a25b1a3a0f685748ad5753d8880f0016c627486
166384c5571fe2365900364d038311e2d875db366686932b5ec602430a369e87
a6ef5c338786657825bd4c057aceb923eb0935e6905e63b4ced7f80857a773dd
64b150d26612ea9ac12052db2017bf1843ccb4b3281b690dc728adfa85c00281
b8e3c09287335f856b4fc2892f69a2f57921ada01914c40988662d57769662a7
86351b9b66493dab79594d986de2100d65ba0ff4ea58b81538d24a4435a258fa
c25404aa7f41f658b1385065e158dcb60115732720f40459aaac15e406953a90
ac52997d1ccd070060efc65db9e653354467fad56ec713c86e7540c423acf266
9f52fa6f4ac6888d871ef3e847c029a8aafbb92e17b24aa079b1f419ba6175b4
42afb11909d4a56b70a0335b28739218aa7c9348e2c3c2f3eb3d15a41e6417c0
dd94bfeb21419b311a7bb13a180bbe833218a9a6b17447cc85f225859587a730
77049acbcfd44d0f025438e15d1538270d586e1bf83192a9459cf63c0e972f85
297679831ecf121509851cb8340f6f107b0fa1a0efd1b36a8189bc085c4f5cb7
84e553f41b918f80397ce1956f785bee377ca9aa8be6998ada30c26b7c3d8c6b
55254cc96203b20c42aee0ac4e1ebb408e49a9e3f879d0ab0785eb7025425d13
05a2299c015e120d163b0e19494ce57253d0246d182745cb8197ab7438b3c1bb
7972bec5a306eba3567855c014699fef65ae54c770a0d85c18400cf642aedc66
0777ba4b138502bd5a7812f621f84a48296b98dd4322b6f15828b8a8f0e00a8b
a44a53c3a8b143571b0740abd567daf1cde9c79c204b6d5e259d1766a31bbbcb
4e6a05cf4502176b301c1c2f41247750157bcec85e809b30a4d60d7747cdd0f5
b99aa8c826987517793aaa8080a0b124a8558df72bbe37b75f4edbb6be8216d6
c633fb2b2280e25113d8695e43481c3eeb397eb192505229b67a201ea893c3e2
cb32da8bc342fa4dea0578a24e16d8f8f9383a95b77050f4d9fd2f5733eec1d6
3ef3c23ebf9918173669a7202122232425262728292a2b2c2d2e2f3031323334
35363738393a3b3c3d3e3f` }
    }
  }
}
```

C.1.3. ML-KEM-1024 Private Key Examples

Each of the examples includes the textual encoding [RFC7468] followed by the so-called "pretty print"; the private keys are the same.

C.1.3.1. Seed Format

```
-----BEGIN PRIVATE KEY-----
MFQCAQAwCwYJYIZIAWUDBAQDBEKAQAABAgMEBQYHCAkKCwwNDg8QERITFBUWFxgZ
GhscHR4fICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9Pj8=
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.3 }
  }
  OCTET_STRING {
    [0 PRIMITIVE] { `000102030405060708090a0b0c0d0e0f10111213141
5161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f30313233343
5363738393a3b3c3d3e3f` }
  }
}
```

C.1.3.2. Expanded Format

```
-----BEGIN PRIVATE KEY-----
MIIMeAIBADALBglghkgBZQMEBAMEggxkBIIMYPd7f2sVxz/izFRrZ/t3TKGbQs1G
Pqn7uYTKR3p3tscQh8vwUavkc2qQcsbocMgxHFWWP1AKPHsbjypYVY9JxiUntsWU
teess7z1lyc6V0NRfRUSCL1Kph51umewvVlKmUkZYnrAqATUieFxM2vDOfRmZwbl
E0QSs2aCPVAxjIvyYasSCiigT+wBzBXytxkSzuVKqO7YVGlLa6iGtet2YebVaqwh
PMHYFNWSs5VVT650R200NxFjEpv4ZFJyUGBswhpTdGsgmXB3u6FVczsopOf6B3Y5
lSR2PrSBzqoRNmw0dKBGhfQMPwiwQk9Av/lJoKyScEw7oMbrNvH1tiHYvytjJ761
fNP6y5QYb+P8mrChQ0uykdLJu3ByMFfiJUBZZW9WWRmjLPdFed6JaBzSxak1pStK
qi0ky11cniBynsVJLsNpYe+4ooy8AKwwNSMpXz2ANqvBYDMHznDXhIo1ZXpWh91Y
mSfqY3MWJquybsTkMbjrazsLweglc+5zsaAhGDGDUoEIri6srduVtGSguYRpwxnM
J7+gG8MQVKaMBVArFmK4ef6YoXEcNCb2Q2ywIUzqN5rDp+X7YBhKN8HaHtphxsOc
HdToR4RYEfKjWKQ3MVKFNtSjKRsEFYwsPcZBYkiCZ4vHgF9YqdlMcQRWeEaiBE5l
rs4qIlNytgJHmaVHfWAjdQSqXArFe8cKNVjAjE3mh+8TArT8tVlEE9IsuVm8Mb5C
NFBAPGvFfcQRs/76wQUqxLsWLERUWkyoCJJlf6E6CyxILO1inMSZnZacWT1KrfBz
zD46RY54qKoDlAjmUr6TsgyLQuxbDlAjnaxyYFKFGm0VMS7DntIItyIJpXfGsncB
EolXSdUmDn3URsCwEYwQAL5oAdJhH88AeSqcxPS0mSL5otS5yPpaXQ1gUGYxp+lx
zuhAsI+mPBNynX6lqscDUqmEzbZpMxy6dY/ofsOTGz4xYfzHR6p0lCRon+rhS/fJ
ov+6EwKyErgDctjpBJ22mjoSYdCihZqbTVeJngukFgehtnp8DhKSNon4xjlTd9lw
x0kKQSlhGh0Fw7eBO+2UVCByP3+VJah3k/r7v8qYLma7gGgcgySKidoITBmIL0jz
Hn/AkJOknp/QlpGwIe30Y6/FGbYoU4FhGDRhFfsLiCzGSC88XLzBwYlGl+EjlZiz
Syqaes0VJE0GkMiBlAl6m+2lheh8Q3EkYkwhB2jmIV03ZIJlPriZR4d8EY03DGlq
b/zBAYrkE6CKjQ/6qBmUXaehZ8IpkTKQytHICjaSWHYmEOolPmLcJCJqMMiSwSE2
wybxP0RGZkcSsLkLwGO0AoWTy94GzcIiieJAx+KWtZFywa7ajJngUS0aAWOpQuoz
FI5pN8AmApQkuBuZax3yLqBiPsZca/CTUAzzvzU3Stw5IDXKfFg7mWhbylQaCAex
Y6zQiIvgOF3qgg2kbk27RNLkYsc0uDpHP+0TZCcxWSV8wlmoxWdsHHbUHVa5kH7B
w1mcnokHQDonpwXjYZsEsK0Ebo7IFpwXtGDUTAwMRGTQRMlGGGvHJZZQg6iSvMSV
wFQDEf+bPlGSwwPYj4ukapAceC7wI4jxsq3atqU1D8NjlwDjFUM3M35KF401HNK1
buHwv+o0qs+jPS7HkeUHUtTQNMsclRVyyqpcTZCUe2sXWm3Txip3u496ya4kcZtT
wrEgoodphuIXtyvXzuRKcmWxHO4asiYXYrMaNzg4aWnAgl+3lFLmUuEUL8c8nfb7
pBF5W0cXkispui1Tq+WowNzBYBsJbJbXk4/VpoqHl8e5R3qGpHLrXaJQyy/sMY2D
yPQ7vo4Rw143fTSTZshcQ4JZf2/CegBRwPsAsCwByiD5pCfxclmUd8ppDMEyfg8C
X4DsM4qAoVnjCMEqJ9safhuWCpnTffwihy5Rkw8oxlGrIh9Tq67iC62aPqvLq5Ey
Ub8TW+spYXtXVDM8TarbIjg0HCrZN4GGKA9kSUQLeEunj12sRNj2Wzt0IZUDl8OR
Oi3SPsbRy3F7NqX8la8ZHieClpSMElTqhrTsAEuUwpRQERGRgjs1FMmsHqPZglzL
hjk6LfsEZU+iGS03v60cSXxlAu7lyoCnO/zguvWlSohYWkATl6PSMvQmp6+wgrwh
pEMXCQ6qx1ksLqiKZTxEkeoZOTEzX1LpiaPEzFbZxVNzLVfEcPtBq3WbZdLQREU4
L82cTjRKESj6nhHgQ1jhku0BSyMjKn7isi4jcX9EER7jNXU5nDdkbamBPsmyEq/p
Tl3FwjMKcpTMH0I0ptP7tPFoWriJLASssXzRwXDXsGEbanF2x5TMjGf1X8kjwq0g
MQDzZZkYgsMCQ9d4E4Q7XsfJZAMiY3BgkuzwDHUWvmTkWYykImwGm7XmfkF1zyKG
yN1cSIpsWGHzG6oL0CaUcOi1Ud07zTjIbBL5zbF2x33ItsAqcB9HiQLIVT9pTA2C
cntMSlwsEEEhKqEnSAi4IRGzd+x1IU6bGXj3YATUE52YYT9LjpjSCve1NAc6UJqV
m3p1ZPm0DKIYv2GCkyCoUCAXlU0yjXrGx2nsKXAHVuewaFs0DV4RgFlQSkmppQoQ
GY6xCleEZ460J9e0uruVUpM7BiiXlz4TGOrwoOrDdYSmVAGxcD4EKszYN1MUg/JB
ytzRwdN4EZ5pRCnbGZrIkeTFNDdXCFuzrng2ZzUMRFjZdnLoYegLHSZ5UQ6jpvI2
DHekaULHoGpVTSKAgMhLR67xTbF2IMsWwGqzChvkzacIK+n4fpwhHEaRY0mluo6q
UgHHKUo8CIW1O2V0UhCIJexkbJCgRhIyTufQMa/lNDEyy+9ntu+xpewoCbdzU4zn
ez2LBOsLPCJWAR5McWwZqLoHUr9xSSEXZJ8GFcMpD8KaRv3kvVLbkobWAziCRCWc
FaesK2QKYMwDN2pYQaP7ikc1aPqbGiZyFfNMAWl7Dw5icXXXIQW3cHwpueYUvcM6
b2yBipU3C0J4gte0dnlqnsbrmTJ0zZsjkagrpF4zk9Lprpchyp1sG5iLWCdxP5Cm
WF3pQzUowCsDzhC7X3IBOND7tMMMEma5GOUpJd/hezf5XSK8pU9HWRmshZCYwPDQ
isWHXvKbVv0UHm7xX3AKC2bzlZXFiBdzc8RmmyG8Bx5MOqXwtKMbYljzXaJKw80p
x/IJJBDFB4NVsTj7U6a5rm4LnAgkPnuqRcRzduuMfxPUz1Gqc2+jFUDJJB83DaVE
v5+cKNmlfi8qfKlaTktGbmQas7zHat8ROdVnpvErUvOmXn7AquJryqjFWDOwTlmZ
jryaGTD7ttIjPFPSwfi5UY48Lec6Gd7ms4Clsylxz2ThKf1sH6bnXUojRQHpZt06
VAr1yPTzSmtKJT7ihJJWbV5nxvVYVfywUG+wbBVnRNmgOjGib6lMrRTxV7fzA9B6
acdzdo/LTQecCQWXA6DDqU3kuZ6jovFlg9D5Fwo5UNsHtPC8MIApJ/n3lhtiWYkm
NqlQKicFMDY3eZ3TRNpFHBz3v2eEDOsweauMa4wZJ/ZAU8YSRQxFyeYDvBZmbllr
```

```
NHHhA7bxVEdCTRcCIEgRH/vTfhxnD2TxS4p7MrlMGkm0XdL8OM1SidkQrWNgLPXh
MELGSsZ5e4n7VRrQjgWpLSAMzLfnEu8jyTEss1DwKatTfihzR/0wdawQkGp4Pxxs
B8y4j0EijEvhxkD3kLXDpdXTynkkldd LxGFWJljAesYAJ2uSSrW8m+HwSUy3b4L0
YKdICXJmM4HhaZlgYdeZhZ7FTU9cpcQRwB2xWXsWWXdmneE6koo0r7rCWP6oxHZC
OclCHcMRm/W0dpkgaXgyexxTRe90anmDhB8FbiU0EAqyTU6au9CxfGqVvUw8DkD2
nhYSrO6yi5kIbJURbnIEJziTOQv0a4mbNihrDr8ZR7uYhPcyyifagrGbXcDMf4iF
cUkQiIsjEMT5MZ1BCzTmQzuQA+IXa7mVJXRWEG6JUhY7i6WSUwzFqgrrQ605j+np
e6pSPXpEMWd8PTrwcZ5HXbhcqVr1CJvqvrBbL6q0iWumD4HIhHKle0aoKIJqDN+0
RvgYkYLSv16sTsHMXer1mcihPkgjVAbRf/3cg0S2xmmEqGiqkvoCInoIaVDrDIcB
7VjcYod2uYOILhF1YTSeXBMafhFqBGOGHX0YZjxWJ8OMcUfdqt/Uis16RTUgISIj
JCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+Pw==
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.3 }
  }
  OCTET_STRING {
    OCTET_STRING { `f77b7f6b15c73fe2cc546b67fb774ca19b42cd463ea9
fbb984ca477a77b6c71087cbf051abe4736a9072c6e870c8311c55963f500a3c
7b1b8f2a58558f49c62527b6c594b5e7acb3bcf597273a5743517d151208bd4a
a61e75ba67b0bd594a994919627ac0a804d489e171336bc339f4666706e51344
12b366823d50318c8bf261ab120a28a04fec01cc15f2b71912cee54aa8eed854
694b6ba886b5eb7661e6d56aac213cc1d814d592b395554fae74476d34371163
129bf864527250606cc21a53746b20997077bba155733b28a4e7fa0776399524
763eb481ceaa11366c3474a04685f40c3f08b0424f40bff949a0ac92704c3ba0
c6eb36f1f5b621d8bf2b6327beb57cd3facb94186fe3fc9ab0a1434bb291d2c9
bb70723057e2254059656f565919a32cf74579de89681cd2c5a935a52b4aaa2d
24cb5d5c9e20729ec5492ec36961efb8a28cbc00ac303523295f3d8036abc160
3307ce70d7848a35657a5687dd589927ea63731626abb26ec4e431b8eb6b3b0b
c1e82573ee73b1a021183183528108ae2eacaddb95b464a0b98469c319cc27bf
a01bc31054a68c05502b1662b879fe98a1711c3426f6436cb0214cea379ac3a7
e5fb60184a37c1da1eda61c6c39c1dd4e847845811f2a358a43731528536d4a3
291b04158c2c3dc641624882678bc7805f58a9d94c7104567846a2044e65aece
2a225372b6024799a5477d60237504aa5c0ac57bc70a3558c08c4de687ef1302
b4fcb5594413d22cb959bc31be423450403c6bc57dc411b3fefac1052ac4bb16
2c44545a4ca80892657fa13a0b2c482ced629cc4999d969c593d4aadf073cc3e
3a458e78a8aa039408e652be93b20c8b42ec5b0e50239dac726052851a6d1531
2ec39ed208b72209a577c6b2770112895749d5260e7dd446c0b0118c1000be68
01d2611fcf00792a9cc4f4b49922f9a2d4b9c8fa5a5d0d60506631a7e971cee8
40b08fa63c13729d7ea5aac70352a984cdb669331cba758fe87ec3931b3e3161
fcc747aa749424689feae14bf7c9a2ffba1302b212b80372d8e9049db69a3a12
61d0a2859a9b4d57899e0ba41607a1b67a7c0e12923689f8c6395377d970c749
0a4129611a1d05c3b7813bed945420723f7f9525a87793fafbbfca982e66bb80
681c83248a89da084c19882f48f31e7fc09093a49e9fd09691b021edf463afc5
19b628538161183461l5fb0b882cc6482f3c5cbcc1c1894697e1239598b34b2a
9a7acd15244d0690c88194097a9beda585e87c437124624c210768e6215d3764
82653eb89947877c118d370c696a6ffcc1018ae413a08a8d0ffaa819945da7a1
67c229913290cad1c80a369258762610ea253e62dc24226a30c892c12136c326
f13f4446664712b0b90bc063b4028593cbde06cdc22289e240c7e296b59172c1
aeda8c99e0512d1a0163a942ea33148e6937c026029424b81b996b1df22ea062
3ec65c6bf093500cf3bf35374adc392035ca7c583b99685bca541a0807b163ac
d0888be0385dea820da46e4dbb44d2e462c734b83a473fed1364273159257cc2
59a8c5676c1c76d41d56b9907ec1c3599c9e8907403a27a705e3619b04b0ad04
6e8ec8169c17b460d44c0c0c4464d044c946186bc725965083a892bcc495c054
0311ff9b3e5192c303d88f8ba46a901c782ef02388f1b2addab6a5350fc36397
00e3154337337e4a178d351cd2b56ee1f0bfea34aacfa33d2ec791e50752d4d0
34cb1c951572caaa5c4d90947b6b175a6dd3c62a77bb8f7ac9ae24719b53c2b1
20a2876986e217b72bd7cee44a7265b11cee1ab2261762b31a3738386969c082
5fb79452e652e1142fc73c9df6fba411795b4717922b29ba2d53abe5a8c0dcc1
601b096c96d7938fd5a68a8797c7b9477a86a472eb5da250cb2fec318d83c8f4
3bbe8e11c35e377d349366c85c4382597f6fc27a0051c0fb00b02c01ca20f9a4
27f172599477ca690cc1327e0f025f80ec338a80a159e308c12a27db1a7e1b96
0a99d37dfc22872e51930f28c651ab221f53abaee20bad9a3eabcbab913251bf
135beb29617b5754333c4daadb2238341c2ad9378186280f6449440b784ba78f
5dac44d8f65b3b7421950397c3913a2dd23ec6d1cb717b36a5fc95af191e2782
96948c1254ea86b4ec004b94c29450111191823b3514c9ac1ea3d9825ccb8639
3a2dfb04654fa2192d37bfad1c497c6502eee5ca80a73bfce0baf5a54a88585a
401397a3d232f426a7afb082bc21a44317090eaac7592c2ea88a653c4491ea19
```

```
3931335f52e989a3c4cc56d9c553732d57c470fb41ab759b65d2d04445382fcd
9c4e344a1128fa9e11e04358e192ed014b23232a7ee2b22e23717f44111ee335
75399c37646da9813ec9b212afe94e5dc5c2330a7294cc1f4234a6d3fbb4f168
5ab8892c04acb17cd1c170d7b0611b6a7176c794cc8c67f55fc923c2ad203100
f365991882c30243d77813843b5ec7c964032263706092ecf00c7516be64e459
8ca4226c069bb5e67e4175cf2286c8dd5c488a6c5861f31baa0bd0269470e8b5
51dd3bcd38c86c12f9cdb176c77dc8b6c02a701f478902c8553f694c0d82727b
4c4a5c2c1041212aa1274808b82111b377ec75214e9b1978f76004d4139d9861
3f4b8e98d20af7b534073a509a959b7a7564f9b40ca218bf61829320a8502017
954d328d7ac6c769ec29700756e7b0685b340d5e118059504a49a9a50a10198e
b10a5784678eb427d7b4babb9552933b062897973e1318eaf0a0eac37584a654
01b1703e042accd837531483f241cadcd1c1d378119e694429db199ac891e4c5
343757085bb3ae783667350c4458d97672e861e80b1d2679510ea3a6f2360c77
a46942c7a06a554d228080c84b47aef14db17620cb16c06ab30a1be4cda7082b
e9f87e9c211c46916349a5ba8eaa5201c7294a3c0885b53b657452108825ec64
6c90a04612324ee7d031afe5343132cbef67b6efb1a5ec2809b773538ce77b3d
8b04eb0b3c2256011e4c716c19a8ba0752bf71492117649f0615c3290fc29a46
fde4bd52db9286d603388244259c15a7ac2b640a60cc03376a5841a3fb8a4735
68fa9b1a267215f34c01697b0f0e627175d72105b7707c29b9e614bdc33a6f6c
818a95370b427882d7b476796a9ec6eb993274cd9b2391a82ba45e3393d2e9ae
9721ca9d6c1b988b5827713f90a6585de9433528c02b03ce10bb5f720138d0fb
b4c30c1266b918e52925dfe17b37f95d22bca54f475919ac859098c0f0d08ac5
875ef29b56fd141e6ef15f700a0b66f39595c588177373c4669b21bc071e4c3a
a5f0b4a31b6258f35da24ac3cd29c7f2092410c5078355b138fb53a6b9ae6e0b
9c08243e7baa45c47376eb8c7f13d4cf51aa736fa31540c9241f370da544bf9f
9c28d9a57e2f2a7ca95a4e4b466e641ab3bcc76adf1139d567a6f12b52f3a65e
7ec0aae26bcaa8c55833b04e59998ebc9a1930fbb6d2233c53d2c1f8b9518e3c
2de73a19dee6b380a5b32971cf64e129fd6c1fa6e75d4a234501e966dd3a540a
f5c8f4f34a6b4a253ee28492566d5e67c6f55855fcb0506fb06c156744d9a03a
31a26fa94cad14f157b7f303d07a69c773768fcb4d079c09059703a0c3a94de4
b99ea3a2f16583d0f9170a3950db07b4f0bc30802927f9f7961b6259892636a9
502a2705303637799dd344da451c1cf7bf67840ceb3079ab8c6b8c1927f64053
c612450c45c9e603bc16666e596b3471e103b6f15447424d17022048111ffbd3
7e1c670f64f14b8a7b32b94c1a49b45dd2fc38cd5289d910ad63602cf5e13042
c64ac6797b89fb551ad08e05a92d200cccb7e712ef23c9312cb350f029ab537e
287347fd3075ac10906a783f1c6c07ccb88f41228c4be1c640f790b5c3a5d5d3
ca792495d74bc461562658c07ac600276b924ab5bc9be1f0494cb76f82f460a7
480972663381e169996061d799859ec54d4f5ca5c411c01db1597b165977669d
e13a928a34afbac258fea8c4764239c9421dc3119bf5b47699206978327b1c53
45ef746a7983841f056e2534100ab24d4e9abbd0b17c6a95bd4c3c0e40f69e16
12aceeb28b99086c95116e7204273893390bf46b899b36286b0ebf1947bb9884
f732ca27da82b19b5dc0cc7f8885714910888b2310c4f9319d410b34e6433b90
03e2176bb995257456106e8952163b8ba592530cc5aa0aeb43ad398fe9e97baa
523d7a4431677c3d3af0719e475db85ca95af5089beabeb05b2faab4896ba60f
81c88472a57b46a828826a0cdfb446f8189182d2bf5eac4ec1cc5deaf599c8a1
3e48235406d17ffddc8344b6c66984a868aa92fa02227a086950eb0c8701ed58
dc628776b983882e117561349e5c131a7e116a0463861d7d18663c5627c38c71
47ddaadfd48acd7a4535202122232425262728292a2b2c2d2e2f303132333435
363738393a3b3c3d3e3f` }
  }
}
```

C.1.3.3. Both Format

```
-----BEGIN PRIVATE KEY-----
MIIMvgIBADALBglghkgBZQMEBAMEggyqMIIMpgRAAAECAwQFBgcICQoLDA0ODxAR
EhMUFRYXGBkaGxwdHh8gISIjJCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+PwSC
DGD3e39rFcc/4sxUa2f7d0yhm0LNRj6p+7mEykd6d7bHEIfL8FGr5HNqkHLG6HDI
MRxVlj9QCjx7G48qWFWPScYlJ7bFlLXnrLO89ZcnOldDUX0VEgi9SqYedbpnsL1Z
SplJGWJ6wKgE1InhcTNrwzn0ZmcG5RNEErNmgj1QMYyL8mGrEgoooE/sAcwV8rcZ
Es7lSqju2FRpS2uohrXrdmHm1WqsITzB2BTVkrOVVU+udEdtNDcRYxKb+GRSclBg
bMIaU3RrIJlwd7uhVXM7KKTn+gd2OZUkdj60gc6qETZsNHSgRoX0DD8IsEJPQL/5
SaCsknBMO6DG6zbx9bYh2L8rYye+tXzT+suUGG/j/JqwoUNLspHSybtwcjBX4iVA
WWVvVlkZoyz3RXneiWgc0sWpNaUrSqotJMtdXJ4gcp7FSS7DaWHvuKKMvACsMDUj
KV89gDarwWAzB85w14SKNWV6VofdWJkn6mNzFiarsm7E5DG462s7C8HoJXPuc7Gg
IRgxg1KBCK4urK3blbRkoLmEacMZzCe/oBvDEFSmjAVQKxZiuHn+mKFxHDQm9kNs
sCFM6jeaw6fl+2AYSjfB2h7aYcbDnB3U6EeEWBHyo1ikNzFShTbUoykbBBWMLD3G
QWJIgmeLx4BfWKnZTHEEVnhGogROZa7OKiJTcrYCR5mlR31gI3UEqlwKxXvHCjVY
wIxN5ofvEwK0/LVZRBPSLLlZvDG+QjRQQDxrxX3EEbP++sEFKsS7FixEVFpMqAiS
ZX+hOgssSCztYpzEmZ2WnFk9Sq3wc8w+OkWOeKiqA5QI5lK+k7IMi0LsWw5QI52s
cmBShRptFTEuw57SCLciCaV3xrJ3ARKJV0nVJg591EbAsBGMEAC+aAHSYR/PAHkq
nMT0tJki+aLUucj6Wl0NYFBmMafpcc7oQLCPpjwTcp1+parHA1KphM22aTMcunWP
6H7Dkxs+MWH8x0eqdJQkaJ/q4Uv3yaL/uhMCshK4A3LY6QSdtpo6EmHQooWam01X
iZ4LpBYHobZ6fA4SkjaJ+MY5U3fZcMdJCkEpYRodBcO3gTvtlFQgcj9/lSWod5P6
+7/KmC5mu4BoHIMkionaCEwZiC9I8x5/wJCTpJ6f0JaRsCHt9GOvxRm2KFOBYRg0
YRX7C4gsxkgvPFy8wcGJRpfhI5WYs0sqmnrNFSRNBpDIgZQJepvtpYXofENxJGJM
IQdo5iFdN2SCZT64mUeHfBGNNwxpam/8wQGK5BOgio0P+qgZlF2noWfCKZEykMrR
yAo2klh2JhDqJT5i3CQiajDIksEhNsMm8T9ERmZHErC5C8BjtAKFk8veBs3CIoni
QMfilrWRcsGu2oyZ4FEtGgFjqULqMxSOaTfAJgKUJLgbmWsd8i6gYj7GXGvwk1AM
8781N0rcOSA1ynxYO5loW8pUGggHsWOs0IiL4Dhd6oINpG5Nu0TS5GLHNLg6Rz/t
E2QnMVklfMJZqMVnbBx21B1WuZB+wcNZnJ6JB0A6J6cF42GbBLCtBG6OyBacF7Rg
1EwMDERk0ETJRhhrxyWWUIOokrzElcBUAxH/mz5RksMD2I+LpGqQHHgu8COI8bKt
2ralNQ/DY5cA4xVDNzN+SheNNRzStW7h8L/qNKrPoz0ux5HlB1LU0DTLHJUVcsqq
XE2QlHtrF1pt08Yqd7uPesmuJHGbU8KxIKKHaYbiF7cr187kSnJlsRzuGrImF2Kz
Gjc4OGlpwIJft5RS5lLhFC/HPJ32+6QReVtHF5IrKbotU6vlqMDcwWAbCWyW15OP
1aaKh5fHuUd6hqRy612iUMsv7DGNg8j0O76OEcNeN300k2bIXEOCWX9vwnoAUcD7
ALAsAcog+aQn8XJZlHfKaQzBMn4PAl+A7DOKgKFZ4wjBKifbGn4blgqZ0338Iocu
UZMPKMZRqyIfU6uu4gutmj6ry6uRMlG/E1vrKWF7V1QzPE2q2yI4NBwq2TeBhigP
ZElEC3hLp49drETY9ls7dCGVA5fDkTot0j7G0ctxezal/JWvGR4ngpaUjBJU6oa0
7ABLlMKUUBERkYI7NRTJrB6j2YJcy4Y5Oi37BGVPohktN7+tHEl8ZQLu5cqApzv8
4Lr1pUqIWFpAE5ej0jL0JqevsIK8IaRDFwkOqsdZLC6oimU8RJHqGTkxM19S6Ymj
xMxW2cVTcy1XxHD7Qat1m2XS0ERFOC/NnE40ShEo+p4R4ENY4ZLtAUsjIyp+4rIu
I3F/RBEe4zV1OZw3ZG2pgT7JshKv6U5dxcIzCnKUzB9CNKbT+7TxaFq4iSwErLF8
0cFw17BhG2pxdseUzIxn9V/JI8KtIDEA82WZGILDAkPXeBOEO17HyWQDImNwYJLs
8Ax1Fr5k5FmMpCJsBpu15n5Bdc8ihsjdXEiKbFhh8xuqC9AmlHDotVHdO804yGwS
+c2xdsd9yLbAKnAfR4kCyFU/aUwNgnJ7TEpcLBBBISqhJ0gIuCERs3fsdSFOmxl4
92AE1BOdmGE/S46Y0gr3tTQHOlCalZt6dWT5tAyiGL9hgpMgqFAgF5VNMo16xsdp
7ClwB1bnsGhbNA1eEYBZUEpJqaUKEBmOsQpXhGeOtCfXtLq7lVKTOwYol5c+Exjq
8KDqw3WEplQBsXA+BCrM2DdTFIPyQcrc0cHTeBGeaUQp2xmayJHkxTQ3Vwhbs654
Nmc1DERY2XZy6GHoCx0meVEOo6byNgx3pGlCx6BqVU0igIDIS0eu8U2xdiDLFsBq
swob5M2nCCvp+H6cIRxGkWNJpbqOqlIBxylKPAiFtTtldFIQiCXsZGyQoEYSMk7n
0DGv5TQxMsvvZ7bvsaXsKAm3c1OM53s9iwTrCzwiVgEeTHFsGai6B1K/cUkhF2Sf
BhXDKQ/Cmkb95L1S25KG1gM4gkQlnBWnrCtkCmDMAzdqWEGj+4pHNWj6mxomchXz
TAFpew8OYnF11yEFt3B8KbnmFL3DOm9sgYqVNwtCeILXtHZ5ap7G65kydM2bI5Go
K6ReM5PS6a6XIcqdbBuYi1gncT+Qplhd6UM1KMArA84Qu19yATjQ+7TDDBJmuRjl
KSXf4Xs3+V0ivKVPR1kZrIWQmMDw0IrFh17ym1b9FB5u8V9wCgtm85WVxYgXc3PE
ZpshvAceTDql8LSjG2JY812iSsPNKcfyCSQQxQeDVbE4+1Omua5uC5wIJD57qkXE
c3brjH8T1M9RqnNvoxVAySQfNw2lRL+fnCjZpX4vKnypWk5LRm5kGrO8x2rfETnV
Z6bxK1Lzpl5+wKria8qoxVgzsE5ZmY68mhkw+7bSIzxT0sH4uVGOPC3nOhne5rOA
pbMpcc9k4Sn9bB+m511KI0UB6WbdOlQK9cj080prSiU+4oSSVm1eZ8b1WFX8sFBv
sGwVZ0TZoDoxom+pTK0U8Ve38wPQemnHc3aPy00HnAkFlwOgw6lN5Lmeo6LxZYPQ
```

```
+RcKOVDbB7TwvDCAKSf595YbYlmJJjapUConBTA2N3md00TaRRwc979nhAzrMHmr
jGuMGSf2QFPGEkUMRcnmA7wWZm5ZazRx4QO28VRHQk0XAiBIER/7034cZw9k8UuK
ezK5TBpJtF3S/DjNUonZEK1jYCz14TBCxkrGeXuJ+1Ua0I4FqS0gDMy35xLvI8kx
LLNQ8CmrU34oc0f9MHWsEJBqeD8cbAfMuI9BIoxL4cZA95C1w6XV08p5JJXXS8Rh
ViZYwHrGACdrkkq1vJvh8ElMt2+C9GCnSAlyZjOB4WmZYGHXmYWexU1PXKXEEcAd
sVl7Fll3Zp3hOpKKNK+6wlj+qMR2QjnJQh3DEZv1tHaZIGl4MnscU0XvdGp5g4Qf
BW4lNBAKsk1OmrvQsXxqlb1MPA5A9p4WEqzusouZCGyVEW5yBCc4kzkL9GuJmzYo
aw6/GUe7mIT3Mson2oKxm13AzH+IhXFJEIiLIxDE+TGdQQs05kM7kAPiF2u5lSV0
VhBuiVIWO4ulklMMxaoK60OtOY/p6XuqUj16RDFnfD068HGeR124XKla9Qib6r6w
Wy+qtIlrpg+ByIRypXtGqCiCagzftEb4GJGC0r9erE7BzF3q9ZnIoT5II1QG0X/9
3INEtsZphKhoqpL6AiJ6CGlQ6wyHAe1Y3GKHdrmDiC4RdWE0nlwTGn4RagRjhh19
GGY8VifDjHFH3arf1IrNekU1ICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9
Pj8=
-----END PRIVATE KEY-----
```

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.3 }
  }
  OCTET_STRING {
    SEQUENCE {
      OCTET_STRING { `000102030405060708090a0b0c0d0e0f1011121314
15161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334
35363738393a3b3c3d3e3f` }
      OCTET_STRING { `f77b7f6b15c73fe2cc546b67fb774ca19b42cd463e
a9fbb984ca477a77b6c71087cbf051abe4736a9072c6e870c8311c55963f500a
3c7b1b8f2a58558f49c62527b6c594b5e7acb3bcf597273a5743517d151208bd
4aa61e75ba67b0bd594a994919627ac0a804d489e171336bc339f4666706e513
4412b366823d50318c8bf261ab120a28a04fec01cc15f2b71912cee54aa8eed8
54694b6ba886b5eb7661e6d56aac213cc1d814d592b395554fae74476d343711
63129bf864527250606cc21a53746b20997077bba155733b28a4e7fa07763995
24763eb481ceaa11366c3474a04685f40c3f08b0424f40bff949a0ac92704c3b
a0c6eb36f1f5b621d8bf2b6327beb57cd3facb94186fe3fc9ab0a1434bb291d2
c9bb70723057e2254059656f565919a32cf74579de89681cd2c5a935a52b4aaa
2d24cb5d5c9e20729ec5492ec36961efb8a28cbc00ac303523295f3d8036abc1
603307ce70d7848a35657a5687dd589927ea63731626abb26ec4e431b8eb6b3b
0bc1e82573ee73b1a021183183528108ae2eacaddb95b464a0b98469c319cc27
bfa01bc31054a68c05502b1662b879fe98a1711c3426f6436cb0214cea379ac3
a7e5fb60184a37c1da1eda61c6c39c1dd4e847845811f2a358a43731528536d4
a3291b04158c2c3dc641624882678bc7805f58a9d94c7104567846a2044e65ae
ce2a225372b6024799a5477d60237504aa5c0ac57bc70a3558c08c4de687ef13
02b4fcb5594413d22cb959bc31be423450403c6bc57dc411b3fefac1052ac4bb
162c44545a4ca80892657fa13a0b2c482ced629cc4999d969c593d4aadf073cc
3e3a458e78a8aa039408e652be93b20c8b42ec5b0e50239dac726052851a6d15
312ec39ed208b72209a577c6b2770112895749d5260e7dd446c0b0118c1000be
6801d2611fcf00792a9cc4f4b49922f9a2d4b9c8fa5a5d0d60506631a7e971ce
e840b08fa63c13729d7ea5aac70352a984cdb669331cba758fe87ec3931b3e31
61fcc747aa749424689feae14bf7c9a2ffba1302b212b80372d8e9049db69a3a
1261d0a2859a9b4d57899e0ba41607a1b67a7c0e12923689f8c6395377d970c7
490a4129611a1d05c3b7813bed945420723f7f9525a87793fafbbfca982e66bb
80681c83248a89da084c19882f48f31e7fc09093a49e9fd09691b021edf463af
c519b628538161183461l5fb0b882cc6482f3c5cbcc1c1894697e1239598b34b
2a9a7acd15244d0690c88194097a9beda585e87c437124624c210768e6215d37
6482653eb89947877c118d370c696a6ffcc1018ae413a08a8d0ffaa819945da7
a167c229913290cad1c80a369258762610ea253e62dc24226a30c892c12136c3
26f13f4446664712b0b90bc063b4028593cbde06cdc22289e240c7e296b59172
c1aeda8c99e0512d1a0163a942ea33148e6937c026029424b81b996b1df22ea0
623ec65c6bf093500cf3bf35374adc392035ca7c583b99685bca541a0807b163
acd0888be0385dea820da46e4dbb44d2e462c734b83a473fed1364273159257c
c259a8c5676c1c76d41d56b9907ec1c3599c9e8907403a27a705e3619b04b0ad
046e8ec8169c17b460d44c0c0c4464d044c946186bc725965083a892bcc495c0
540311ff9b3e5192c303d88f8ba46a901c782ef02388f1b2addab6a5350fc363
9700e3154337337e4a178d351cd2b56ee1f0bfea34aacfa33d2ec791e50752d4
d034cb1c951572caaa5c4d90947b6b175a6dd3c62a77bb8f7ac9ae24719b53c2
b120a2876986e217b72bd7cee44a7265b11cee1ab2261762b31a3738386969c0
825fb79452e652e1142fc73c9df6fba411795b4717922b29ba2d53abe5a8c0dc
c1601b096c96d7938fd5a68a8797c7b9477a86a472eb5da250cb2fec318d83c8
f43bbe8e11c35e377d349366c85c4382597f6fc27a0051c0fb00b02c01ca20f9
a427f172599477ca690cc1327e0f025f80ec338a80a159e308c12a27db1a7e1b
960a99d37dfc22872e51930f28c651ab221f53abaee20bad9a3eabcbab913251
bf135beb29617b5754333c4daadb2238341c2ad9378186280f6449440b784ba7
```

```
8f5dac44d8f65b3b7421950397c3913a2dd23ec6d1cb717b36a5fc95af191e27
8296948c1254ea86b4ec004b94c29450111191823b3514c9ac1ea3d9825ccb86
393a2dfb04654fa2192d37bfad1c497c6502eee5ca80a73bfce0baf5a54a8858
5a401397a3d232f426a7afb082bc21a44317090eaac7592c2ea88a653c4491ea
193931335f52e989a3c4cc56d9c553732d57c470fb41ab759b65d2d04445382f
cd9c4e344a1128fa9e11e04358e192ed014b23232a7ee2b22e23717f44111ee3
3575399c37646da9813ec9b212afe94e5dc5c2330a7294cc1f4234a6d3fbb4f1
685ab8892c04acb17cd1c170d7b0611b6a7176c794cc8c67f55fc923c2ad2031
00f365991882c30243d77813843b5ec7c964032263706092ecf00c7516be64e4
598ca4226c069bb5e67e4175cf2286c8dd5c488a6c5861f31baa0bd0269470e8
b551dd3bcd38c86c12f9cdb176c77dc8b6c02a701f478902c8553f694c0d8272
7b4c4a5c2c1041212aa1274808b82111b377ec75214e9b1978f76004d4139d98
613f4b8e98d20af7b534073a509a959b7a7564f9b40ca218bf61829320a85020
17954d328d7ac6c769ec29700756e7b0685b340d5e118059504a49a9a50a1019
8eb10a5784678eb427d7b4babb9552933b062897973e1318eaf0a0eac37584a6
5401b1703e042accd837531483f241cadcd1c1d378119e694429db199ac891e4
c5343757085bb3ae783667350c4458d97672e861e80b1d2679510ea3a6f2360c
77a46942c7a06a554d228080c84b47aef14db17620cb16c06ab30a1be4cda708
2be9f87e9c211c46916349a5ba8eaa5201c7294a3c0885b53b657452108825ec
646c90a04612324ee7d031afe5343132cbef67b6efb1a5ec2809b773538ce77b
3d8b04eb0b3c2256011e4c716c19a8ba0752bf71492117649f0615c3290fc29a
46fde4bd52db9286d603388244259c15a7ac2b640a60cc03376a5841a3fb8a47
3568fa9b1a267215f34c01697b0f0e627175d72105b7707c29b9e614bdc33a6f
6c818a95370b427882d7b476796a9ec6eb993274cd9b2391a82ba45e3393d2e9
ae9721ca9d6c1b988b5827713f90a6585de9433528c02b03ce10bb5f720138d0
fbb4c30c1266b918e52925dfe17b37f95d22bca54f475919ac859098c0f0d08a
c5875ef29b56fd141e6ef15f700a0b66f39595c588177373c4669b21bc071e4c
3aa5f0b4a31b6258f35da24ac3cd29c7f2092410c5078355b138fb53a6b9ae6e
0b9c08243e7baa45c47376eb8c7f13d4cf51aa736fa31540c9241f370da544bf
9f9c28d9a57e2f2a7ca95a4e4b466e641ab3bcc76adf1139d567a6f12b52f3a6
5e7ec0aae26bcaa8c55833b04e59998ebc9a1930fbb6d2233c53d2c1f8b9518e
3c2de73a19dee6b380a5b32971cf64e129fd6c1fa6e75d4a234501e966dd3a54
0af5c8f4f34a6b4a253ee28492566d5e67c6f55855fcb0506fb06c156744d9a0
3a31a26fa94cad14f157b7f303d07a69c773768fcb4d079c09059703a0c3a94d
e4b99ea3a2f16583d0f9170a3950db07b4f0bc30802927f9f7961b6259892636
a9502a2705303637799dd344da451c1cf7bf67840ceb3079ab8c6b8c1927f640
53c612450c45c9e603bc16666e596b3471e103b6f15447424d17022048111ffb
d37e1c670f64f14b8a7b32b94c1a49b45dd2fc38cd5289d910ad63602cf5e130
42c64ac6797b89fb551ad08e05a92d200cccb7e712ef23c9312cb350f029ab53
7e287347fd3075ac10906a783f1c6c07ccb88f41228c4be1c640f790b5c3a5d5
d3ca792495d74bc461562658c07ac600276b924ab5bc9be1f0494cb76f82f460
a7480972663381e169996061d799859ec54d4f5ca5c411c01db1597b16597766
9de13a928a34afbac258fea8c4764239c9421dc3119bf5b47699206978327b1c
5345ef746a7983841f056e2534100ab24d4e9abbd0b17c6a95bd4c3c0e40f69e
1612aceeb28b99086c95116e7204273893390bf46b899b36286b0ebf1947bb98
84f732ca27da82b19b5dc0cc7f8885714910888b2310c4f9319d410b34e6433b
9003e2176bb995257456106e8952163b8ba592530cc5aa0aeb43ad398fe9e97b
aa523d7a4431677c3d3af0719e475db85ca95af5089beabeb05b2faab4896ba6
0f81c88472a57b46a828826a0cdfb446f8189182d2bf5eac4ec1cc5deaf599c8
a13e48235406d17ffddc8344b6c66984a868aa92fa02227a086950eb0c8701ed
58dc628776b983882e117561349e5c131a7e116a0463861d7d18663c5627c38c
7147ddaadfd48acd7a4535202122232425262728292a2b2c2d2e2f3031323334
35363738393a3b3c3d3e3f` }
    }
  }
}
```

C.2. Example Public Keys

The following is the ML-KEM-512 public key corresponding to the private key in the previous section. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the public keys are the same.

```
-----BEGIN PUBLIC KEY-----
MIIDMjALBglghkgBZQMEBAEDggMhADmVgV5ZfRBDVc8pqlMzyTJRhp1bzb5IcST2
Ari2pmwWxHYWSK12XPXYAGtRXpBafwrAdrDGLvoygVPnylcBaZ8TBfHmvG+QsOSb
aTUSts6ZKouAFt38GmYsfj+WGcvYad13GvMIlszVkYrGy3dGbF53mZbWf/mqvJdQ
Pyx7fi0ADYZFD7GAfKTKvaRlgloxx4mht6SRqzhydl0yDQtxkg+iE8lAk0Frg7gS
Tmn2XmLLUADcw3qpoP/3OXDEdy81fSQYnKb1MFVowOI3ajdipoxgXlY8XSCVcuD8
dTLKKUcpU1VntfxBPF6HktJGRTbMgI+YrddGZPFBVm+QFqkKVBgpqYoEZM5BqLtE
wtT6PCwglGByjvFKGnxMm5jRIgO0zDUpFgqasteDj3/2tTrgWqMafWRrevpsRZMl
JqPDdVYZvplMIRwqMcBbNEeDbLIVC+GCna5rBMVTXP9Ubjkrp5dBFyD5JPSQpaxU
lfITVtVQt4KmTBaItrZVvMeEIZekNML2Vjtbfwmni8xIgjJ4NWHRb0y6tnVUAAUH
gVcMZmBLgXrRJSKUc26LAYYaS1p0UZuLb+UUiaUHI5Llh2JscTd2V10zgGocjicy
r5fCaA9RZmMxxOuLvAQxxPloMtrxs8RVKPuhU/bHixwZhwKUfM0zdyekb7U7oR3l
y0GRNGhZUWy2rXJADzzyCbI2rvNaWArIfrPjD6/WaXPKin3SZ1r0H3oXthQzzRr4
D3cIhp9mVIhJeYCxrBCgzctjagDthoGzXkKRJMqANQcluF+DperDpKPMFgCQPmUp
NWC5szblrw1SnawaBIEZMCy3qbzBELlIUb8CEX8ZncSFqFK3Rz8JuDGmgx1bVMC3
kNIlz2u5LZRiomzbM92lEjx6rw4moLg2Ve6ii/OoB0clAY/WuuS2Ac9huqtxp6PT
UZejQ+dLSicsEl1UCJZCbYW3lY07OKa6mH7DciXHtEzbEt3kU5tKsII2NoPwS/eg
nMXEHf6DChsWLgsyQzQ2LwhKFEZ3IzRLrdAA+NjFN8SPmY8FMHzr0e3guBw7xZoG
WhttY7Js
-----END PUBLIC KEY-----
```

```
SEQUENCE {
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.1 }
  }
  BIT_STRING { `00` `3995815e597d104355cf29aa5333c93251869d5bcdb
e487124f602b8b6a66c16c4761648ad765cf5d8006b515e905a7f0ac076b0c62
efa328153e7ca5701699f1305f1e6bc6f90b0e49b693512b6ce992a8b8016ddf
c1a662c7e3f9619cbd869dd771af30896ccd5918ac6cb77466c5e779996d67ff
9aabc97503f2c7b7e2d000d86450fb1807ca4cabda465825a31c789a1b7a491a
b3872765d320d0b71920fa213c94093416b83b8124e69f65e62cb5000dcc37aa
9a0fff73970c4772f357d24189ca6f5305568c0e2376a3762a68c605e563c5d2
09572e0fc7532ca294729535567b5fc413c5e8792d2464536cc808f98add7466
4f141566f9016a90a541829a98a0464ce41a8bb44c2d4fa3c2c209460728ef14
a1a7c4c9b98d12203b4cc3529160a9ab2d7838f7ff6b53ae05aa31a7d646b7af
a6c45932526a3c3755619be994c211c2a31c05b3447836cb2150be1829dae6b0
4c5535cff546e392ba797411720f924f490a5ac5495f21356d550b782a64c168
8b6b655bcc7842197a434c2f6563b5b7f09a78bcc488232783561d16f4cbab67
55400050781570c66604b817ad1252294736e8b01861a4b5a74519b8b6fe5148
9a5072392e587626c713776575d33806a1c8e2732af97c2680f51666331c4eb8
bbc0431c4f96832daf1b3c45528fba153f6c78b1c198702947ccd337727a46fb
53ba11de5cb4191346859516cb6ad72400f3cf209b236aef35a580ac87eb3e30
fafd66973ca8a7dd2675af41f7a17b61433cd1af80f7708869f665488497980b
1ac10a0cdcb636a00ed8681b35e429124ca80350725b85f83a5eac3a4a3cc160
0903e65293560b9b336e5af0d529dac1a048119302cb7a9bcc110b94851bf021
17f199dc485a852b7473f09b831a6831d5b54c0b790d225cf6bb92d9462a26cd
b33dda5123c7aaf0e26a0b83655eea28bf3a8074725018fd6bae4b601cf61baa
b71a7a3d35197a343e74b4a272c125d540896426d85b7958d3b38a6ba987ec37
225c7b44cdb12dde4539b4ab082363683f04bf7a09cc5c41dfe830a1b162e0b3
24334362f084a14467723344badd000f8d8c537c48f998f05307cebd1ede0b81
c3bc59a065a1b6d63b26c` }
}
```

The following is the ML-KEM-768 public key corresponding to the private key in the previous section. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the public keys are the same.

```
-----BEGIN PUBLIC KEY-----
MIIEsjALBglghkgBZQMEBAIDggShACmKoQ1CPI3aBp0CvFnmzfA6CWuLPaTKubgM
pKFJB2cszvHsT68jSgvFt+nUc/KzEzs7JqHRdctnp4BZGWmcAvdlMbmcX4kYBwS7
TKRTXFuJcmecZgoHxeUUuHAJyGLrj1FXaV77P8QKne9rgcHMAqJJrk8JStDZvTSF
wcHGgIBSCnyMYyAyzuc4FU5cUXbAfaVgJHdqQw/nbqz2ZaP3uDIQIhW8gvEJOcg1
VwQzao+sHYHkuwSFql18dNa1m75cXpcqDYusQRtVtdVVfNaAoaj3G064a8SMmgUJ
cxpUvZ1ykLJ5Y+Q3Lcmxmc/crAsBrNKKYjlREuTENkjWIsSMgjTQFEDozDdskn8j
pa/JrAR0xmInTkJFJchVLs47P+JlFt6QG8fVFb3olVjmJslcgLkzQvgBAATznmxs
lIccXjRMqzlmyDX5qWpZr9McQChrOLHBp4RwurlHUYk0RTzoZzapGfH1ptUQqG9U
VPw5gMtcdlvSvV97NrFBDWY1yM60fE3aDXaijqyTnHHDAkgEhmxxYmZYRCFjwsIh
F+UKzvzmN4qYVlIwKk7wws4Mxxa3eW4ray43d9+hrD2iWaMbWptTD4y2OKgaYqww
GEmrr5WnMBvaMAaJCb/bfmfbzLs4pVUaJbGjoPaFdIrVdT2IgPABbGJ0hhZjhMVX
H+I2WQA2TQODEeLYdds2ZoaTK17GAkMKNp6Hpu9cM4eGZXglvUwFes65I+sJNeaQ
XmO0ztf4CFenc91ksVDSZhLqmsEgUtsgF78YQ8y0sygbaQ3HKK36hcACgbjjwJKH
M1+Fa0/CiS9povV5Ia2gGRTECYhmLVd2lmKnhjUbm2ZJPat5WU2YbeIQDWW6D/Tq
WLgVONJKRDWiWPrCVASqf0H2WLE4UGXhWNy2ARVzJyD0BFmqrBXkBpU6kKxSmX0c
zQcAYO/GXbnmUzVEZ/rVbscTyG51QMQjrPJmn1L6b0rGiI2HHvPoR8ApqKr7uS4X
skqgebH0GbphdbRCr7EZCdSla3CgM1soc5IYqnyTSOLDwvPrPRWkHmQXwN2Uv+sh
QZsxGnuxOhgLvoMyGKmmsXRHzIXyJYWVh6cwdwSay8/UTQ8CVDjhXRU4Jw1Ybhv4
MZKpRZz2PA6XL4UpdnmDHs8SFQmFHLg0D28Qew+hoO/Rs2qBibwIXE9ct4TlU/Qb
kY+AOXzhlW94W+43fKmqi+aZitowwmt8PYxrVSVMyWIDsgxCruCsTh67QI5JqeP4
edCrB4XrcCVCXRMFoimcAV4SDRY7DhlJTOVyU9AkbRgnRcuBl6t0OLPBu3lyvsWj
BuujVnhVwBRpn+9lrlTHcKDYXBhADPZCrtxmB3e6SxOFAr1aeBL2IfhKSClrmN1D
IrbxWCi4qPDgCoukSlPDqLFDVxsHQKvVZ9rxzenHnCBLbV4lnRdmoxu7y05qBc9F
AhdrMBwcL0Ekd1AVe87IXoCbMKTWDXdHzdD1uZqoyCaYdRd5OqqAgKCxJKhVjfcr
vje3X07btr6CFtbGM/srIoDiURPYaV5DSBw+6zl+sZJQUim2eiAeqJPD4ssy2ovD
QvpN6gV4
-----END PUBLIC KEY-----
```

```
SEQUENCE {
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.2 }
  }
  BIT_STRING { `00` `298aa10d423c8dda069d02bc59e6cdf03a096b8b3da
4cab9b80ca4a14907672ccef1ec4faf234a0bc5b7e9d473f2b3133b3b26a1d17
5cb67a7805919699c02f76531b99c5f89180704bb4ca4535c5b8972679c660a0
7c5e514b87009c862eb8f5157695efb3fc40a9def6b81c1cc02a249ae4f094ad
0d9bd3485c1c1c68080520a7c8c632032cee738154e5c5176c07da56024776a4
30fe76eacf665a3f7b832102215bc82f10939c8355704336a8fac1d81e4bb048
5aa5d7c74d6b59bbe5c5e972a0d8bac411b55b5d5557cd680a1a8f71b4eb86bc
48c9a0509731a54bd9d7290b27963e4372dc9b199cfdcac0b01acd28a6239511
2e4c43648d622c48c8234d01440e8cc376c927f23a5afc9ac0474c662274e424
525c8552ece3b3fe26516de901bc7d515bde89558e626c95c80b93342f801000
4f39e6c6c94871c5e344cab3966c835f9a96a59afd31c40286b38b1c1a78470b
ab947518934453ce86736a919f1f5a6d510a86f5454fc3980cb5c765bd2bd5f7
b36b1410d6635c8ceb47c4dda0d76a28eac939c71c3024804866c71626658442
163c2c22117e50acefce6378a985652302a4ef0c2ce0cc716b7796e2b6b2e377
7dfa1ac3da259a31b5a9b530f8cb638a81a62ac301849abaf95a7301bda30068
909bfdb7e67dbccbb38a5551a25b1a3a0f685748ad5753d8880f0016c6274861
66384c5571fe2365900364d038311e2d875db366686932b5ec602430a369e87a
6ef5c338786657825bd4c057aceb923eb0935e6905e63b4ced7f80857a773dd6
4b150d26612ea9ac12052db2017bf1843ccb4b3281b690dc728adfa85c00281b
8e3c09287335f856b4fc2892f69a2f57921ada01914c40988662d57769662a78
6351b9b66493dab79594d986de2100d65ba0ff4ea58b81538d24a4435a258fac
25404aa7f41f658b1385065e158dcb60115732720f40459aaac15e406953a90a
c52997d1ccd070060efc65db9e653354467fad56ec713c86e7540c423acf2669
f52fa6f4ac6888d871ef3e847c029a8aafbb92e17b24aa079b1f419ba6175b44
2afb11909d4a56b70a0335b28739218aa7c9348e2c3c2f3eb3d15a41e6417c0d
d94bfeb21419b311a7bb13a180bbe833218a9a6b17447cc85f225859587a7307
7049acbcfd44d0f025438e15d1538270d586e1bf83192a9459cf63c0e972f852
97679831ecf121509851cb8340f6f107b0fa1a0efd1b36a8189bc085c4f5cb78
4e553f41b918f80397ce1956f785bee377ca9aa8be6998ada30c26b7c3d8c6b5
5254cc96203b20c42aee0ac4e1ebb408e49a9e3f879d0ab0785eb7025425d130
5a2299c015e120d163b0e19494ce57253d0246d182745cb8197ab7438b3c1bb7
972bec5a306eba3567855c014699fef65ae54c770a0d85c18400cf642aedc660
777ba4b138502bd5a7812f621f84a48296b98dd4322b6f15828b8a8f0e00a8ba
44a53c3a8b143571b0740abd567daf1cde9c79c204b6d5e259d1766a31bbbcb4
e6a05cf4502176b301c1c2f41247750157bcec85e809b30a4d60d7747cdd0f5b
99aa8c826987517793aaa8080a0b124a8558df72bbe37b75f4edbb6be8216d6c
633fb2b2280e25113d8695e43481c3eeb397eb192505229b67a201ea893c3e2c
b32da8bc342fa4dea0578` }
}
```

The following is the ML-KEM-1024 public key corresponding to the private key in the previous section. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the public keys are the same.

```
-----BEGIN PUBLIC KEY-----
MIIGMjALBglghkgBZQMEBAMDggYhAEuUwpRQERGRgjs1FMmsHqPZglzLhjk6LfsE
ZU+iGS03v60cSXxlAu7lyoCnO/zguvWlSohYWkATl6PSMvQmp6+wgrwhpEMXCQ6q
x1ksLqiKZTxEkeoZOTEzX1LpiaPEzFbZxVNzLVfEcPtBq3WbZdLQREU4L82cTjRK
ESj6nhHgQ1jhku0BSyMjKn7isi4jcX9EER7jNXU5nDdkbamBPsmyEq/pTl3FwjMK
cpTMH0I0ptP7tPFoWriJLASssXzRwXDXsGEbanF2x5TMjGf1X8kjwq0gMQDzZZkY
gsMCQ9d4E4Q7XsfJZAMiY3BgkuzwDHUWvmTkWYykImwGm7XmfkF1zyKGyN1cSIps
WGHzG6oL0CaUcOi1Ud07zTjIbBL5zbF2x33ItsAqcB9HiQLIVT9pTA2CcntMSlws
EEEhKqEnSAi4IRGzd+x1IU6bGXj3YATUE52YYT9LjpjSCve1NAc6UJqVm3p1ZPm0
DKIYv2GCkyCoUCAXlU0yjXrGx2nsKXAHVuewaFs0DV4RgFlQSkmppQoQGY6xCleE
Z460J9e0uruVUpM7BiiXlz4TGOrwoOrDdYSmVAGxcD4EKszYN1MUg/JBytzRwdN4
EZ5pRCnbGZrIkeTFNDdXCFuzrng2ZzUMRFjZdnLoYegLHSZ5UQ6jpvI2DHekaULH
oGpVTSKAgMhLR67xTbF2IMsWwGqzChvkzacIK+n4fpwhHEaRY0mluo6qUgHHKUo8
CIW1O2V0UhCIJexkbJCgRhIyTufQMa/lNDEyy+9ntu+xpewoCbdzU4znez2LBOsL
PCJWAR5McWwZqLoHUr9xSSEXZJ8GFcMpD8KaRv3kvVLbkobWAziCRCWcFaesK2QK
YMwDN2pYQaP7ikc1aPqbGiZyFfNMAWl7Dw5icXXXIQW3cHwpueYUvcM6b2yBipU3
C0J4gte0dnlqnsbrmTJ0zZsjkagrpF4zk9Lprpchyp1sG5iLWCdxP5CmWF3pQzUo
wCsDzhC7X3IBOND7tMMMEma5GOUpJd/hezf5XSK8pU9HWRmshZCYwPDQisWHXvKb
Vv0UHm7xX3AKC2bzlZXFiBdzc8RmmyG8Bx5MOqXwtKMbYljzXaJKw80px/IJJBDF
B4NVsTj7U6a5rm4LnAgkPnuqRcRzduuMfxPUz1Gqc2+jFUDJJB83DaVEv5+cKNml
fi8qfKlaTktGbmQas7zHat8ROdVnpvErUvOmXn7AquJryqjFWDOwTlmZjryaGTD7
ttIjPFPSwfi5UY48Lec6Gd7ms4Clsylxz2ThKf1sH6bnXUojRQHpZt06VAr1yPTz
SmtKJT7ihJJWbV5nxvVYVfywUG+wbBVnRNmgOjGib6lMrRTxV7fzA9B6acdzdo/L
TQecCQWXA6DDqU3kuZ6jovFlg9D5Fwo5UNsHtPC8MIApJ/n3lhtiWYkmNqlQKicF
MDY3eZ3TRNpFHBz3v2eEDOsweauMa4wZJ/ZAU8YSRQxFyeYDvBZmbllrNHHhA7bx
VEdCTRcCIEgRH/vTfhxnD2TxS4p7MrlMGkm0XdL8OM1SidkQrWNgLPXhMELGSsZ5
e4n7VRrQjgWpLSAMzLfnEu8jyTEss1DwKatTfihzR/0wdawQkGp4PxxsB8y4j0Ei
jEvhxkD3kLXDpdXTynkkldd LxGFWJljAesYAJ2uSSrW8m+HwSUy3b4L0YKdICXJm
M4HhaZlgYdeZhZ7FTU9cpcQRwB2xWXsWWXdmneE6koo0r7rCWP6oxHZCOclCHcMR
m/W0dpkgaXgyexxTRe90anmDhB8FbiU0EAqyTU6au9CxfGqVvUw8DkD2nhYSrO6y
i5kIbJURbnIEJziTOQv0a4mbNihrDr8ZR7uYhPcyyifagrGbXcDMf4iFcUkQiIsj
EMT5MZ1BCzTmQzuQA+IXa7mVJXRWEG6JUhY7i6WSUwzFqgrrQ605j+npe6pSPXpE
MWd8PTrwcZ5HXbhcqVr1CJvqvrBbL6q0iWumD4HIhHKle0aoKIJqDN+0RvgYkYLS
v16sTsHMXer1mcihPkgjVAbRf/3cg0S2xmmEqGiqkvoCInoIaVDrDIcB7VjcYod2
uYOILhF1
-----END PUBLIC KEY-----
```

```
SEQUENCE {
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.3 }
  }
  BIT_STRING { `00` `4b94c29450111191823b3514c9ac1ea3d9825ccb863
93a2dfb04654fa2192d37bfad1c497c6502eee5ca80a73bfce0baf5a54a88585
a401397a3d232f426a7afb082bc21a44317090eaac7592c2ea88a653c4491ea1
93931335f52e989a3c4cc56d9c553732d57c470fb41ab759b65d2d04445382fc
d9c4e344a1128fa9e11e04358e192ed014b23232a7ee2b22e23717f44111ee33
575399c37646da9813ec9b212afe94e5dc5c2330a7294cc1f4234a6d3fbb4f16
85ab8892c04acb17cd1c170d7b0611b6a7176c794cc8c67f55fc923c2ad20310
0f365991882c30243d77813843b5ec7c964032263706092ecf00c7516be64e45
98ca4226c069bb5e67e4175cf2286c8dd5c488a6c5861f31baa0bd0269470e8b
551dd3bcd38c86c12f9cdb176c77dc8b6c02a701f478902c8553f694c0d82727
b4c4a5c2c1041212aa1274808b82111b377ec75214e9b1978f76004d4139d986
13f4b8e98d20af7b534073a509a959b7a7564f9b40ca218bf61829320a850201
7954d328d7ac6c769ec29700756e7b0685b340d5e118059504a49a9a50a10198
eb10a5784678eb427d7b4babb9552933b062897973e1318eaf0a0eac37584a65
401b1703e042accd837531483f241cadcd1c1d378119e694429db199ac891e4c
5343757085bb3ae783667350c4458d97672e861e80b1d2679510ea3a6f2360c7
7a46942c7a06a554d228080c84b47aef14db17620cb16c06ab30a1be4cda7082
be9f87e9c211c46916349a5ba8eaa5201c7294a3c0885b53b657452108825ec6
46c90a04612324ee7d031afe5343132cbef67b6efb1a5ec2809b773538ce77b3
d8b04eb0b3c2256011e4c716c19a8ba0752bf71492117649f0615c3290fc29a4
6fde4bd52db9286d603388244259c15a7ac2b640a60cc03376a5841a3fb8a473
568fa9b1a267215f34c01697b0f0e627175d72105b7707c29b9e614bdc33a6f6
c818a95370b427882d7b476796a9ec6eb993274cd9b2391a82ba45e3393d2e9a
e9721ca9d6c1b988b5827713f90a6585de9433528c02b03ce10bb5f720138d0f
bb4c30c1266b918e52925dfe17b37f95d22bca54f475919ac859098c0f0d08ac
5875ef29b56fd141e6ef15f700a0b66f39595c588177373c4669b21bc071e4c3
aa5f0b4a31b6258f35da24ac3cd29c7f2092410c5078355b138fb53a6b9ae6e0
b9c08243e7baa45c47376eb8c7f13d4cf51aa736fa31540c9241f370da544bf9
f9c28d9a57e2f2a7ca95a4e4b466e641ab3bcc76adf1139d567a6f12b52f3a65
e7ec0aae26bcaa8c55833b04e59998ebc9a1930fbb6d2233c53d2c1f8b9518e3
c2de73a19dee6b380a5b32971cf64e129fd6c1fa6e75d4a234501e966dd3a540
af5c8f4f34a6b4a253ee28492566d5e67c6f55855fcb0506fb06c156744d9a03
a31a26fa94cad14f157b7f303d07a69c773768fcb4d079c09059703a0c3a94de
4b99ea3a2f16583d0f9170a3950db07b4f0bc30802927f9f7961b6259892636a
9502a2705303637799dd344da451c1cf7bf67840ceb3079ab8c6b8c1927f6405
3c612450c45c9e603bc16666e596b3471e103b6f15447424d17022048111ffbd
37e1c670f64f14b8a7b32b94c1a49b45dd2fc38cd5289d910ad63602cf5e1304
2c64ac6797b89fb551ad08e05a92d200cccb7e712ef23c9312cb350f029ab537
e287347fd3075ac10906a783f1c6c07ccb88f41228c4be1c640f790b5c3a5d5d
3ca792495d74bc461562658c07ac600276b924ab5bc9be1f0494cb76f82f460a
7480972663381e169996061d799859ec54d4f5ca5c411c01db1597b165977669
de13a928a34afbac258fea8c4764239c9421dc3119bf5b47699206978327b1c5
345ef746a7983841f056e2534100ab24d4e9abbd0b17c6a95bd4c3c0e40f69e1
612aceeb28b99086c95116e7204273893390bf46b899b36286b0ebf1947bb988
4f732ca27da82b19b5dc0cc7f8885714910888b2310c4f9319d410b34e6433b9
003e2176bb995257456106e8952163b8ba592530cc5aa0aeb43ad398fe9e97ba
a523d7a4431677c3d3af0719e475db85ca95af5089beabeb05b2faab4896ba60
f81c88472a57b46a828826a0cdfb446f8189182d2bf5eac4ec1cc5deaf599c8a
13e48235406d17ffddc8344b6c66984a868aa92fa02227a086950eb0c8701ed5
8dc628776b983882e1175` }
}
```

C.3. Example Certificates

The following is the ML-KEM-512 certificate corresponding to the public key in the previous section signed with the ML-DSA-44 private key from [RFC9881]. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the certificates are the same.

```
-----BEGIN CERTIFICATE-----
MIINpDCCBBqgAwIBAgIUFZ/+byL9XMQsUk32/V4o0N44808wCwYJYIZIAWUDBAMR
MCIxDTALBgNVBAoTBElFVEYxETAPBgNVBAMTCExBTVBTIFdHMB4XDTIwMDIwMzA0
MzIxMFoXDTQwMDEyOTA0MzIxMFowIjENMAsGA1UEChMESUVURjERMA8GA1UEAxMI
TEFNUFMgV0cwggMyMAsGCWCGSAFlAwQEAQOCAyEAOZWBXll9EENVzymqUzPJMlGG
nVvNvkhxJPYCuLambBbEdhZIrXZc9dgAa1FekFp/CsB2sMYu+jKBU+fKVwFpnxMF
8ea8b5Cw5JtpNRK2zpkqi4AW3fwaZix+P5YZy9hp3Xca8wiWzNWRisbLd0ZsXneZ
ltZ/+aq8l1A/LHt+LQANhkUPsYB8pMq9pGWCWjHHiaG3pJGrOHJ2XTINC3GSD6IT
yUCTQWuDuBJOafZeYstQANzDeqmg//c5cMR3LzV9JBicpvUwVWjA4jdqN2KmjGBe
VjxdIJVy4Px1MsopRylTVWe1/EE8XoeS0kZFNsyAj5it10Zk8UFWb5AWqQpUGCmp
igRkzkGou0TC1Po8LCCUYHKO8UoafEybmNEiA7TMNSkWCpqy14OPf/a1OuBaoxp9
ZGt6+mxFkyUmo8N1Vhm+mUwhHCoxwFs0R4NsshUL4YKdrmsExVNc/1RuOSunl0EX
IPkk9JClrFSV8hNW1VC3gqZMFoi2tlW8x4Qhl6Q0wvZWO1t/CaeLzEiCMng1YdFv
TLq2dVQABQeBVwxmYEuBetElIpRzbosBhhpLWnRRm4tv5RSJpQcjkuWHYmxxN3ZX
XTOAahyOJzKvl8JoD1FmYzHE64u8BDHE+Wgy2vGzxFUo+6FT9seLHBmHApR8zTN3
J6RvtTuhHeXLQZE0aFlRbLatckAPPPIJsjau81pYCsh+s+MPr9Zpc8qKfdJnWvQf
ehe2FDPNGvgPdwiGn2ZUiEl5gLGsEKDNy2NqAO2GgbNeQpEkyoA1ByW4X4Ol6sOk
o8wWAJA+ZSk1YLmzNuWvDVKdrBoEgRkwLLepvMEQuUhRvwIRfxmdxIWoUrdHPwm4
MaaDHVtUwLeQ0iXPa7ktlGKibNsz3aUSPHqvDiaguDZV7qKL86gHRyUBj9a65LYB
z2G6q3Gno9NRl6ND50tKJywSXVQIlkJthbeVjTs4prqYfsNyJce0TNsS3eRTm0qw
gjY2g/BL96CcxcQd/oMKGxYuCzJDNDYvCEoURncjNEut0AD42MU3xI+ZjwUwfOvR
7eC4HDvFmgZaG21jsmyjUjBQMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUDsWS
pZcefo2geKhuRnTy+xH26NcwHwYDVR0jBBgwFoAUMpoHsfq7SPUqMJ8RoYmPhI4j
Iv8wCwYJYIZIAWUDBAMRA4IJdQDcV8LA/De8Ss6UL3tMcHXKc0iTXaBPPLyoCimW
KG/BhZ299qdyg6Qv/hWMxXfuQLvBIJUiE9boIUvDJH1Bv5q+wBXDM4Pcb585a972
fB7Lj7rTYwGezp4QRGsn4bMOUHtOS/9MaD9LAw8XlEDSl69KgN+jN+Cak+PS1Q3O
u+TpeM2fo304+3vTfHlNiePSNOqkd1pzs2nwVIbQGIWctpF1rIHC7NJ/XOO3ZsN3
Cr758OLyAotCdGCRnj16Fhxh1rJ976b6y+Yo96CDMgl22lYPJoihlBekuKc4ugkE
g4vJEwAtPlMoaogn7XJcWkKIhGKp1M7nG9KvgQxCRvIfRURuDyHaiOAkOayK+Hp6
4AV02pbYX/w1X9bW1KOeId42EUQpF2iFu3ilOJi1JmMFyMP8lZZYq/8fPv3KGZPF
YJpd6yaA7ReIQaNiFgCMqx7nw/Zti7sa2a5dor3YqYRjZ8UlJUuYUKxNDde/u46W
mIEGSYcynpOiEYbyeWmXW4ye7qhT1Q7bmFPV8Mjzn3rXytzUzUZfrK8j9cHxAozY
sF7RDuBmauliYfV1jaroCcHrohVTnSSiSMQKV4q6HjKPIpf4qENs4SVh9xkWXdbB
OaiGgFhsI+sxlDGPRwbKrj6gVcbyFuJIPRL1LylJ2qFXzpzHyfAS3fHFvgv+S0AJ
DnfNk3OcT7G9jQhESQOkTXA4LqxPI+0c6asvauXlICnN8RdOjraY4+DQL8cYidEi
SAnXsOKNSzj+b225zdPvfBB/4eJTtV7VdnQOhETJErofxEWbpA8zobl/+bu2smdY
Pg1a83hwVo+HxfkSz1iHW9WT9+iwhnm28RqzLdmmzZGJSfgEFkADriwXUEr+LIkX
0xeMGvyXxdxv9S6Y6y+n0Al0ql0tzGviVoDqA0xNLU+Mupou5ftDTJj7U1oxIUHj
HlFeE06+JRoTPbDcl+cBil31SlxuZ1u7cOE33nbPOw0jWDXeA8M5uE3aMQah5VRf
tZXmdijH4zEN1/++Q5oJAF1SCTsnTkZ0lk3ZlIfpO0H1sJpINzLlBO04dLlQx2Nc
NFIExuPsVO7kW1rDLqkh8srBKrdUa/8ngD3kppXW7iaBhSnUE0N6lrwi5g/fJbNU
H0W7r0b31u0KDQ8cNKlK8PZL5pu/ulJTGZ5Dz4HORwVt2aXQojZfGQ0rashKxes8
F+Ewgse7NUAt3HqX94+0SWpfpNCVlZknK5XfhZJV08XVZ2TkTDoJ6aBLqua/a5Xg
jWTwroAJuB84jx2B1eCeYxjt+3cEaB274XU++H6m5kP/1QtJ3L1r545NaRQAylZF
MwCtCTVyAavhrTcrQwhl8rVGAKOlXaCfHSln8y9u26qMHeL9BIP7JeMeZxCYQQ5b
QxN0WvGmK11W6XG2CTc0qQ0RdUOvfrXTfl5A+I6DS4T2Z26APgkoq2JSQihO3JEg
S7zknl2NoAummhweGU/qSPzX+4/KlxwcCCs8mD8ZkkwhdB5poU4uTES/eCO+rrm3
wxLmiIcv2RwNdN8bRkxm35SQCCfc6riit4AxkaRKz5b27FWedfkH9bOgQaQGxm/v
5IwGHsFGeQFJyV1pNvo0aB9vvMTL3VZOsoXooxrdlc0kv7jJ9Q6eF8ZAFYXvxnaS
D+/OsH1b1+6WCVZIDRzRsMauvaifYUZNMQQ/CKSkDkFPjBDY5Xca9yZkGl+S+Pzz
7ODu6y3lvvUk+V6sPKEAS4ejZOocriV75SPfz0WlRZoljJXOm3tKCo6L2e56ntVs
hRiIBaLG5stQf2EihTSZUf21zNjb15E7KcdbTtr8TE0iJAuVYxBtNRWsVhExOMO/
QqXWnHL015pv8Dubwt6iDr8ObCDNOItPtszlNjCz4yN51aGTrHGZ0CJcbcUWqxOm
W1wrQmnYWUaz1eDahmbnowXshqI8RcGqvzUlZ0/g6nEbAJZgbk7jozC1VlwOKMM4
erhkw5mrrpicX3cvP3wl3JyhB6vbAfK4XQH3CfrnK12BhpgG0+9V5DKxTL02f+5m
ckJI9cZqSYx8rhlDlNbR33kSOY0Ba2RwvmMxhdypd38l5S8oSwTRu5eJ4VrrSeeM
wiW3gIxLA+o+SD2iFKyafsWLeu+Axx5/HlIVB+g82dGKkZrrESEvO9LpdlaS+AMW
```

```
9BccbDD2SGE2UZKlK4zx2QwYvnFG/ZDRjmvQV0dQOxiy0j2l7WHmbedlTTUUd5FU
0cfSG+cJHnToa/VRU4mDHvFpnV+AF0dA1s0oemhN5vOqhDzHnKasFFpUDH88mS7K
gbXELYiHTQEB/s/Hr0crjwVQQCbJFe4bBJzhcnwuOcdNUKLmF7MidvoyKYYu20oE
P6F0/RoDwS2FW3RyrKeSzlLWnuarfTq84iMaPgKrOl8XNfaSgGRsG3kxGe0s3rVs
iwzaO8THoCLp6WpEebfucmSCMXtKfVG/28u/dvQkz1D0oqTcWqhQiDLqZI3HjdDr
io44DARVGKAsEvq75Jq91GXP+1R8yejpP1lZU4onX1i0E8DMuVEU85JN+kFXbS83
6nZHmYhgwj93IvetNiK5cJs2M19LnJj5GrONmPMizoXCIBjzDx0MO/3CoRF5achF
p598lYloyvlS1VYhwmLrpFmz0BB9OEepvdq0ZX11XM532I6WIF4lAUh0YEx1FInO
XJ74LC2uMxa92W6nceJAjiraJKhi4VnURhPa7MUt/2oA5WY8zzmVGn94UlPsEmPj
/nl7vXBVLb9Nojt9AkIO637bT+1wszCvOH8nelnzNDsCBi9B8+mdgzizEN08UKSk
dCaNbCB86LVeo+umyY5abmgr2NOI7XaSTqWMs7ezemR5AkIUka35LgVIKvZw2WEz
G3KxZImSviV+XMsakqGTdXof7k1usEcmbJ/EJLi9ecaxMZKuLjT9sFtNo8uvE/m1
1pf4bGnGXgBERGpZsqnm+JNxDDTbD1WntdPpyeF8/6iXd/eNiHboV830Olj0dXJ4
YbTrQBcWbfUeZ8+8gGJ0bgshMtPCrOdYVMAfWfcu7DyFi0tQdtS1pmo5Co+OwLxe
IyKgwlIYOghCE3r6SBCrx0+sTP0sixV5Refu2JIBkjoywPavmK3+109l1F0BkzST
fQ1pAwENGx0oLVFdZHB1f4CSlZaiq8Te7AtOfX6Qtba4w8bP1+j2FSVCWGt4goSv
s7TAwcrR1drv9BRiaH2qytnr8PcAAAAAAAAAAAAAAAAAAAAAFSM2QA==
-----END CERTIFICATE-----
```

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER { 2 }
    }
    INTEGER { `159ffe6f22fd5cc42c524df6fd5e28d0de38f34f` }
    SEQUENCE {
      OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
      SET {
        SEQUENCE {
          # commonName
          OBJECT_IDENTIFIER { 2.5.4.3 }
          PrintableString { "LAMPS WG" }
        }
      }
    }
    SEQUENCE {
      UTCTime { "200203043210Z" }
      UTCTime { "400129043210Z" }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
      SET {
        SEQUENCE {
          # commonName
          OBJECT_IDENTIFIER { 2.5.4.3 }
          PrintableString { "LAMPS WG" }
        }
      }
    }
    SEQUENCE {
      SEQUENCE {
        OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.1 }
      }
      BIT_STRING { `00` `3995815e597d104355cf29aa5333c93251869d5
bcdbe487124f602b8b6a66c16c4761648ad765cf5d8006b515e905a7f0ac076b
0c62efa328153e7ca5701699f1305f1e6bc6f90b0e49b693512b6ce992a8b801
6ddfc1a662c7e3f9619cbd869dd771af30896ccd5918ac6cb77466c5e779996d
67ff9aabc97503f2c7b7e2d000d86450fb1807ca4cabda465825a31c789a1b7a
491ab3872765d320d0b71920fa213c94093416b83b8124e69f65e62cb5000dcc
37aa9a0fff73970c4772f357d24189ca6f5305568c0e2376a3762a68c605e563
c5d209572e0fc7532ca294729535567b5fc413c5e8792d2464536cc808f98add
```

```
74664f141566f9016a90a541829a98a0464ce41a8bb44c2d4fa3c2c209460728
ef14a1a7c4c9b98d12203b4cc3529160a9ab2d7838f7ff6b53ae05aa31a7d646
b7afa6c45932526a3c3755619be994c211c2a31c05b3447836cb2150be1829da
e6b04c5535cff546e392ba797411720f924f490a5ac5495f21356d550b782a64
c1688b6b655bcc7842197a434c2f6563b5b7f09a78bcc488232783561d16f4cb
ab6755400050781570c66604b817ad1252294736e8b01861a4b5a74519b8b6fe
51489a5072392e587626c713776575d33806a1c8e2732af97c2680f51666331c
4eb8bbc0431c4f96832daf1b3c45528fba153f6c78b1c198702947ccd337727a
46fb53ba11de5cb4191346859516cb6ad72400f3cf209b236aef35a580ac87eb
3e30fafd66973ca8a7dd2675af41f7a17b61433cd1af80f7708869f665488497
980b1ac10a0cdcb636a00ed8681b35e429124ca80350725b85f83a5eac3a4a3c
c1600903e65293560b9b336e5af0d529dac1a048119302cb7a9bcc110b94851b
f02117f199dc485a852b7473f09b831a6831d5b54c0b790d225cf6bb92d9462a
26cdb33dda5123c7aaf0e26a0b83655eea28bf3a8074725018fd6bae4b601cf6
1baab71a7a3d35197a343e74b4a272c125d540896426d85b7958d3b38a6ba987
ec37225c7b44cdb12dde4539b4ab082363683f04bf7a09cc5c41dfe830a1b162
e0b324334362f084a14467723344badd000f8d8c537c48f998f05307cebd1ede
0b81c3bc59a065a1b6d63b26c` }
    }
    [3] {
      SEQUENCE {
        SEQUENCE {
          # keyUsage
          OBJECT_IDENTIFIER { 2.5.29.15 }
          BOOLEAN { TRUE }
          OCTET_STRING {
            BIT_STRING { b`001` }
          }
        }
        SEQUENCE {
          # subjectKeyIdentifier
          OBJECT_IDENTIFIER { 2.5.29.14 }
          OCTET_STRING {
            OCTET_STRING { `0ec592a5971e7e8da078a86e4674f2fb11f6
e8d7` }
          }
        }
        SEQUENCE {
          # authorityKeyIdentifier
          OBJECT_IDENTIFIER { 2.5.29.35 }
          OCTET_STRING {
            SEQUENCE {
              [0 PRIMITIVE] { `329a07b1fabb48f52a309f11a1898f848
e2322ff` }
            }
          }
        }
      }
    }
  }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
  }
  BIT_STRING { `00` `dc57c2c0fc37bc4ace942f7b4c7075ca7348935da04
f3cbca80a2996286fc1859dbdf6a77283a42ffe158cc577ee40bbc120952213d
6e8214bc3247d41bf9abec015c33383dc6f9f396bdef67c1ecb8fbad363019ec
e9e10446b27e1b30e507b4e4bff4c683f4b030f179440d297af4a80dfa337e09
a93e3d2d50dcebbe4e978cd9fa37d38fb7bd37c794d89e3d234eaa4775a73b36
```

```
9f05486d018859cb69175ac81c2ecd27f5ce3b766c3770abef9f0e2f2028b427
460919e3d7a161c61d6b27defa6facbe628f7a083320976da560f2688a19417a
4b8a738ba0904838bc913002d3e53286a8827ed725c5a42888462a9d4cee71bd
2af810c4246f21f45446e0f21da88e02439ac8af87a7ae00574da96d85ffc355
fd6d6d4a39e21de36114429176885bb78a53898b5266305c8c3fc959658abff1
f3efdca1993c5609a5deb2680ed178841a36216008cab1ee7c3f66d8bbb1ad9a
e5da2bdd8a9846367c525254b9850ac4d0dd7bfbb8e969881064987329e93a21
186f27969975b8c9eeea853d50edb9853d5f0c8f39f7ad7cadcd4cd465facaf2
3f5c1f1028cd8b05ed10ee0666ae96261f5758daae809c1eba215539d24a248c
40a578aba1e328f2297f8a8436ce12561f719165dd6c139a88680586c23eb319
4318f4706caae3ea055c6f216e2483d12f52f2949daa157ce9cc7c9f012ddf1c
5be0bfe4b40090e77cd93739c4fb1bd8d08444903a44d70382eac4f23ed1ce9a
b2f6ae5e52029cdf1174e8eb698e3e0d02fc71889d1224809d7b0e28d4b38fe6
f6db9cdd3ef7c107fe1e253b55ed576740e8444c912ba1fc4459ba40f33a1b97
ff9bbb6b267583e0d5af37870568f87c5f912cf58875bd593f7e8b08679b6f11
ab32dd9a6cd918949f804164003ae2c17504afe2c8917d3178c1afc97c5dc6ff
52e98eb2fa7d00974aa5d2dcc6be25680ea034c4d2d4f8cba9a2ee5fb434c98f
b535a312141e31e515e134ebe251a133db0dc97e7018a5df54a5c6e675bbb70e
137de76cf3b0d235835de03c339b84dda3106a1e5545fb595e67628c7e3310dd
7ffbe439a09005d52093b274e4674964dd99487e93b41f5b09a483732e504ed3
874b950c7635c345204c6e3ec54eee45b5ac32ea921f2cac12ab7546bff27803
de4a695d6ee26818529d413437a96bc22e60fdf25b3541f45bbaf46f7d6ed0a0
d0f1c34a94af0f64be69bbfba5253199e43cf81ce47056dd9a5d0a2365f190d2
b6ac84ac5eb3c17e13082c7bb35402ddc7a97f78fb4496a5fa4d0959599272b9
5df859255d3c5d56764e44c3a09e9a04baae6bf6b95e08d64f0ae8009b81f388
f1d81d5e09e6318edfb7704681dbbe1753ef87ea6e643ffd50b49dcbd6be78e4
d691400ca56453300ad09357201abe1ad372b430865f2b54600a3a55da09f1d2
967f32f6edbaa8c1de2fd0483fb25e31e671098410e5b4313745af1a62b5d56e
971b6093734a90d117543af7eb5d37e5e40f88e834b84f6676e803e0928ab625
242284edc91204bbce49e5d8da00ba69a1c1e194fea48fcd7fb8fca971c1c082
b3c983f19924c21741e69a14e2e4c44bf7823beaeb9b7c312e688872fd91c0d7
4df1b464c66df94900827dceab8a2b7803191a44acf96f6ec559e75f907f5b3a
041a406c66fefe48c061ec146790149c95d6936fa34681f6fbcc4cbdd564eb28
5e8a31add95cd24bfb8c9f50e9e17c6401585efc676920fefceb07d5bd7ee960
956480d1cd1b0c6aebda89f61464d31043f08a4a40e414f8c10d8e5771af7266
41a5f92f8fcf3ece0eeeb2de5bef524f95eac3ca1004b87a364ea1cae257be52
3dfcf45a5459a258c95ce9b7b4a0a8e8bd9ee7a9ed56c85188805a2c6e6cb507
f612285349951fdb5ccd8dbd7913b29c75b4edafc4c4d22240b9563106d3515a
c56113138c3bf42a5d69c72f4d79a6ff03b9bc2dea20ebf0e6c20cd388b4fb6c
ce53630b3e32379d5a193ac7199d0225c6dc516ab13a65b5c2b4269d85946b3d
5e0da8666e7a305ec86a23c45c1aabf3525674fe0ea711b0096606e4ee3a330b
5565c0e28c3387ab864c399abae989c5f772f3f7c25dc9ca107abdb01f2b85d0
1f709fae72b5d81869806d3ef55e432b14cbd367fee66724248f5c66a498c7ca
e194394d6d1df7912398d016b6470be633185dca9777f25e52f284b04d1bb978
9e15aeb49e78cc225b7808c4b03ea3e483da214ac9a7ec58b7aef80c71e7f1e5
21507e83cd9d18a919aeb11212f3bd2e9765692f80316f4171c6c30f64861365
192a52b8cf1d90c18be7146fd90d18e6bd05747503b18b2d23da5ed61e66de76
54d3514779154d1c7d21be7091e74e86bf5515389831ef1699d5f80174740d6c
d287a684de6f3aa843cc79ca6ac145a540c7f3c992eca81b5c42d88874d0101f
ecfc7af472b8f05504026c915ee1b049ce1727c2e39c74d50a2e617b32276fa3
229862edb4a043fa174fd1a03c12d855b7472aca792ce52d69ee6ab7d3abce22
31a3e02ab3a5f1735f69280646c1b793119ed2cdeb56c8b0cda3bc4c7a022e9e
96a4479b7ee726482317b4a7d51bfdbcbbf76f424cf50f4a2a4dc5aa8508832e
a648dc78dd0eb8a8e380c045518a02c12fabbe49abdd465cffb547cc9e8e93f5
959538a275f58b413c0ccb95114f3924dfa41576d2f37ea7647998860c23f772
2f7ad3622b9709b36335f4b9c98f91ab38d98f322ce85c22018f30f1d0c3bfdc
2a1117969c845a79f7c958968caf952d55621c262eba459b3d0107d3847a9bdd
ab4657d755cce77d88e96205e25014874604c751489ce5c9ef82c2dae3316bdd
```

```
96ea771e2408e2ada24a862e159d44613daecc52dff6a00e5663ccf39951a7f7
85253ec1263e3fe797bbd70552dbf4da23b7d02420eeb7edb4fed70b330af387
f277a59f3343b02062f41f3e99d8338b310dd3c50a4a474268d6c207ce8b55ea
3eba6c98e5a6e682bd8d388ed76924ea58cb3b7b37a647902421491adf92e054
82af670d961331b72b1648992be257e5ccb1a92a193757a1fee4d6eb047266c9
fc424b8bd79c6b13192ae2e34fdb05b4da3cbaf13f9b5d697f86c69c65e00444
46a59b2a9e6f893710c34db0f55a7b5d3e9c9e17cffa89777f78d8876e857cdf
43a58f475727861b4eb4017166df51e67cfbc8062746e0b2132d3c2ace75854c
01f59f72eec3c858b4b5076d4b5a66a390a8f8ec0bc5e2322a0c252183a08421
37afa4810abc74fac4cfd2c8b157945e7eed89201923a32c0f6af98adfed74f6
5d45d019334937d0d6903010d1b1d282d515d6470757f80929596a2abc4deec0
b4e7d7e90b5b6b8c3c6cfd7e8f6152542586b788284afb3b4c0c1cad1d5daeff
41462687daacad9ebf0f70000000000000000000000000000015233640` }
}
```

The following is the ML-KEM-768 certificate corresponding to the public key in the previous section signed with the ML-DSA-65 private key from [RFC9881]. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the certificates are the same.

```
-----BEGIN CERTIFICATE-----
MIISnTCCBZqgAwIBAgIUFZ/+byL9XMQsUk32/V4o0N44808wCwYJYIZIAWUDBAMS
MCIxDTALBgNVBAoTBElFVEYxETAPBgNVBAMTCExBTVBTIFdHMB4XDTIwMDIwMzA0
MzIxMFoXDTQwMDEyOTA0MzIxMFowIjENMAsGA1UEChMESUVURjERMA8GA1UEAxMI
TEFNUFMgV0cwggSyMAsGCWCGSAFlAwQEAgOCBKEAKYqhDUI8jdoGnQK8WebN8DoJ
a4s9pMq5uAykoUkHZyzO8exPryNKC8W36dRz8rMTOzsmodF1y2engFkZaZwC92Ux
uZxfiRgHBLtMpFNcW4lyZ5xmCgfF5RS4cAnIYuuPUVdpXvs/xAqd72uBwcwCokmu
TwlK0Nm9NIXBwcaAgFIKfIxjIDLO5zgVTlxRdsB9pWAkd2pDD+durPZlo/e4MhAi
FbyC8Qk5yDVXBDNqj6wdgeS7BIWqXXx01rWbvlxelyoNi6xBG1W11VV81oChqPcb
TrhrxIyaBQlzGlS9nXKQsnlj5DctybGZz9ysCwGs0opiOVES5MQ2SNYixIyCNNAU
QOjMN2ySfyOlr8msBHTGYidOQkUlyFUuzjs/4mUW3pAbx9UVveiVWOYmyVyAuTNC
+AEABPOebGyUhxxeNEyrOWbINfmpalmv0xxAKGs4scGnhHC6uUdRiTRFPOhnNqkZ
8fWm1RCob1RU/DmAy1x2W9K9X3s2sUENZjXIzrR8TdoNdqKOrJOcccMCSASGbHFi
ZlhEIWPCwiEX5QrO/OY3iphWUjAqTvDCzgzHFrd5bitrLjd336GsPaJZoxtam1MP
jLY4qBpirDAYSauvlacwG9owBokJv9t+Z9vMuzilVRolsaOg9oV0itV1PYiA8AFs
YnSGFmOExVcf4jZZADZNA4MR4th12zZmhpMrXsYCQwo2noem71wzh4ZleCW9TAV6
zrkj6wk15pBeY7TO1/gIV6dz3WSxUNJmEuqawSBS2yAXvxhDzLSzKBtpDccorfqF
wAKBuOPAkoczX4VrT8KJL2mi9XkhraAZFMQJiGYtV3aWYqeGNRubZkk9q3lZTZht
4hANZboP9OpYuBU40kpENaJY+sJUBKp/QfZYsThQZeFY3LYBFXMnIPQEWaqsFeQG
lTqQrFKZfRzNBwBg78ZdueZTNURn+tVuxxPIbnVAxCOs8mafUvpvSsaIjYce8+hH
wCmoqvu5LheySqB5sfQZumF1tEKvsRkJ1KVrcKAzWyhzkhiqfJNI4sPC8+s9FaQe
ZBfA3ZS/6yFBmzEae7E6GAu+gzIYqaaxdEfMhfIlhZWHpzB3BJrLz9RNDwJUOOFd
FTgnDVhuG/gxkqlFnPY8DpcvhSl2eYMezxIVCYUcuDQPbxB7D6Gg79GzaoGJvAhc
T1y3hOVT9BuRj4A5fOGVb3hb7jd8qaqL5pmK2jDCa3w9jGtVJUzJYgOyDEKu4KxO
HrtAjkmp4/h50KsHhetwJUJdEwWiKZwBXhINFjsOGUlM5XJT0CRtGCdFy4GXq3Q4
s8G7eXK+xaMG66NWeFXAFGmf72WuVMdwoNhcGEAM9kKu3GYHd7pLE4UCvVp4EvYh
+EpIKWuY3UMitvFYKLio8OAKi6RKU8OosUNXGwdAq9Vn2vHN6cecIEttXiWdF2aj
G7vLTmoFz0UCF2swHBwvQSR3UBV7zshegJswpNYNd0fN0PW5mqjIJph1F3k6qoCA
oLEkqFWN9yu+N7dfTtu2voIW1sYz+ysigOJRE9hpXkNIHD7rOX6xklBSKbZ6IB6o
k8PiyzLai8NC+k3qBXijUjBQMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUQry1
oWf6MwRJYS29gYcFanUY94cwHwYDVR0jBBgwFoAUGwVj480zRhScjJ688jsKTlqQ
DuowCwYJYIZIAWUDBAMSA4IM7gDya3x1P7gnc/43+gwI1bbPyLFhkbPTUdbp8wrj
S6y1IBreYKD5+OSNsHx1sQ+vThL20hYZunwSyzM3ud/UFZJcpTYE3hLIqWYYlFfD
KXc9OUYfL4xYtwY9L7NuV9GitoPOZqXGxC8uFBcCPtgXnKKm+2VcUcp3WAdgnW6T
ohOKPc1JMN1ElgywyAeUKGyVu26WhQxltO/tD9NyWjjx88GJQB0EAhd+CUx2gJoG
71QWYaHKKKY2Ap66VvNY8EwfG8xHfd1agWXl+dR7OldlYHAflSrZyczt/m97CBfT
gz0q59YrtpgFC6A8f27DOns49/pcvFrFvnqbrB6olgn4g95w9a+zTjK+0LEOLuZ7
coxK7G52UM4+zm89rgiV6Lf57E+gq6PIg6VJQzWeNlii8vK2c4D9+ru9DWxrQYIp
lO011cW7q37cw1UenD7ouG6zd0Rgq5LIaoeQgwngLFoAEGl213xGJ7nFmPKweq6m
jEWArh8WFdQS8xaArVxh16Qhijpk9aIMRXP8kv7x8ORXIOQkfE2zVQnnjMt7zTO7
YbKY0ujPJwEga8UsP95V3ApLLNc4S9EIm/URSL9i1eA5Yf0/7qZub4512LN3tH9f
QGr96wtIGKmMmD/M/ON86GXWRMvQW8w3DSgi73RuM5WH+IVZ8kRgdwx6ff/Flbd3
PXXmxziQd6JdOIDn2JeTaEfZd6MxJ8juknEQTotIzOhSNJ08zcQqkCu0OQIcNMaK
vzbzEDP+VbiIGxL6n7Y3JRnp+ACA2pWbB5lUl7Ex2OMCO9zrGAL5f98+5RFId7Mz
2gQOah/y2FFHVw72TB3XFzyPuThiTSeXW/sQUMkvGXcb6cgUA25Umuq+tvKuktLt
H7Rrj13+g+cSgkDMKpHPx2aVTaZ3hchDqQhplLu8adVkjaXldrrU/le3JYUwZCsL
4ZCbWfEZeRgq7rVirSSEm8U1psE5mFZ0LqewLz87FKIYmTFVY25Xew+T4O/BC35P
k3xp5pP99ShC+0o0YyStQziC2PmNNzjm6xHGYAYas7gyfpqVz93ooN5lg9uMTnLs
SdAD/jsumB9nLGFPJ9tNYmL6AbnlBZiBwg2oSuIlSUBTCMFmbt+4QvsgeqjHx7nQ
Z+oc8x7D3tSiVcf+sTICFRO6br2FF2PHDlTvKudW6ziFLsYWkkNK4K68p4GO983H
R8pd0uXyhICMHSgriODpHmbTvyV2Vzh9+AKCt8PLiixeKzBL0Q6A2lquMk+cJP8f
Q4QJL/TbUJ1B0yy1GVy6oToID+zM7ZUwI85VEqBnwWqA/UU3pggJg1CjItGrgM9x
fGkPVjPZ9IjadgB0tgfHZ97gW6YiocaXmu6rrYF6rxYkWDaww9Uq8CQsrv7YRb2Q
OeLCem1jyo/98YeMxVxBXZtAqMfgbAd2f0pa9Y3u84OBvdLNIyHXDWgmIhHG4uy1
6JO6OxdU9qoEyw3s/8hCAQbQZfEHTsTTbR+ij35PCZHfYOZiFUZozMCSslHSrbIc
+hmjd5slvDnbuxwCnhJX5dOnWRQtWzbUg4kJFwSven+MCQ6d8CS6RZbEHOwvCD4B
qIHUaR1+lT9bW8kynPMZk6GdKCvyAEVnf9ka4mIiJrzycqBwwdOTlfKsESviE2yd
```

```
9YyBF3adS6eOKiuE71HJ7h1gnpxQJLtrC0q4y4Rmh9arwDb5nQ7QrF4mG+jUMFLL
sR8jd+/QHGmpZ5qhUfxyti2qQOteGjDlXtA2guahqCSX71GUpXLTY3VYisnWzoM/
xdoMhKy+maEJ1mOeyrPnmOXh/mxLWpwcN42QH3u+iktGa66LKNwk5P4+1aSjV62k
6jWvWAF6bSgr7hhffyt8Nr70HklYQg3NZpo5ivpzYzCJ6r5dm0yuL6pxJg098RYu
3CfyjyOHB/FVhx+e9ADQ1I/NbkGyDvIj/AqD0TLbG9AyXU968SP3AEmedi3IZLGO
EtA373hLW/rnVCa15+3rcLcQACfJwv8VwbIpeZSBh7fZ26KcR2Rj0vV7Qn786ZbK
6aG9SlHpRCsV6hiQdsCYr1k+X0a7wrRr80fHrCd07vqG/hl4dbFu/IhMeQ243K6n
3FTnHclYDoKaUQCmlOfgp9/3djAb/rOVwiPMoXkVS8JAJPa3gazejnITG+W209T1
ukA+AYvpAR2qd1ysBjZnZxbEswAWKk2z6O/056/F1AQaIVRgKBIYzuwE1lLNLNV4
OgLUZ791oEfjVx/1QqhgLBd3pY/U3535OlM8lCURjdMo0EuxsrIY3AxDQHdnSTsw
EzE6ZDFLCFEKEEw/iVJul8qKUtFuoqsQMX51A2L1AosbaPzawY6RU2/BWFqew2A4
K5Wm5YDwilHYlpBy3+F1ByNUI5+ayXMFwQi0dqpD6QXpuRm38Ze+qy2YKtaAljeJ
xfcJjdIrx2LiAvKGHO6yMb+JVGliBZr38wS5fJX3sZY1gWE3uG82qMo9ft5ovmoE
ZMMb4GSBfX8WTyncPmO/t7/wv+JbVP/Hx0yv/7WWVY1pPoC6boEtY4YrIHve7lxv
S8NSixJ8ESLzffJZTGc9D/tDM6FRHobUZItSoFZwHpGGbfOrOD1Q8mWaVj2OxXh7
nlWrKX+WSZX59sR+Ez4eHejnNXFT2FGWrUfK05+0YooTn/4jZE/u8X9tSf/HJkKb
NyKoDeJ9lwf60iJFbQNf1zXVc0U3I9y833CvUz3V1XKZoZ6AQXcc5NW+lNpj0CPD
3Z3tjwYGIdpQopZW6qYk66yektO780fYKdqG3W+0QvFmV25DjKx0DcNXDgs6AXn8
Dehq70ogiRaqisQuXE0+Qy9MdXwx/9ytN6m3Th25dNg7PPKuPugbFAg3ev+RuPv0
a3BwLozRyAIp5VGuG7Iu0E80kAXQixkN3YQpcWhXTsJBfsrFyUVJLejYgX0Xmkj+
+2pf4+9IRf2nAwqcYRZylt1N0/x2/vVy7pz57NIoWGsQ9Vy8HcgK/rus1PWRhN36
ic5IoCgko/ctVpKZfX3Rhhm4qjWXEgzsiMj8/RhbKC2m/MobcCNCQUK26fwetMri
Sq62x3XTyaI4HU5kCQUdXcuaa13UvmFxNKqhKqJSYopCOk+2tP49qewc4dPKebbc
qYF8kVhpJB5cwifB3ieaRjU66PaTX2AwZNa0k3XrXmql9pQ6h6K7QJ+DucAJn1n0
FH0XElKBX2ebUC9luqUjHRKeJW/FDZEijj9ez8ssGMD4Elcut/qM1hNh1GB0hDN1
x8yE3KNwHJfs9bQxphoRYnw78rINuwUU9Yild15XLEa9CzUvwmOcwQXku/X4aVPv
0qsUnF414LGeySk/8XUcJewV/u9EdIm1XvL77iifRaV9CeRu4yEYPn737QCW7j+F
Ex4WrWbokI54n+SeBuvZ6Jfs/12lPjFVIsD9MM+YaIVA2846cVJ0Idc+o7MGXK5e
6p/2PjlRktXrYPVHrIRP3Ouc2js0IBEK6STubJFbSnAHTSRQqmcxph1BXLf6A1dd
7dt7R7tKbepBxWKYq5liC9Rqq2oatrbMARH59EWscoEAzZP0L0rio1KPknvM0ZBI
ibiszAb7sqkh7Hq7EoicirdXTjItOitSQWshGiuiKVqCE0jANM7lFhfO63XsFo7G
GuOuqQKDJTx+8F5qHs2s7yC4uZDDmMx+pZ36J6Mae5CcyeXVQDgkBZdU47tVCeB0
7WqaXFAdbJTKVwEkG3PSg9qp8SoDL6c9eQye/Hk1Z/vmf1tYHoPg8iJpx0iD/dEk
/73iGZEAr7U7NM/ldcDxCXO1mfBNSmixq6zp5jJEH9TCo+usT0dQKGW0N1zPyDrH
0qHWt1xSO0G6FPK4zTyEY/84z+ecXFvxxynXLYYCm5kEhK06PYiVY5OKOaBe9vma
qS66MzHNpfjNblJfG9O/HeiJLJ3vV7/F3U/kfxs3PStrMgoXMRt1KBrmIBB3F1xE
5WCaEONmuYSmJMZPbdkB+7rEsbC4v1cnyE0800BAGNYpVyPyTYbfPBthNEmYsBIV
KSYuVQ1259Ju69UE22dqnXnorsCZCXWEpmcmRO8/Gvb0Y7OYFWltDeGLFJRbJ4av
5dtNm2ZH53uLPi3aYsZU9cyfxh7AcbKSfQlRSVKCj6o0BQ3ZvmBPPOvcsUbUU5oo
FgCPOse60fvnKhEEO9zEnuU3RObcQPkDQRmMQ3OhibiGzOEOaU6PCEVJ3P+N+lJm
/0M2lNaYgaks0kmKoYdEmpLdmdGSCCB6HJ+nIIlwodrM0wK9SZUqkd+kFoGvGf7+
XkFvmlJbGn4UCaaHOUaDZsFBMiAcMAAcPv9FIM+A9NIjbC2imd0TJf+tLf6tLA6P
gFHtzTF9yuL8FSI+bbLr9go0PG2SnqPM4RQha4s2OoOvtNkQI2Smvu0AAAAAAAAA
AAAAAAAAAAAAAAAFDBUZHyU=
-----END CERTIFICATE-----
```

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER { 2 }
    }
    INTEGER { `159ffe6f22fd5cc42c524df6fd5e28d0de38f34f` }
    SEQUENCE {
      OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
      SET {
        SEQUENCE {
          # commonName
          OBJECT_IDENTIFIER { 2.5.4.3 }
          PrintableString { "LAMPS WG" }
        }
      }
    }
    SEQUENCE {
      UTCTime { "200203043210Z" }
      UTCTime { "400129043210Z" }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
      SET {
        SEQUENCE {
          # commonName
          OBJECT_IDENTIFIER { 2.5.4.3 }
          PrintableString { "LAMPS WG" }
        }
      }
    }
    SEQUENCE {
      SEQUENCE {
        OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.2 }
      }
      BIT_STRING { `00` `298aa10d423c8dda069d02bc59e6cdf03a096b8
b3da4cab9b80ca4a14907672ccef1ec4faf234a0bc5b7e9d473f2b3133b3b26a
1d175cb67a7805919699c02f76531b99c5f89180704bb4ca4535c5b8972679c6
60a07c5e514b87009c862eb8f5157695efb3fc40a9def6b81c1cc02a249ae4f0
94ad0d9bd3485c1c1c68080520a7c8c632032cee738154e5c5176c07da560247
76a430fe76eacf665a3f7b832102215bc82f10939c8355704336a8fac1d81e4b
b0485aa5d7c74d6b59bbe5c5e972a0d8bac411b55b5d5557cd680a1a8f71b4eb
86bc48c9a0509731a54bd9d7290b27963e4372dc9b199cfdcac0b01acd28a623
```

```
95112e4c43648d622c48c8234d01440e8cc376c927f23a5afc9ac0474c662274
e424525c8552ece3b3fe26516de901bc7d515bde89558e626c95c80b93342f80
10004f39e6c6c94871c5e344cab3966c835f9a96a59afd31c40286b38b1c1a78
470bab947518934453ce86736a919f1f5a6d510a86f5454fc3980cb5c765bd2b
d5f7b36b1410d6635c8ceb47c4dda0d76a28eac939c71c3024804866c7162665
8442163c2c22117e50acefce6378a985652302a4ef0c2ce0cc716b7796e2b6b2
e3777dfa1ac3da259a31b5a9b530f8cb638a81a62ac301849abaf95a7301bda3
0068909bfdb7e67dbccbb38a5551a25b1a3a0f685748ad5753d8880f0016c627
486166384c5571fe2365900364d038311e2d875db366686932b5ec602430a369
e87a6ef5c338786657825bd4c057aceb923eb0935e6905e63b4ced7f80857a77
3dd64b150d26612ea9ac12052db2017bf1843ccb4b3281b690dc728adfa85c00
281b8e3c09287335f856b4fc2892f69a2f57921ada01914c40988662d5776966
2a786351b9b66493dab79594d986de2100d65ba0ff4ea58b81538d24a4435a25
8fac25404aa7f41f658b1385065e158dcb60115732720f40459aaac15e406953
a90ac52997d1ccd070060efc65db9e653354467fad56ec713c86e7540c423acf
2669f52fa6f4ac6888d871ef3e847c029a8aafbb92e17b24aa079b1f419ba617
5b442afb11909d4a56b70a0335b28739218aa7c9348e2c3c2f3eb3d15a41e641
7c0dd94bfeb21419b311a7bb13a180bbe833218a9a6b17447cc85f225859587a
73077049acbcfd44d0f025438e15d1538270d586e1bf83192a9459cf63c0e972
f85297679831ecf121509851cb8340f6f107b0fa1a0efd1b36a8189bc085c4f5
cb784e553f41b918f80397ce1956f785bee377ca9aa8be6998ada30c26b7c3d8
c6b55254cc96203b20c42aee0ac4e1ebb408e49a9e3f879d0ab0785eb7025425
d1305a2299c015e120d163b0e19494ce57253d0246d182745cb8197ab7438b3c
1bb7972bec5a306eba3567855c014699fef65ae54c770a0d85c18400cf642aed
c660777ba4b138502bd5a7812f621f84a48296b98dd4322b6f15828b8a8f0e00
a8ba44a53c3a8b143571b0740abd567daf1cde9c79c204b6d5e259d1766a31bb
bcb4e6a05cf4502176b301c1c2f41247750157bcec85e809b30a4d60d7747cdd
0f5b99aa8c826987517793aaa8080a0b124a8558df72bbe37b75f4edbb6be821
6d6c633fb2b2280e25113d8695e43481c3eeb397eb192505229b67a201ea893c
3e2cb32da8bc342fa4dea0578` }
    }
    [3] {
      SEQUENCE {
        SEQUENCE {
          # keyUsage
          OBJECT_IDENTIFIER { 2.5.29.15 }
          BOOLEAN { TRUE }
          OCTET_STRING {
            BIT_STRING { b`001` }
          }
        }
        SEQUENCE {
          # subjectKeyIdentifier
          OBJECT_IDENTIFIER { 2.5.29.14 }
          OCTET_STRING {
            OCTET_STRING { `42bcb5a167fa330449612dbd8187056a7518
f787` }
          }
        }
        SEQUENCE {
          # authorityKeyIdentifier
          OBJECT_IDENTIFIER { 2.5.29.35 }
          OCTET_STRING {
            SEQUENCE {
              [0 PRIMITIVE] { `1b0563e3cd3346149c8c9ebcf23b0a4e5
a900eea` }
            }
          }
```

```
        }
      }
    }
  }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
  }
  BIT_STRING { `00` `f26b7c753fb82773fe37fa0c08d5b6cfc8b16191b3d
351d6e9f30ae34bacb5201ade60a0f9f8e48db07c75b10faf4e12f6d21619ba7
c12cb3337b9dfd415925ca53604de12c8a966189457c329773d39461f2f8c58b
7063d2fb36e57d1a2b683ce66a5c6c42f2e1417023ed8179ca2a6fb655c51ca7
75807609d6e93a2138a3dcd4930dd44960cb0c80794286c95bb6e96850c65b4e
fed0fd3725a38f1f3c189401d0402177e094c76809a06ef541661a1ca28a6360
29eba56f358f04c1f1bcc477ddd5a8165e5f9d47b3a576560701f952ad9c9cce
dfe6f7b0817d3833d2ae7d62bb698050ba03c7f6ec33a7b38f7fa5cbc5ac5be7
a9bac1ea89609f883de70f5afb34e32bed0b10e2ee67b728c4aec6e7650ce3ec
e6f3dae0895e8b7f9ec4fa0aba3c883a54943359e3658a2f2f2b67380fdfabbb
d0d6c6b41822994ed35d5c5bbab7edcc3551e9c3ee8b86eb3774460ab92c86a8
7908309e02c5a00106976d77c4627b9c598f2b07aaea68c4580ae1f1615d412f
31680ad5c61d7a4218a3a64f5a20c4573fc92fef1f0e45720e4247c4db35509e
78ccb7bcd33bb61b298d2e8cf2701206bc52c3fde55dc0a4b2cd7384bd1089bf
51148bf62d5e03961fd3feea66e6f8e75d8b377b47f5f406afdeb0b4818a98c9
83fccfce37ce865d644cbd05bcc370d2822ef746e339587f88559f24460770c7
a7dffc595b7773d75e6c7389077a25d3880e7d897936847d977a33127c8ee927
1104e8b48cce852349d3ccdc42a902bb439021c34c68abf36f31033fe55b8881
b12fa9fb6372519e9f80080da959b07995497b131d8e3023bdceb1802f97fdf3
ee5114877b333da040e6a1ff2d85147570ef64c1dd7173c8fb938624d27975bf
b1050c92f19771be9c814036e549aeabeb6f2ae92d2ed1fb46b8f5dfe83e7128
240cc2a91cfc766954da67785c843a9086994bbbc69d5648da5e576bad4fe57b
7258530642b0be1909b59f11979182aeeb562ad24849bc535a6c1399856742ea
7b02f3f3b14a218993155636e577b0f93e0efc10b7e4f937c69e693fdf52842f
b4a346324ad433882d8f98d3738e6eb11c660061ab3b8327e9a95cfdde8a0de6
583db8c4e72ec49d003fe3b2e981f672c614f27db4d6262fa01b9e5059881c20
da84ae22549405308c1666edfb842fb207aa8c7c7b9d067ea1cf31ec3ded4a25
5c7feb132021513ba6ebd851763c70e54ef2ae756eb38852ec61692434ae0aeb
ca7818ef7cdc747ca5dd2e5f284808c1d282b88e0e91e66d3bf257657387df80
282b7c3cb8a2c5e2b304bd10e80da5aae324f9c24ff1f4384092ff4db509d41d
32cb5195cbaa13a080feccced953023ce5512a067c16a80fd4537a608098350a
322d1ab80cf717c690f5633d9f488da760074b607c767dee05ba622a1c6979ae
eabad817aaf16245836b0c3d52af0242caefed845bd9039e2c27a6d63ca8ffdf
1878cc55c415d9b40a8c7e06c07767f4a5af58deef38381bdd2cd2321d70d682
62211c6e2ecb5e893ba3b1754f6aa04cb0decffc8420106d065f1074ec4d36d1
fa28f7e4f0991df60e662154668ccc092b251d2adb21cfa19a3779b25bc39dbb
b1c029e1257e5d3a759142d5b36d48389091704af7a7f8c090e9df024ba4596c
41cec2f083e01a881d4691d7e953f5b5bc9329cf31993a19d282bf20045677fd
91ae2622226bcf272a070c1d39395f2ac112be2136c9df58c8117769d4ba78e2
a2b84ef51c9ee1d609e9c5024bb6b0b4ab8cb846687d6abc036f99d0ed0ac5e2
61be8d43052cbb11f2377efd01c69a9679aa151fc72b62daa40eb5e1a30e55ed
03682e6a1a82497ef5194a572d36375588ac9d6ce833fc5da0c84acbe99a109d
6639ecab3e798e5e1fe6c4b5a9c1c378d901f7bbe8a4b466bae8b28dc24e4fe3
ed5a4a357ada4ea35af58017a6d282bee185f7f2b7c36bef41e4958420dcd669
a398afa73633089eabe5d9b4cae2faa71260d3df1162edc27f28f238707f1558
71f9ef400d0d48fcd6e41b20ef223fc0a83d132db1bd0325d4f7af123f700499
e762dc864b18e12d037ef784b5bfae75426b5e7edeb70b7100027c9c2ff15c1b
22979948187b7d9dba29c476463d2f57b427efce996cae9a1bd4a51e9442b15e
a189076c098af593e5f46bbc2b46bf347c7ac2774eefa86fe197875b16efc884
c790db8dcaea7dc54e71dc9580e829a5100a694e7e0a7dff776301bfeb395c22
3cca179154bc24024f6b781acde8e72131be5b6d3d4f5ba403e018be9011daa7
```

```
75cac0636676716c4b300162a4db3e8eff4e7afc5d4041a215460281218ceec0
4d652cd2cd5783a02d467bf75a047e3571ff542a8602c1777a58fd4df9df93a5
33c9425118dd328d04bb1b2b218dc0c43407767493b3013313a64314b08510a1
04c3f89526e97ca8a52d16ea2ab10317e750362f5028b1b68fcdac18e91536fc
1585a9ec360382b95a6e580f08a51d8969072dfe175072354239f9ac97305c10
8b476aa43e905e9b919b7f197beab2d982ad680963789c5f7098dd22bc762e20
2f2861ceeb231bf89546962059af7f304b97c95f7b19635816137b86f36a8ca3
d7ede68be6a0464c31be064817d7f164f29dc3e63bfb7bff0bfe25b54ffc7c74
cafffb596558d693e80ba6e812d63862b207bdeee5c6f4bc3528b127c1122f37
df2594c673d0ffb4333a1511e86d4648b52a056701e91866df3ab383d50f2659
a563d8ec5787b9e55ab297f964995f9f6c47e133e1e1de8e7357153d85196ad4
7cad39fb4628a139ffe23644feef17f6d49ffc726429b3722a80de27d9707fad
222456d035fd735d573453723dcbcdf70af533dd5d57299a19e8041771ce4d5b
e94da63d023c3dd9ded8f060621da50a29656eaa624ebac9e92d3bbf347d829d
a86dd6fb442f166576e438cac740dc3570e0b3a0179fc0de86aef4a208916aa8
ac42e5c4d3e432f4c757c31ffdcad37a9b74e1db974d83b3cf2ae3ee81b14083
77aff91b8fbf46b70702e8cd1c80229e551ae1bb22ed04f349005d08b190ddd8
4297168574ec2417ecac5c945492de8d8817d179a48fefb6a5fe3ef4845fda70
30a9c61167296dd4dd3fc76fef572ee9cf9ecd228586b10f55cbc1dc80afebba
cd4f59184ddfa89ce48a02824a3f72d5692997d7dd18619b8aa3597120cec88c
8fcfd185b282da6fcca1b7023424142b6e9fc1eb4cae24aaeb6c775d3c9a2381
d4e6409051d5dcb9a6b5dd4be617134aaa12aa252628a423a4fb6b4fe3da9ec1
ce1d3ca79b6dca9817c915869241e5cc227c1de279a46353ae8f6935f603064d
6b49375eb5e6aa5f6943a87a2bb409f83b9c0099f59f4147d171252815f679b5
02f65baa5231d129e256fc50d91228e3f5ecfcb2c18c0f812572eb7fa8cd6136
1d46074843375c7cc84dca3701c97ecf5b431a61a11627c3bf2b20dbb0514f58
8a5775e572c46bd0b352fc2639cc105e4bbf5f86953efd2ab149c5e35e0b19ec
9293ff1751c25ec15feef447489b55ef2fbee289f45a57d09e46ee321183e7ef
7ed0096ee3f85131e16ad66e8908e789fe49e06ebd9e897ecff5da53e315522c
0fd30cf98688540dbce3a71527421d73ea3b3065cae5eea9ff63e395192d5eb6
0f547ac844fdceb9cda3b3420110ae924ee6c915b4a70074d2450aa6731a61d4
15cb7fa03575deddb7b47bb4a6dea41c56298ab99620bd46aab6a1ab6b6cc011
1f9f445ac728100cd93f42f4ae2a3528f927bccd1904889b8accc06fbb2a921e
c7abb12889c8ab7574e322d3a2b52416b211a2ba2295a821348c034cee51617c
eeb75ec168ec61ae3aea90283253c7ef05e6a1ecdacef20b8b990c398cc7ea59
dfa27a31a7b909cc9e5d5403824059754e3bb5509e074ed6a9a5c501d6c94ca5
701241b73d283daa9f12a032fa73d790c9efc793567fbe67f5b581e83e0f2226
9c74883fdd124ffbde2199100afb53b34cfe575c0f10973b599f04d4a68b1aba
ce9e632441fd4c2a3ebac4f47502865b4375ccfc83ac7d2a1d6b75c523b41ba1
4f2b8cd3c8463ff38cfe79c5c5bf1c729d72d86029b990484ad3a3d889563938
a39a05ef6f99aa92eba3331cda5f8cd6e525f1bd3bf1de8892c9def57bfc5dd4
fe47f1b373d2b6b320a17311b75281ae6201077175c44e5609a10e366b984a62
4c64f6dd901fbbac4b1b0b8bf5727c84d3cd3404018d6295723f24d86df3c1b6
1344998b0121529262e550d76e7d26eebd504db676a9d79e8aec099097584a66
72644ef3f1af6f463b39815696d0de18b14945b2786afe5db4d9b6647e77b8b3
e2dda62c654f5cc9fc61ec071b2927d09514952828faa34050dd9be604f3cebd
cb146d4539a2816008f3ac7bad1fbe72a11043bdcc49ee53744e6dc40f903411
98c4373a189b886cce10e694e8f084549dcff8dfa5266ff433694d69881a92cd
2498aa187449a92dd99d19208207a1c9fa7208970a1daccd302bd49952a91dfa
41681af19fefe5e416f9a525b1a7e1409a68739468366c14132201c30001c3ef
f4520cf80f4d2236c2da299dd1325ffad2dfead2c0e8f8051edcd317dcae2fc1
5223e6db2ebf60a343c6d929ea3cce114216b8b363a83afb4d9102364a6beed0
00000000000000000000000000000000000050c15191f25` }
}
```

The following is the ML-KEM-1024 certificate corresponding to the public key in the previous section signed with the ML-DSA-87 private key from [RFC9881]. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the certificates are the same.

```
-----BEGIN CERTIFICATE-----
MIIZQzCCBxqgAwIBAgIUFZ/+byL9XMQsUk32/V4o0N44808wCwYJYIZIAWUDBAMT
MCIxDTALBgNVBAoTBElFVEYxETAPBgNVBAMTCExBTVBTIFdHMB4XDTIwMDIwMzA0
MzIxMFoXDTQwMDEyOTA0MzIxMFowIjENMAsGA1UEChMESUVURjERMA8GA1UEAxMI
TEFNUFMgV0cwggYyMAsGCWCGSAFlAwQEAwOCBiEAS5TClFAREZGCOzUUyaweo9mC
XMuGOTot+wRlT6IZLTe/rRxJfGUC7uXKgKc7/OC69aVKiFhaQBOXo9Iy9Canr7CC
vCGkQxcJDqrHWSwuqIplPESR6hk5MTNfUumJo8TMVtnFU3MtV8Rw+0GrdZtl0tBE
RTgvzZxONEoRKPqeEeBDWOGS7QFLIyMqfuKyLiNxf0QRHuM1dTmcN2RtqYE+ybIS
r+lOXcXCMwpylMwfQjSm0/u08WhauIksBKyxfNHBcNewYRtqcXbHlMyMZ/VfySPC
rSAxAPNlmRiCwwJD13gThDtex8lkAyJjcGCS7PAMdRa+ZORZjKQibAabteZ+QXXP
IobI3VxIimxYYfMbqgvQJpRw6LVR3TvNOMhsEvnNsXbHfci2wCpwH0eJAshVP2lM
DYJye0xKXCwQQSEqoSdICLghEbN37HUhTpsZePdgBNQTnZhhP0uOmNIK97U0BzpQ
mpWbenVk+bQMohi/YYKTIKhQIBeVTTKNesbHaewpcAdW57BoWzQNXhGAWVBKSaml
ChAZjrEKV4RnjrQn17S6u5VSkzsGKJeXPhMY6vCg6sN1hKZUAbFwPgQqzNg3UxSD
8kHK3NHB03gRnmlEKdsZmsiR5MU0N1cIW7OueDZnNQxEWNl2cuhh6AsdJnlRDqOm
8jYMd6RpQsegalVNIoCAyEtHrvFNsXYgyxbAarMKG+TNpwgr6fh+nCEcRpFjSaW6
jqpSAccpSjwIhbU7ZXRSEIgl7GRskKBGEjJO59Axr+U0MTLL72e277Gl7CgJt3NT
jOd7PYsE6ws8IlYBHkxxbBmougdSv3FJIRdknwYVwykPwppG/eS9UtuShtYDOIJE
JZwVp6wrZApgzAM3alhBo/uKRzVo+psaJnIV80wBaXsPDmJxddchBbdwfCm55hS9
wzpvbIGKlTcLQniC17R2eWqexuuZMnTNmyORqCukXjOT0umulyHKnWwbmItYJ3E/
kKZYXelDNSjAKwPOELtfcgE40Pu0wwwSZrkY5Skl3+F7N/ldIrylT0dZGayFkJjA
8NCKxYde8ptW/RQebvFfcAoLZvOVlcWIF3NzxGabIbwHHkw6pfC0oxtiWPNdokrD
zSnH8gkkEMUHg1WxOPtTprmubgucCCQ+e6pFxHN264x/E9TPUapzb6MVQMkkHzcN
pUS/n5wo2aV+Lyp8qVpOS0ZuZBqzvMdq3xE51Wem8StS86ZefsCq4mvKqMVYM7BO
WZmOvJoZMPu20iM8U9LB+LlRjjwt5zoZ3uazgKWzKXHPZOEp/WwfpuddSiNFAelm
3TpUCvXI9PNKa0olPuKEklZtXmfG9VhV/LBQb7BsFWdE2aA6MaJvqUytFPFXt/MD
0Hppx3N2j8tNB5wJBZcDoMOpTeS5nqOi8WWD0PkXCjlQ2we08LwwgCkn+feWG2JZ
iSY2qVAqJwUwNjd5ndNE2kUcHPe/Z4QM6zB5q4xrjBkn9kBTxhJFDEXJ5gO8FmZu
WWs0ceEDtvFUR0JNFwIgSBEf+9N+HGcPZPFLinsyuUwaSbRd0vw4zVKJ2RCtY2As
9eEwQsZKxnl7iftVGtCOBaktIAzMt+cS7yPJMSyzUPApq1N+KHNH/TB1rBCQang/
HGwHzLiPQSKMS+HGQPeQtcOl1dPKeSSV10vEYVYmWMB6xgAna5JKtbyb4fBJTLdv
gvRgp0gJcmYzgeFpmWBh15mFnsVNT1ylxBHAHbFZexZZd2ad4TqSijSvusJY/qjE
dkI5yUIdwxGb9bR2mSBpeDJ7HFNF73RqeYOEHwVuJTQQCrJNTpq70LF8apW9TDwO
QPaeFhKs7rKLmQhslRFucgQnOJM5C/RriZs2KGsOvxlHu5iE9zLKJ9qCsZtdwMx/
iIVxSRCIiyMQxPkxnUELNOZDO5AD4hdruZUldFYQbolSFjuLpZJTDMWqCutDrTmP
6el7qlI9ekQxZ3w9OvBxnkdduFypWvUIm+q+sFsvqrSJa6YPgciEcqV7RqgogmoM
37RG+BiRgtK/XqxOwcxd6vWZyKE+SCNUBtF//dyDRLbGaYSoaKqS+gIieghpUOsM
hwHtWNxih3a5g4guEXWjUjBQMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQU2oIY
LDnr2zUNkE7kvFB7cgQ/+iMwHwYDVR0jBBgwFoAUiYhnULV8JNs/wBLmHt5ZdTM3
N08wCwYJYIZIAWUDBAMTA4ISFAB0Ilvfx69mChnV48hOgGE9RRQLmMKyjFn4sKDx
FO8grAAsxKw9hdEkv+TKqayLkCkxeDnhL/HIOnDRXxZ9iVUMcCUrhcerYIIZiUeu
CJYYHAk0Wv/eQF+qzT3UNREKdljBD7rlem7wRC7oT6vf304BFsDOQmL3yL3gh8hI
ycxU5SMh3dH6Gj1wSug91LVBV/QhLebDixXuKOe/q5dyNQRk1lI4im5ysGCkGzdq
UZuanqBYvvE0c1dvvgeG9+qV9ARQOxmOaKYQMENVVA9HbzGV66GUrR19jK9z1bRI
OSzFCba83oGHKyC9bHCLfvtXFXRxNVlDHGk7dRm2dAOds/iWJL4cu/M2O8rWaxIt
ypfeieyKbr6CQjGzWqQ5lNYC3piMO9Byl6QxvZqBPhFeLbXYc3ZFhk250oz7m+LF
DpHX0+uf4SROW51EDoo3gN3hQPp9usgYQcfprP/SpxGmxJ03GaHv/tFF/pEwCAT+
sGPjYGsT14KVNG//guI4cHs9pE6s5Y8lslD1AUjFg8VQlIqF2JCPnaOGyagdEem3
mazLJ0y2KCnFMhqp3oGaVWXC2LSwyOLe0XKeJWRbuvXQ4Wl81OItyLX86fjol8bO
nCG83V3w4L3Omizd9SdnBtd6uv+1S6oxEvNcs7+pw6TN/6EuUaRPhi/jYr8Zpplq
JfsCOUoLs6hJLjrD5QMmCCxYCrV76ea6Moyyr1/0mfElOkkTLMLzKN5p4vqPEdAd
N5vDAT8g4Yn0MsRPqqK0pXyUA7Ax9ISGuQebeF9rBEtoEIG+bq4wXBWxmG2gQ3Ki
ctNDS5LUZS23n85pZ8t002IX6fXD3JYtn4UMJEjbSh3+s6WY3A1qG00bLJL4chIq
+G8mBAZm0/e0Kxb+H7Y1tWZnTe+pi08fKwRcPTEdHXLKU8bS53e3A851y8cNrGs0
dNHaDQHjcboFgDhXS4geBY6iwzHGdmfDKcA5mxURP+XUgG6HBLuCYCmx0S5OzP+F
ZY+bChnR7z0j8bTl4YOOIiaHyh2CW8frGsIlw1tBINezLWa7sr+4rx6C1CK0F2J/
IdYIdEMLiL8Yx85wL0q0EufDoc/HPQRe3hDDtYsex3RMr83osZI+okf+3vtMoLv3
```

```
CJxyZIp8Di65SuZRHZ5KNW/DGFWGAobRHbS6Va37KTjzysg1VsdM6wqcIYFvOMV/
mvUVJ2MbXSawQuwKVMjYeibT8n55S9iL7mcfnivLgl7QNO86vaks8ZRpnZEA+FVS
QiS0K9eZnBTI7L4bzJKZHgTg0tcd13qZXZtUpQdXxquS63o0lDZs7k5iKx7Xt3Pz
T1f2y5ADQIrSPJ9Ytw71TubGotB39vkiqwvrF2fl7n/Ia8aEHp3k6x1OUbOcQ7G7
PW+sE2mdgy+2FcSlyomFXDent9ayH135V2k87/YYwtJjt2rFMSRogut01AtKJ/On
C1E2X5s5U9FXmeuy1ss/U6zHZ+VEiSSZlBu1ej6/yrsCAsu03/HepXMfbh4NuB4X
yUTGRYg4rF12nH8ah9Er33b4iYM6zf5JVPRPba+6oDjQHYAjvD+gRF9D5t64PcaQ
JAA381HRYqtigLpS1NaAD2bUvg2JYsZEkymXs1w+iG8aLBcakJpqmwKazFczcpZJ
nAfhVAopjRQTyGxyslH+01Kd4ZUiP4LKZCkNrQjsNspIHIaAPMp0kL/FA03tfGwe
sZvcvlnJYD7PIrwxCWdIFW24A6yaGKg4xE1NO9oJQWLRNDDY6IyOYf9jw4YNlcG5
wsJ5IsbUcUckGOPHiRx9IHSiOFewb5KWjQUN79wA9/w1SWToG2fUSrfUSNhEvsV5
F+As9EcQvgVGtINulzWWHxfCGbfVHZ8EO35xQG077xcEGMhMz9eNWQR8GdQOLy2k
QjNlZV9U9pKa5CcVjkBRHPpfsFOMT4qHW6Arv6VoNcTwUuobFtl6DYWTeU/qrmN3
e5gM176CKneRS8IoDF8nZeCDCeHAD17g4V9UUKNaeHaVQZ4elvvVwPhZvdrTGoIp
+VZrYIJqltUCZwvBvsxy6ILzZHCGTLTQwWaHSiaRLVKUPVymXVBnzj2cReDb4pk8
/bQu/03ZSquOub6PTV/8U7ejb4fXXa6TEWQa2Sao7ziqYIUTfwoPzNfvz4eLFMPw
j7USnBXe8mV+MOgL2ncK7aobOIyfPwal5IEAA5ovPmY63T1JQGdAoumKTO7NOVb5
hR/fXq25OrWf77Df3vlNdi5n1GC7UFXN2FdJ4wJl3X8my5L3sVOtzAWKMAqBLbqN
cKFKxMvbYI6gBT79Vm9f4LgwGEf9lFQUk3ysP/uQFwURGGglzPN4GmIrNHPNx5yB
bUU74kQ8d5KOYmP09S6gyxVd17nau6i4BkxwA69HnIS7RDXfg7kFnrnNvk0ySHFb
a8YmLTK4n5HEO2KRSoayIjMq5j7CvTZZag/emL3dSdFsNsnqJclUl5RImlXg5xnv
nf5x+lXcx7IZ3fBau3yE001C4W+ljlh9EzaRqTt0vT2JuJ/Mn4iRws/a7CYdX3+L
FINsrgkOJwbgUOFZGG/LShXe1OjPxbVnE0TMl35QqC6tYyY+57lqb1cBc3+ZPmTc
Q7yOeHfGAhdI7aYRV8Gqt2nx8ZwuhCJRuuxWGYjbpx9StbbVeSmQyQODoUUeXvBR
7DjFqKVRz3CXFW0j8SMRJiXCk8pQb3J+cbyA2AuXJkBlkIYswLVgH2NT3onbnhO6
0YbkUiv7d8AARktu1VHDpJWr5JgMSQ05k5b2rqKD0CPHWphapFFyEDBESeLLmnUH
WXf0aNl7VrYrXYRzEXzUGDf61yUJbBw9gTLMDC8WGHl/NPth57aZ1Ao/IB8Ir3z2
vXABqKz3Byk8klGzEa37tist+sZjN87DhKGjAUcolgoOn8F9p+SAwnLVLMhBo+Yi
Fpu5hwAIggzYhC+fgH17Oz8m8SEL+o6LUoAtleMZPQCgbSb88CvBZPHBPa3l6+qF
cORCrafkR7eKWUBCcJejSzUvap2ViqDSnerLHl0cppKvL0B9Jf++DO5RARKhTLdL
BKCHsfGVWJh+cpePHdMM0Kzax5K46RjbKrK0v7qD5oHfHQOI6RV3oJ/SXuZr5HRq
jHgy6quxwksp5w1il324kdoQ+VzaVHNbd7Oyngk8hM1RC2/HVyE/8xJjlZUxMolx
/D460FpuXdxyuYg7Z46sHNv1o3O7sRiOFXJfOH9wVb6H4PAo3T8kK1HASaA4fXq1
lj4NGV4eSD0bxDNJv+7uywbUTTKzy5ObF4swVgkfQHtRkGoXZwSTkIGnGw+bwOwO
GIz2W0T4YZVwbHs6gChn7cCQnqUmrFH+wZn54qY5FDX9ZyGsP2qxeb5zh7GtZx4T
WjcEkEok2O2YwvteSxYUPM/5lkol5edy9e5kua8YKEEFue04CghZv37ROQnh5+/s
NFZooNTzP7iPDcYuPMYSCpbowrVaRRxu7A3+IK37n9gkB9NMXT4xXizv79ey3gO9
xrk+2aa8GTC4JEXM3EUjiLIhlQ/GFLk6xPi0y9/dX4txmRzGi6DEyi6yfpog2xho
56zUqHZ2qcKBmEyrKzd99JmDe3Riw9C0Lci3SzKP1DvNQktDerm5TkyhJbOQl5Y5
fjkksJjUdEvWOGysJHx7GlUZRGPytXgTuXKEZ6oMObXt6+/lQFdB4117dsamPdl+
IXyc9FxgwMCyaECP72CuvJwCNRrPEIxlRJAaMPYhalgltqGGFm8vDhyKgfbAyhIv
OrkH6/7oOY8V/9SS6XtRIZD8WpLsxIKhB+spvtFSA3mkgLOw+Vx46CtV+91f5rJd
HcDAqOMl/KebHbt0gTKiIncx4ICUS3OcTmF5MEhSxwBHqTGeF2u6w62h9jlpp+JD
m34hh9A1gH3OwsnBGcBMxb6H23iXNGYZYyWyneIluQTvRT0CnKra8hgm8ONjXK6F
N8BZepxBL1Bu7TQIH1iYUW5LnQzIEm6eIf/iaUz6S4RRT042Cek8YWWpkhAf4ko0
0syLPVpPPxSZMpj2rUKmyOiPxLtHeVhE1QHeUS9YqkjEH9W31g68lzI/1OwIAPmX
8/0W2ehncAXZzcvaqKn3sVF0ntfY6zexcvkWKnQntyrVik6feikCRDym5CguxGzv
leBp4PVF9kMJ+lbRTCgvu+rAu70sm7HRYkbtvUQzdAkdIQYNGYa5Ah9+y/oI0vy1
C4Yz5c5D4XLN6lomHL/N/e2A6RPwCa4i5BdVDButLBAiXg8QLeicikPLxmnzVJdV
hat/2VgWDPmrW2hOfHgka+S4muOUcxHkLLKz4vIy4H6aUztSnjod5P/03JrQOm8q
iBzhOYA9tzOKxNOn8SxlWlJHhT8vb7KX3pT9dKmWqfTPn5gYlnT8rexudJkcX0pY
Qm9cLNKThdRAwP/t7Yk9evt6qh7g///JMZjKMIHtPE+mL5m/xiBjGNiA1JkV5/vl
55tWqRGoJMv0qgcPvM9IKvUMk65x2gjH5os1fuV52BgVOpcwhbLJEmHG4wd/IEo9
GrW7rFFGL4vyUNhxxXsmAsfhYsoSRR/s3GlX1FwPDxqUw+VS2duVCHYvKDBsZaLP
Ergt6fDalHKZVTnI2tVGNH3fFpAmBC5V8Iq8thzK4fRK2yF8nGP4HYSWNqQc2P5o
hB8wvEofpGjitBdNqlujkBMcNsLPPk9ZnUmQ3/erzFw34b0jTMUBrsfleaG2Kf1S
9CG6YUiULoMoRh8cPSSrvaGCxfNx9M/WkaI8JvDsEL19ASBYqu3bOV2bCutPgbfP
Bd1C6N8fNNzJ7hPSVAqz980TtfmgK+dj4NqhEw5AaVxy4+9IVGt6JhYAT8F//ATK
```

```
xfAe44nD1Bj8UGN+seYwEk7dKaCd703yP6CNu9447k/3xkvtwcwtL40Kqmza6913
B64HvQ2GjSaOdIAkaPq1ACy+2OI+S1kIvOTKBemHF3KMJf02+1ZdAhwJ4uJSnGDi
uVT8svHM779FgIUMZjOmdE8dI7jpRKsw3czgucG2r/EPYRVa1B8cQd9iq8Xw1/Ce
7CbgROAqmfboMupDgA+QEV9Nf2aAwqQTEs6yG5saOtoNiCULXwNmh18RPWhZhKqm
voXPxnZyZ2VsN3jlcFB2WG5lngf+r//d32QX8ptGQHmETXxIvMmRG2p2TS7PAthx
T45SNsbL5jNQFysjJQWTlGGYGjNGQJHtqhmiIwpUICoJNymGfYEkrg84QKo7+NdX
xZFd7HAAw9MdSl1tvkLX+uiFzl+2d/d+SvAxHD3qDitg/90tUDLAoAxmaYO3lmFy
kTuJUMVJLhkavp3LC2Q5K+mgevqlnw4h+sw2lY0a7RVLLnHc6/FVi/sC/Smu1u8u
019R3unx8faluUtqsRvlxAjtH1feQdIApy5FFp5m8t+Ixpe1QipBTN3Aa+g3bph0
hWw7u9JgPOja0lIJDDyGwWhyv4iCsII1OSKhHdLn3U34BCQ8nTY2DPqvojpRKg7u
PVnSPpbAdLnfSU3Z+x4eQZiZLKQ8LwcOnU6+J8S2Mneboj4t8chpblbFqXEX2GDy
jE6JffIAEtZan8bJyuD9lNJgr4raeyt2rqRLmpoY1Emk5HSioIjsgUTu92FeMp/b
YWP6Fc/rXHoYl5xR5kUW4BtiB+592H/XdJzPHJQx2kjzS4gh1NH5s0yENMOWYTar
0HJecZth4BF3SNDzElWcOvGWnMQj/fpkHgAq+aqXa2UCd4P/FaEXVUOuxy+vnHwe
qqigp/mWD19+DiTyv7WEe+o/AomHctLyigGFlR2zs3yLXSwNnDJ6YANpgMlEspwS
3ToM7PbcVC9vDfjKhGdAhvdVT1lr7IU0fYeMVppE6HkoKS6tbsokb9qtbvtvWCfz
I6342qm7BW6/SiZEx/Sl/DzF8qA3eLHM0xFR2kvHsn+5AB5ucy2ZOJF2W9XuwYSU
BPoRrmdIWKQYC8/MD5PtZMqUoEGvHl6jFpfbO6+RP6NakpA+q4Tl4xuDNyeKqOdD
9+XdE3acWR/r+JseircGaBDDkpjBElcYgZuLfqKrx1+G5i6t6gWopcNtLmVcuAWv
HVT854OIkNIUoqfnESODrczb3C5kjJ230df4V156qMbJBwwcJFtzf5ObyO3ycnd/
kNggIp4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQIDxcdKS4x
-----END CERTIFICATE-----
```

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER { 2 }
    }
    INTEGER { `159ffe6f22fd5cc42c524df6fd5e28d0de38f34f` }
    SEQUENCE {
      OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
      SET {
        SEQUENCE {
          # commonName
          OBJECT_IDENTIFIER { 2.5.4.3 }
          PrintableString { "LAMPS WG" }
        }
      }
    }
    SEQUENCE {
      UTCTime { "200203043210Z" }
      UTCTime { "400129043210Z" }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
      SET {
        SEQUENCE {
          # commonName
          OBJECT_IDENTIFIER { 2.5.4.3 }
          PrintableString { "LAMPS WG" }
        }
      }
    }
    SEQUENCE {
      SEQUENCE {
        OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.4.3 }
      }
      BIT_STRING { `00` `4b94c29450111191823b3514c9ac1ea3d9825cc
b86393a2dfb04654fa2192d37bfad1c497c6502eee5ca80a73bfce0baf5a54a8
8585a401397a3d232f426a7afb082bc21a44317090eaac7592c2ea88a653c449
1ea193931335f52e989a3c4cc56d9c553732d57c470fb41ab759b65d2d044453
82fcd9c4e344a1128fa9e11e04358e192ed014b23232a7ee2b22e23717f44111
ee33575399c37646da9813ec9b212afe94e5dc5c2330a7294cc1f4234a6d3fbb
4f1685ab8892c04acb17cd1c170d7b0611b6a7176c794cc8c67f55fc923c2ad2
03100f365991882c30243d77813843b5ec7c964032263706092ecf00c7516be6
```

```
4e4598ca4226c069bb5e67e4175cf2286c8dd5c488a6c5861f31baa0bd026947
0e8b551dd3bcd38c86c12f9cdb176c77dc8b6c02a701f478902c8553f694c0d8
2727b4c4a5c2c1041212aa1274808b82111b377ec75214e9b1978f76004d4139
d98613f4b8e98d20af7b534073a509a959b7a7564f9b40ca218bf61829320a85
02017954d328d7ac6c769ec29700756e7b0685b340d5e118059504a49a9a50a1
0198eb10a5784678eb427d7b4babb9552933b062897973e1318eaf0a0eac3758
4a65401b1703e042accd837531483f241cadcd1c1d378119e694429db199ac89
1e4c5343757085bb3ae783667350c4458d97672e861e80b1d2679510ea3a6f23
60c77a46942c7a06a554d228080c84b47aef14db17620cb16c06ab30a1be4cda
7082be9f87e9c211c46916349a5ba8eaa5201c7294a3c0885b53b65745210882
5ec646c90a04612324ee7d031afe5343132cbef67b6efb1a5ec2809b773538ce
77b3d8b04eb0b3c2256011e4c716c19a8ba0752bf71492117649f0615c3290fc
29a46fde4bd52db9286d603388244259c15a7ac2b640a60cc03376a5841a3fb8
a473568fa9b1a267215f34c01697b0f0e627175d72105b7707c29b9e614bdc33
a6f6c818a95370b427882d7b476796a9ec6eb993274cd9b2391a82ba45e3393d
2e9ae9721ca9d6c1b988b5827713f90a6585de9433528c02b03ce10bb5f72013
8d0fbb4c30c1266b918e52925dfe17b37f95d22bca54f475919ac859098c0f0d
08ac5875ef29b56fd141e6ef15f700a0b66f39595c588177373c4669b21bc071
e4c3aa5f0b4a31b6258f35da24ac3cd29c7f2092410c5078355b138fb53a6b9a
e6e0b9c08243e7baa45c47376eb8c7f13d4cf51aa736fa31540c9241f370da54
4bf9f9c28d9a57e2f2a7ca95a4e4b466e641ab3bcc76adf1139d567a6f12b52f
3a65e7ec0aae26bcaa8c55833b04e59998ebc9a1930fbb6d2233c53d2c1f8b95
18e3c2de73a19dee6b380a5b32971cf64e129fd6c1fa6e75d4a234501e966dd3
a540af5c8f4f34a6b4a253ee28492566d5e67c6f55855fcb0506fb06c156744d
9a03a31a26fa94cad14f157b7f303d07a69c773768fcb4d079c09059703a0c3a
94de4b99ea3a2f16583d0f9170a3950db07b4f0bc30802927f9f7961b6259892
636a9502a2705303637799dd344da451c1cf7bf67840ceb3079ab8c6b8c1927f
64053c612450c45c9e603bc16666e596b3471e103b6f15447424d17022048111
ffbd37e1c670f64f14b8a7b32b94c1a49b45dd2fc38cd5289d910ad63602cf5e
13042c64ac6797b89fb551ad08e05a92d200cccb7e712ef23c9312cb350f029a
b537e287347fd3075ac10906a783f1c6c07ccb88f41228c4be1c640f790b5c3a
5d5d3ca792495d74bc461562658c07ac600276b924ab5bc9be1f0494cb76f82f
460a7480972663381e169996061d799859ec54d4f5ca5c411c01db1597b16597
7669de13a928a34afbac258fea8c4764239c9421dc3119bf5b47699206978327
b1c5345ef746a7983841f056e2534100ab24d4e9abbd0b17c6a95bd4c3c0e40f
69e1612aceeb28b99086c95116e7204273893390bf46b899b36286b0ebf1947b
b9884f732ca27da82b19b5dc0cc7f8885714910888b2310c4f9319d410b34e64
33b9003e2176bb995257456106e8952163b8ba592530cc5aa0aeb43ad398fe9e
97baa523d7a4431677c3d3af0719e475db85ca95af5089beabeb05b2faab4896
ba60f81c88472a57b46a828826a0cdfb446f8189182d2bf5eac4ec1cc5deaf59
9c8a13e48235406d17ffddc8344b6c66984a868aa92fa02227a086950eb0c870
1ed58dc628776b983882e1175` }
    }
    [3] {
      SEQUENCE {
        SEQUENCE {
          # keyUsage
          OBJECT_IDENTIFIER { 2.5.29.15 }
          BOOLEAN { TRUE }
          OCTET_STRING {
            BIT_STRING { b`001` }
          }
        }
        SEQUENCE {
          # subjectKeyIdentifier
          OBJECT_IDENTIFIER { 2.5.29.14 }
          OCTET_STRING {
            OCTET_STRING { `da82182c39ebdb350d904ee4bc507b72043f
```

```
fa23` }
          }
        }
        SEQUENCE {
          # authorityKeyIdentifier
          OBJECT_IDENTIFIER { 2.5.29.35 }
          OCTET_STRING {
            SEQUENCE {
              [0 PRIMITIVE] { `89886750b57c24db3fc012e61ede59753
337374f` }
            }
          }
        }
      }
    }
  }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
  }
  BIT_STRING { `00` `74225bdfc7af660a19d5e3c84e80613d45140b98c2b
28c59f8b0a0f114ef20ac002cc4ac3d85d124bfe4caa9ac8b9029317839e12ff
1c83a70d15f167d89550c70252b85c7ab6082198947ae0896181c09345affde4
05faacd3dd435110a7658c10fbae57a6ef0442ee84fabdfdf4e0116c0ce4262f
7c8bde087c848c9cc54e52321ddd1fa1a3d704ae83dd4b54157f4212de6c38b1
5ee28e7bfab9772350464d652388a6e72b060a41b376a519b9a9ea058bef1347
3576fbe0786f7ea95f404503b198e68a610304355540f476f3195eba194ad1d7
d8caf73d5b448392cc509b6bcde81872b20bd6c708b7efb571574713559431c6
93b7519b674039db3f89624be1cbbf3363bcad66b122dca97de89ec8a6ebe824
231b35aa43994d602de988c3bd07297a431bd9a813e115e2db5d8737645864db
9d28cfb9be2c50e91d7d3eb9fe1244e5b9d440e8a3780dde140fa7dbac81841c
7e9acffd2a711a6c49d3719a1effed145fe91300804feb063e3606b13d782953
46fff82e238707b3da44eace58f25b250f50148c583c550948a85d8908f9da38
6c9a81d11e9b799accb274cb62829c5321aa9de819a5565c2d8b4b0c8e2ded17
29e25645bbaf5d0e1697cd4e22dc8b5fce9f8e897c6ce9c21bcdd5df0e0bdce9
a2cddf5276706d77abaffb54baa3112f35cb3bfa9c3a4cdffa12e51a44f862fe
362bf19a6996a25fb02394a0bb3a8492e3ac3e50326082c580ab57be9e6ba328
cb2af5ff499f1253a49132cc2f328de69e2fa8f11d01d379bc3013f20e189f43
2c44faaa2b4a57c9403b031f48486b9079b785f6b044b681081be6eae305c15b
1986da04372a272d3434b92d4652db79fce6967cb74d36217e9f5c3dc962d9f8
50c2448db4a1dfeb3a598dc0d6a1b4d1b2c92f872122af86f26040666d3f7b42
b16fe1fb635b566674defa98b4f1f2b045c3d311d1d72ca53c6d2e777b703ce7
5cbc70dac6b3474d1da0d01e371ba058038574b881e058ea2c331c67667c329c
0399b15113fe5d4806e8704bb826029b1d12e4eccff85658f9b0a19d1ef3d23f
1b4e5e1838e222687ca1d825bc7eb1ac225c35b4120d7b32d66bbb2bfb8af1e8
2d422b417627f21d60874430b88bf18c7ce702f4ab412e7c3a1cfc73d045ede1
0c3b58b1ec7744cafcde8b1923ea247fedefb4ca0bbf7089c72648a7c0e2eb94
ae6511d9e4a356fc31855860286d11db4ba55adfb2938f3cac83556c74ceb0a9
c21816f38c57f9af51527631b5d26b042ec0a54c8d87a26d3f27e794bd88bee6
71f9e2bcb825ed034ef3abda92cf194699d9100f855524224b42bd7999c14c8e
cbe1bcc92991e04e0d2d71dd77a995d9b54a50757c6ab92eb7a3494366cee4e6
22b1ed7b773f34f57f6cb9003408ad23c9f58b70ef54ee6c6a2d077f6f922ab0
beb1767e5ee7fc86bc6841e9de4eb1d4e51b39c43b1bb3d6fac13699d832fb61
5c4a5ca89855c37a7b7d6b21f5df957693ceff618c2d263b76ac531246882eb7
4d40b4a27f3a70b51365f9b3953d15799ebb2d6cb3f53acc767e544892499941
bb57a3ebfcabb0202cbb4dff1dea5731f6e1e0db81e17c944c6458838ac5d769
c7f1a87d12bdf76f889833acdfe4954f44f6dafbaa038d01d8023bc3fa0445f4
3e6deb83dc690240037f351d162ab6280ba52d4d6800f66d4be0d8962c644932
997b35c3e886f1a2c171a909a6a9b029acc57337296499c07e1540a298d1413c
```

```
86c72b251fed3529de195223f82ca64290dad08ec36ca481c86803cca7490bfc
5034ded7c6c1eb19bdcbe59c9603ecf22bc31096748156db803ac9a18a838c44
d4d3bda094162d13430d8e88c8e61ff63c3860d95c1b9c2c27922c6d47147241
8e3c7891c7d2074a23857b06f92968d050defdc00f7fc354964e81b67d44ab7d
448d844bec57917e02cf44710be0546b4836e9735961f17c219b7d51d9f043b7
e71406d3bef170418c84ccfd78d59047c19d40e2f2da4423365655f54f6929ae
427158e40511cfa5fb0538c4f8a875ba02bbfa56835c4f052ea1b16d97a0d859
3794feaae63777b980cd7be822a77914bc2280c5f2765e08309e1c00f5ee0e15
f5450a35a787695419e1e96fbd5c0f859bddad31a8229f9566b60826a96d5026
70bc1becc72e882f36470864cb4d0c166874a26912d52943d5ca65d5067ce3d9
c45e0dbe2993cfdb42eff4dd94aab8eb9be8f4d5ffc53b7a36f87d75dae93116
41ad926a8ef38aa6085137f0a0fccd7efcf878b14c3f08fb5129c15def2657e3
0e80bda770aedaa1b388c9f3f06a5e48100039a2f3e663add3d49406740a2e98
a4ceecd3956f9851fdf5eadb93ab59fefb0dfdef94d762e67d460bb5055cdd85
749e30265dd7f26cb92f7b153adcc058a300a812dba8d70a14ac4cbdb608ea00
53efd566f5fe0b8301847fd945414937cac3ffb90170511186825ccf3781a622
b3473cdc79c816d453be2443c77928e6263f4f52ea0cb155dd7b9dabba8b8064
c7003af479c84bb4435df83b9059eb9cdbe4d3248715b6bc6262d32b89f91c43
b62914a86b222332ae63ec2bd36596a0fde98bddd49d16c36c9ea25c95497944
89a55e0e719ef9dfe71fa55dcc7b219ddf05abb7c84d34d42e16fa58e587d133
691a93b74bd3d89b89fcc9f8891c2cfdaec261d5f7f8b14836cae090e2706e05
0e159186fcb4a15ded4e8cfc5b5671344cc977e50a82ead63263ee7b96a6f570
1737f993e64dc43bc8e7877c6021748eda61157c1aab769f1f19c2e842251bae
c561988dba71f52b5b6d5792990c90383a1451e5ef051ec38c5a8a551cf70971
56d23f123112625c293ca506f727e71bc80d80b9726406590862cc0b5601f635
3de89db9e13bad186e4522bfb77c000464b6ed551c3a495abe4980c490d39939
6f6aea283d023c75a985aa4517210304449e2cb9a75075977f468d97b56b62b5
d8473117cd41837fad725096c1c3d8132cc0c2f1618797f34fb61e7b699d40a3
f201f08af7cf6bd7001a8acf707293c9251b311adfbb62b2dfac66337cec384a
1a3014728960a0e9fc17da7e480c272d52cc841a3e622169bb9870008820cd88
42f9f807d7b3b3f26f1210bfa8e8b52802d95e3193d00a06d26fcf02bc164f1c
13dade5ebea8570e442ada7e447b78a5940427097a34b352f6a9d958aa0d29de
acb1e5d1ca692af2f407d25ffbe0cee510112a14cb74b04a087b1f19558987e7
2978f1dd30cd0acdac792b8e918db2ab2b4bfba83e681df1d0388e91577a09fd
25ee66be4746a8c7832eaabb1c24b29e70d62977db891da10f95cda54735b77b
3b29e093c84cd510b6fc757213ff31263959531328971fc3e3ad05a6e5ddc72b
9883b678eac1cdbf5a373bbb1188e15725f387f7055be87e0f028dd3f242b51c
049a0387d7ab5963e0d195e1e483d1bc43349bfeeeecb06d44d32b3cb939b178
b3056091f407b51906a176704939081a71b0f9bc0ec0e188cf65b44f86195706
c7b3a802867edc0909ea526ac51fec199f9e2a6391435fd6721ac3f6ab179be7
387b1ad671e135a3704904a24d8ed98c2fb5e4b16143ccff9964a25e5e772f5e
e64b9af18284105b9ed380a0859bf7ed13909e1e7efec345668a0d4f33fb88f0
dc62e3cc6120a96e8c2b55a451c6eec0dfe20adfb9fd82407d34c5d3e315e2ce
fefd7b2de03bdc6b93ed9a6bc1930b82445ccdc452388b221950fc614b93ac4f
8b4cbdfdd5f8b71991cc68ba0c4ca2eb27e9a20db1868e7acd4a87676a9c2819
84cab2b377df499837b7462c3d0b42dc8b74b328fd43bcd424b437ab9b94e4ca
125b3909796397e3924b098d4744bd6386cac247c7b1a55194463f2b57813b97
28467aa0c39b5edebefe5405741e35d7b76c6a63dd97e217c9cf45c60c0c0b26
8408fef60aebc9c02351acf108c6544901a30f6216a5825b6a186166f2f0e1c8
a81f6c0ca122f3ab907ebfee8398f15ffd492e97b512190fc5a92ecc482a107e
b29bed1520379a480b3b0f95c78e82b55fbdd5fe6b25d1dc0c0a8e325fca79b1
dbb748132a2227731e080944b739c4e6179304852c70047a9319e176bbac3ada
1f63969a7e2439b7e2187d035807dcec2c9c119c04cc5be87db7897346619632
5b29de225b904ef453d029caadaf21826f0e3635cae8537c0597a9c412f506ee
d34081f5898516e4b9d0cc8126e9e21ffe2694cfa4b84514f4e3609e93c6165a
992101fe24a34d2cc8b3d5a4f3f14993298f6ad42a6c8e88fc4bb47795844d50
1de512f58aa48c41fd5b7d60ebc97323fd4ec0800f997f3fd16d9e8677005d9c
dcbdaa8a9f7b151749ed7d8eb37b172f9162a7427b72ad58a4e9f7a2902443ca
```

```
6e4282ec46cef95e069e0f545f64309fa56d14c282fbbeac0bbbd2c9bb1d1624
6edbd443374091d21060d1986b9021f7ecbfa08d2fcb50b8633e5ce43e172cde
a5a261cbfcdfded80e913f009ae22e417550c1bad2c10225e0f102de89c8a43c
bc669f354975585ab7fd958160cf9ab5b684e7c78246be4b89ae3947311e42cb
2b3e2f232e07e9a533b529e3a1de4fff4dc9ad03a6f2a881ce139803db7338ac
4d3a7f12c655a5247853f2f6fb297de94fd74a996a9f4cf9f98189674fcadec6
e74991c5f4a58426f5c2cd29385d440c0ffeded893d7afb7aaa1ee0ffffc9319
8ca3081ed3c4fa62f99bfc6206318d880d49915e7fbe5e79b56a911a824cbf4a
a070fbccf482af50c93ae71da08c7e68b357ee579d818153a973085b2c91261c
6e3077f204a3d1ab5bbac51462f8bf250d871c57b2602c7e162ca12451fecdc6
957d45c0f0f1a94c3e552d9db9508762f28306c65a2cf12b82de9f0da9472995
539c8dad546347ddf169026042e55f08abcb61ccae1f44adb217c9c63f81d849
636a41cd8fe68841f30bc4a1fa468e2b4174daa5ba390131c36c2cf3e4f599d4
990dff7abcc5c37e1bd234cc501aec7e579a1b629fd52f421ba6148942e83284
61f1c3d24abbda182c5f371f4cfd691a23c26f0ec10bd7d012058aaeddb395d9
b0aeb4f81b7cf05dd42e8df1f34dcc9ee13d2540ab3f7cd13b5f9a02be763e0d
aa1130e40695c72e3ef48546b7a2616004fc17ffc04cac5f01ee389c3d418fc5
0637eb1e630124edd29a09def4df23fa08dbbde38ee4ff7c64bedc1cc2d2f8d0
aaa6cdaebdd7707ae07bd0d868d268e74802468fab5002cbed8e23e4b5908bce
4ca05e98717728c25fd36fb565d021c09e2e2529c60e2b954fcb2f1ccefbf458
0850c6633a6744f1d23b8e944ab30ddcce0b9c1b6aff10f61155ad41f1c41df6
2abc5f0d7f09eec26e044e02a99f6e832ea43800f90115f4d7f6680c2a41312c
eb21b9b1a3ada0d88250b5f0366875f113d685984aaa6be85cfc6767267656c3
778e5705076586e659e07feafffdddf6417f29b464079844d7c48bcc9911b6a7
64d2ecf02d8714f8e5236c6cbe63350172b232505939461981a33464091edaa1
9a2230a54202a093729867d8124ae0f3840aa3bf8d757c5915dec7000c3d31d4
a5d6dbe42d7fae885ce5fb677f77e4af0311c3dea0e2b60ffdd2d5032c0a00c6
66983b7966172913b8950c5492e191abe9dcb0b64392be9a07afaa59f0e21fac
c36958d1aed154b2e71dcebf1558bfb02fd29aed6ef2ed35f51dee9f1f1f6a5b
94b6ab11be5c408ed1f57de41d200a72e45169e66f2df88c697b5422a414cddc
06be8376e9874856c3bbbd2603ce8dad252090c3c86c16872bf8882b08235392
2a11dd2e7dd4df804243c9d36360cfaafa23a512a0eee3d59d23e96c074b9df4
94dd9fb1e1e4198992ca43c2f070e9d4ebe27c4b632779ba23e2df1c8696e56c
5a97117d860f28c4e897df20012d65a9fc6c9cae0fd94d260af8ada7b2b76aea
44b9a9a18d449a4e474a2a088ec8144eef7615e329fdb6163fa15cfeb5c7a189
79c51e64516e01b6207ee7dd87fd7749ccf1c9431da48f34b8821d4d1f9b34c8
434c3966136abd0725e719b61e0117748d0f312559c3af1969cc423fdfa641e0
02af9aa976b65027783ff15a1175543aec72faf9c7c1eaaa8a0a7f9960f5f7e0
e24f2bfb5847bea3f02898772d2f28a0185951db3b37c8b5d2c0d9c327a60036
980c944b29c12dd3a0cecf6dc542f6f0df8ca84674086f7554f596bec85347d8
78c569a44e87928292ead6eca246fdaad6efb6f5827f323adf8daa9bb056ebf4
a2644c7f4a5fc3cc5f2a03778b1ccd31151da4bc7b27fb9001e6e732d9938917
65bd5eec1849404fa11ae674858a4180bcfcc0f93ed64ca94a041af1e5ea3169
7db3baf913fa35a92903eab84e5e31b8337278aa8e743f7e5dd13769c591febf
89b1e8ab7066810c39298c1125718819b8b7ea2abc75f86e62eadea05a8a5c36
d2e655cb805af1d54fce7838890d214a2a7e7112383adccdbdc2e648c9db7d1d
7f8575e7aa8c6c9070c1c245b737f939bc8edf272777f90d820229e000000000
000000000000000000000000000000000000000000004080f171d292e31` }
}
```

C.4. Examples of Bad Private Keys

> WARNING: These private keys are purposely bad. Do not use them in production systems.

The following examples demonstrate inconsistent seed and expanded private keys.

C.4.1. ML-KEM Inconsistent Seed and Expanded Private Keys

Four `ML-KEM-512-PrivateKey` examples of inconsistent seed and expanded private keys are shown as follows:

1. The first `ML-KEM-512-PrivateKey` example includes the `both CHOICE`, i.e., both `seed` and `expandedKey` are included. The `seed` and `expanded` values can be checked for inconsistencies.
2. The second `ML-KEM-512-PrivateKey` example includes only `expandedKey`. The expanded private key has a mutated `s_0` and a valid public key hash, but a pairwise consistency check would find that the public key fails to match private.
3. The third `ML-KEM-512-PrivateKey` example includes only `expandedKey`. The expanded private key has a mutated H(ek); both a public key digest check and a pairwise consistency check should fail.
4. The fourth `ML-KEM-512-PrivateKey` example includes the `both CHOICE`, i.e., both `seed` and `expandedKey` are included. There is mismatch of the seed and expanded private key in only the `z` implicit rejection secret; here, the private and public vectors match and the pairwise consistency check passes, but z is different.

The following is the first example:

```
-----BEGIN PRIVATE KEY-----
MIIGvgIBADALBglghkgBZQMEBAEEggaqMIIGpgRAAAECAwQFBgcICQoLDA0ODxAR
EhMUFRYXGBkaGxwdHh8hIiMkJSYnKCkqKywtLi8wMTIzNDU2Nzg5Ojs8PT4/QASC
BmDvsn6JOEO1+bZhFYaTegU33BzhWY5u8TDVVBiwaUFnGLk3E4KY1lkkOQvUIErq
c6VzJCCGVwzLkAdwiCoTOZIeHEYlqwgwpJUosrxyCyFgSFL9d57oFT3+QyRXG5tG
Z6yFlUbOoVEPV5ltPMMKMY3QBrartJ/LOwD2QT6F4hF5wXkl2bU8dgwLDAJYxZhd
eQNgMTo6rLojsTCL939wAcA1ks/zfCXBJD+J8FAzBikeocuHoaM49HaPzIzm95fE
co8AWycN0JG8djQHiqjfaMYpNg0ldjW82ZycuxOtenMbZsc+GLFUmWiqZjxgupeV
G4+lQZpRmsKU0ptIymHRcsMUCMHicS+19miPXIOPEQvORmEOqa0e12RZkkLj6y27
Uk4kZ5TB82bpqjccBB1Oq4lQ88ns0V2fYMVt5UFCoM153A8tBBNbfAPnIWrpRQHa
+TdRbDHeyhTHg2/GExQ8lhhfB4DP/C+v+XBY4F5xMh4euYjsWXsPC5MPyX1n6aDe
eYnB9q61wWkTK6indGy1clrZwQX70Ta7I8brALnFQDuUlzhqE8f51osDoBUHqCEm
eh0Za60KkLtpppJFWElopV7adFlUSzNG8IIV8p2hk5PxN6gYGBcLtsrp1ruBYkLg
GaZp1MWYIEiMc4nv4jOYO7yTZCRkwJN8e4wBlyr6ysU17FdsuxI7wJRHYa26pyxh
6h0kg1utBI8xSTZXA4/Ep0JZmMOdAxP97IsoF2IpPE8AlTqsKkZSSH99ZCyg2aLT
5JsFAVw5wQbHuYwaUgFWM2Z4xk81IJKVbKZD4SCboXaeYRSjdkCCp0oItlz8t8cF
WVw9G29Otkqcu8Y5jJzMYwSUARi5VmuIdKK4JLGshait+hvQ2xCzEEPQqbn7rIZ3
ecO4uKllgS/og7cVtb6tSFdSElRfxBLw024tYiKszHLKB0hbVzR2Gy0xKVef8Xsi
CJg8GxdrunLDlrfe237IW7VX4UvBdp3V4YGG+scfw1tMV0o7FWK8+sEMd1VVhBZX
q0aRqxBRo8uY5m1IG2pIYDqSZmlIRr/zGygxEYYCeK+p2x5YyDpt2IEIoVWu8cCm
loiUsRuop7njMsrudKX/hipV3DfkmwHUtKe6BaAb2MKLprTD1T+QCyWMgpBoImQW
I2F6qEbx4pGmwhssh0iF9ikVUnA7GQSpNyPpV4LuksVV28LwDBdfLJuwuIo4R5Xg
1Ju86oha8Qz7xHKpQ7MKRS7l7I+D4V2Uopy/MrLU/Hxeg5Go663FkA+2QJ76km8y
+qE8o28vM25KSgdLAnsUeIPgnIkXfGWc0Sc5ZytrscTGIcXAQsiQhxWLcz2IFylr
ODGwJXVnN2Dt+a2QV46nFX8kF2LUo0OEy0j/XEMJ8MqgmQTaNhgtLCUpCIYwS3S7
Fz/HRj/+AzbZISXgNV5dQF700VAsjEfftEN3AcGIgWzZ5D0+waOM98MejCU5vLyF
lbe4gXyv9jmgw1cI6wsGsFtIHBzwwIc8Oy+PWqNswRPIGHJWNn+ZKTaetmrspooj
wme20LlsCg2asSt6gTs/C7BWVbAZcwTuR2hadCelkhKC0zz4Jmyqhim4GMQTnEGG
wYcd92UvxsLZZMaOBGUG4y1oUnmy1hoKORa2y8xCVs7saBUDaanfGivRaoTByGal
EG4ugDqhfI6RG7A2CCKkfLsdNDGBuRLqYg6RZXN0ai679nnZYsJTV0m/YV8iioKU
mFhvgx4sK44rMAIKgmC+7LxHvHGra45wtjgwpg8NYH/vcbxvYwk/IyaOmQKGiGIA
zLqF+4OEVlMQlUOxeh3spjJtm4rV2kUshji24i9h4ROPZ8DVZq4lqTfxJcsaVnJQ
4HhdomaWKnJ6lEpgMreOQlyYxp2GOAJf52GdIyKsAV9y2bfWMmuHhAniYarDxz0N
+6JY0Q67VTT7AVHVx1aeVh3Vg6qVi7XX447eQoMy230pwnAMSI4fARfjZwA/5mev
42xo+n6QWhj1BC8iEafPhBz/F5BtGVQwjMSii111xw/9+lygBlJOSR+8Gbu45oQ/
uRoNz67mpuEldXK2fWtiQmYsoAnY0qhOArxWajY+/0pEdTMpOV105HVzD50LQ05m
hHpZnF6s80FNh4KdUx3AVX9XISIjJCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+
P0A=
-----END PRIVATE KEY-----
```

The following is the second example:

```
-----BEGIN PRIVATE KEY-----
MIIGeAIBADALBglghkgBZQMEBAEEggZkBIIGYHFVT9Q2NE8nhbGzsbrBhLZnkAMz
bCbxWn3oeMSCXGvgPzxKSA91t0hqrTHToAUYYj/SB6tSjdYnIUlYNa4AYsNnt0px
uvEKrQ6KKQIHa+MTSL6xXMwJV83rtK/yJnVrvGAbZWireErLrrNHAvD4aiYgIRiy
KyP4NVh3bHnBTbqYM3nIA+DcwxYKEXVwMOacaRl5jYHraYqaRIOpnlpcssMcmmYX
mfPMiceQcG6gQWKQRdQqg67YiGDjlMaRh+IQXSjMFOw5NZLWfdAKpD/otOrkQUAC
hmtccTxqjX0Wz3i4GdbxLp5adCM5CPCxXjxLqDKcXN2lXISSjjqoBj5aqWdkA/kX
NbEQEMf1kwkTZNyGRFvIBIQKmiFyQhJGn4p7DOCsaY64bK05p/SCTZpRY6rCHuaA
iwU8ij+ssLZ0S1Jiu8smpD9mTIcytkz8es8JlgX0HHlgYJdqxDODP+ADQ/sYKDAK
QkdBEW5LRbsnbqgRKaDbTG5gvOYREB6MYlR0kl4CImeTCKPncI0Zcqe0I+sjKFHD
bS7VPT7Tu3UAY3BhpdwikvocRmwHNUaDMovsLB7Sy1yZt47KCWkDjPfDTdEYck4x
yuCGIGs0MCtSD10Xet7Vs8zgKszoCOomvMByYl/bk/F0WKX8HU2jlDgKH1fpzGYQ
lDigdfDSgT/MShmcx22zgj8nCwBhWUGSlAQRo3/7r64sFQFlzsXGv3PFlfuSzRUx
JgfaBwd4ZSvZlEvEi8fRpTQzi60LrWZWxdUCznhQqxWHJE7rWPQ5q14IV0pxjIqs
PXfHmLuhVCczvnNEjyP7cMDlNTonyIMixSGEk6+7OAhkNNbWCla6iH3UmMOrJqCH
CZOBWqakCXXyGK3KFYLWT/yGUvuzqab7wwT5GUX6Sq7yh4/XFd9wET0jefRIhvgS
yD/ytxmmnh7HSuSxWszTrtWlPOdqewmCRxYzuXPLQKGgAV0KQk+hGkecAjAXQ20q
KQDpk+taCgZ0AMf0qt8gH8T6MSZKY7rpXMjWXDmVgV5ZfRBDVc8pqlMzyTJRhp1b
zb5IcST2Ari2pmwWxHYWSK12XPXYAGtRXpBafwrAdrDGLvoygVPnylcBaZ8TBfHm
vG+QsOSbaTUSts6ZKouAFt38GmYsfj+WGcvYad13GvMIlszVkYrGy3dGbF53mZbW
f/mqvJdQPyx7fi0ADYZFD7GAfKTKvaRlgloxx4mht6SRqzhydl0yDQtxkg+iE8lA
k0Frg7gSTmn2XmLLUADcw3qpoP/3OXDEdy81fSQYnKb1MFVowOI3ajdipoxgXlY8
XSCVcuD8dTLKKUcpU1VntfxBPF6HktJGRTbMgI+YrddGZPFBVm+QFqkKVBgpqYoE
ZM5BqLtEwtT6PCwglGByjvFKGnxMm5jRIgO0zDUpFgqasteDj3/2tTrgWqMafWRr
evpsRZMlJqPDdVYZvplMIRwqMcBbNEeDbLIVC+GCna5rBMVTXP9Ubjkrp5dBFyD5
JPSQpaxUlfITVtVQt4KmTBaItrZVvMeEIZekNML2Vjtbfwmni8xIgjJ4NWHRb0y6
tnVUAAUHgVcMZmBLgXrRJSKUc26LAYYaS1p0UZuLb+UUiaUHI5Llh2JscTd2V10z
gGocjicyr5fCaA9RZmMxxOuLvAQxxPloMtrxs8RVKPuhU/bHixwZhwKUfM0zdyek
b7U7oR3ly0GRNGhZUWy2rXJADzzyCbI2rvNaWArIfrPjD6/WaXPKin3SZ1r0H3oX
thQzzRr4D3cIhp9mVIhJeYCxrBCgzctjagDthoGzXkKRJMqANQcluF+DperDpKPM
FgCQPmUpNWC5szblrw1SnawaBIEZMCy3qbzBELlIUb8CEX8ZncSFqFK3Rz8JuDGm
gx1bVMC3kNIlz2u5LZRiomzbM92lEjx6rw4moLg2Ve6ii/OoB0clAY/WuuS2Ac9h
uqtxp6PTUZejQ+dLSicsEl1UCJZCbYW3lY07OKa6mH7DciXHtEzbEt3kU5tKsII2
NoPwS/egnMXEHf6DChsWLgsyQzQ2LwhKFEZ3IzRLrdAA+NjFN8SPmY8FMHzr0e3g
uBw7xZoGWhttY7JsgvEB/2SAY7N24rtsW3RV9lWlDC/q2t4VDvoODm82WuogISIj
JCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+Pw==
-----END PRIVATE KEY-----
```

The following is the third example:

```
-----BEGIN PRIVATE KEY-----
MIIGeAIBADALBglghkgBZQMEBAEEggZkBIIGYHBVT9Q2NE8nhbGzsbrBhLZnkAMz
bCbxWn3oeMSCXGvgPzxKSA91t0hqrTHToAUYYj/SB6tSjdYnIUlYNa4AYsNnt0px
uvEKrQ6KKQIHa+MTSL6xXMwJV83rtK/yJnVrvGAbZWireErLrrNHAvD4aiYgIRiy
KyP4NVh3bHnBTbqYM3nIA+DcwxYKEXVwMOacaRl5jYHraYqaRIOpnlpcssMcmmYX
mfPMiceQcG6gQWKQRdQqg67YiGDjlMaRh+IQXSjMFOw5NZLWfdAKpD/otOrkQUAC
hmtccTxqjX0Wz3i4GdbxLp5adCM5CPCxXjxLqDKcXN2lXISSjjqoBj5aqWdkA/kX
NbEQEMf1kwkTZNyGRFvIBIQKmiFyQhJGn4p7DOCsaY64bK05p/SCTZpRY6rCHuaA
iwU8ij+ssLZ0S1Jiu8smpD9mTIcytkz8es8JlgX0HHlgYJdqxDODP+ADQ/sYKDAK
QkdBEW5LRbsnbqgRKaDbTG5gvOYREB6MYlR0kl4CImeTCKPncI0Zcqe0I+sjKFHD
bS7VPT7Tu3UAY3BhpdwikvocRmwHNUaDMovsLB7Sy1yZt47KCWkDjPfDTdEYck4x
yuCGIGs0MCtSD10Xet7Vs8zgKszoCOomvMByYl/bk/F0WKX8HU2jlDgKH1fpzGYQ
lDigdfDSgT/MShmcx22zgj8nCwBhWUGSlAQRo3/7r64sFQFlzsXGv3PFlfuSzRUx
JgfaBwd4ZSvZlEvEi8fRpTQzi60LrWZWxdUCznhQqxWHJE7rWPQ5q14IV0pxjIqs
PXfHmLuhVCczvnNEjyP7cMDlNTonyIMixSGEk6+7OAhkNNbWCla6iH3UmMOrJqCH
CZOBWqakCXXyGK3KFYLWT/yGUvuzqab7wwT5GUX6Sq7yh4/XFd9wET0jefRIhvgS
yD/ytxmmnh7HSuSxWszTrtWlPOdqewmCRxYzuXPLQKGgAV0KQk+hGkecAjAXQ20q
KQDpk+taCgZ0AMf0qt8gH8T6MSZKY7rpXMjWXDmVgV5ZfRBDVc8pqlMzyTJRhp1b
zb5IcST2Ari2pmwWxHYWSK12XPXYAGtRXpBafwrAdrDGLvoygVPnylcBaZ8TBfHm
vG+QsOSbaTUSts6ZKouAFt38GmYsfj+WGcvYad13GvMIlszVkYrGy3dGbF53mZbW
f/mqvJdQPyx7fi0ADYZFD7GAfKTKvaRlgloxx4mht6SRqzhydl0yDQtxkg+iE8lA
k0Frg7gSTmn2XmLLUADcw3qpoP/3OXDEdy81fSQYnKb1MFVowOI3ajdipoxgXlY8
XSCVcuD8dTLKKUcpU1VntfxBPF6HktJGRTbMgI+YrddGZPFBVm+QFqkKVBgpqYoE
ZM5BqLtEwtT6PCwglGByjvFKGnxMm5jRIgO0zDUpFgqasteDj3/2tTrgWqMafWRr
evpsRZMlJqPDdVYZvplMIRwqMcBbNEeDbLIVC+GCna5rBMVTXP9Ubjkrp5dBFyD5
JPSQpaxUlfITVtVQt4KmTBaItrZVvMeEIZekNML2Vjtbfwmni8xIgjJ4NWHRb0y6
tnVUAAUHgVcMZmBLgXrRJSKUc26LAYYaS1p0UZuLb+UUiaUHI5Llh2JscTd2V10z
gGocjicyr5fCaA9RZmMxxOuLvAQxxPloMtrxs8RVKPuhU/bHixwZhwKUfM0zdyek
b7U7oR3ly0GRNGhZUWy2rXJADzzyCbI2rvNaWArIfrPjD6/WaXPKin3SZ1r0H3oX
thQzzRr4D3cIhp9mVIhJeYCxrBCgzctjagDthoGzXkKRJMqANQcluF+DperDpKPM
FgCQPmUpNWC5szblrw1SnawaBIEZMCy3qbzBELlIUb8CEX8ZncSFqFK3Rz8JuDGm
gx1bVMC3kNIlz2u5LZRiomzbM92lEjx6rw4moLg2Ve6ii/OoB0clAY/WuuS2Ac9h
uqtxp6PTUZejQ+dLSicsEl1UCJZCbYW3lY07OKa6mH7DciXHtEzbEt3kU5tKsII2
NoPwS/egnMXEHf6DChsWLgsyQzQ2LwhKFEZ3IzRLrdAA+NjFN8SPmY8FMHzr0e3g
uBw7xZoGWhttY7Jsg/EB/2SAY7N24rtsW3RV9lWlDC/q2t4VDvoODm82WuogISIj
JCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+Pw==
-----END PRIVATE KEY-----
```

The following is the fourth example:

```
-----BEGIN PRIVATE KEY-----
MIIGvgIBADALBglghkgBZQMEBAEEggaqMIIGpgRAAAECAwQFBgcICQoLDA0ODxAR
EhMUFRYXGBkaGxwdHh8gISIjJCUmJygpKissLS4vMDEyMzQ1Njc4OTo7PD0+PwSC
BmBwVU/UNjRPJ4Wxs7G6wYS2Z5ADM2wm8Vp96HjEglxr4D88SkgPdbdIaq0x06AF
GGI/0gerUo3WJyFJWDWuAGLDZ7dKcbrxCq0OiikCB2vjE0i+sVzMCVfN67Sv8iZ1
a7xgG2Voq3hKy66zRwLw+GomICEYsisj+DVYd2x5wU26mDN5yAPg3MMWChF1cDDm
nGkZeY2B62mKmkSDqZ5aXLLDHJpmF5nzzInHkHBuoEFikEXUKoOu2Ihg45TGkYfi
EF0ozBTsOTWS1n3QCqQ/6LTq5EFAAoZrXHE8ao19Fs94uBnW8S6eWnQjOQjwsV48
S6gynFzdpVyEko46qAY+WqlnZAP5FzWxEBDH9ZMJE2TchkRbyASECpohckISRp+K
ewzgrGmOuGytOaf0gk2aUWOqwh7mgIsFPIo/rLC2dEtSYrvLJqQ/ZkyHMrZM/HrP
CZYF9Bx5YGCXasQzgz/gA0P7GCgwCkJHQRFuS0W7J26oESmg20xuYLzmERAejGJU
dJJeAiJnkwij53CNGXKntCPrIyhRw20u1T0+07t1AGNwYaXcIpL6HEZsBzVGgzKL
7Cwe0stcmbeOyglpA4z3w03RGHJOMcrghiBrNDArUg9dF3re1bPM4CrM6AjqJrzA
cmJf25PxdFil/B1No5Q4Ch9X6cxmEJQ4oHXw0oE/zEoZnMdts4I/JwsAYVlBkpQE
EaN/+6+uLBUBZc7Fxr9zxZX7ks0VMSYH2gcHeGUr2ZRLxIvH0aU0M4utC61mVsXV
As54UKsVhyRO61j0OateCFdKcYyKrD13x5i7oVQnM75zRI8j+3DA5TU6J8iDIsUh
hJOvuzgIZDTW1gpWuoh91JjDqyaghwmTgVqmpAl18hityhWC1k/8hlL7s6mm+8ME
+RlF+kqu8oeP1xXfcBE9I3n0SIb4Esg/8rcZpp4ex0rksVrM067VpTznansJgkcW
M7lzy0ChoAFdCkJPoRpHnAIwF0NtKikA6ZPrWgoGdADH9KrfIB/E+jEmSmO66VzI
1lw5lYFeWX0QQ1XPKapTM8kyUYadW82+SHEk9gK4tqZsFsR2Fkitdlz12ABrUV6Q
Wn8KwHawxi76MoFT58pXAWmfEwXx5rxvkLDkm2k1ErbOmSqLgBbd/BpmLH4/lhnL
2GnddxrzCJbM1ZGKxst3Rmxed5mW1n/5qryXUD8se34tAA2GRQ+xgHykyr2kZYJa
MceJobekkas4cnZdMg0LcZIPohPJQJNBa4O4Ek5p9l5iy1AA3MN6qaD/9zlwxHcv
NX0kGJym9TBVaMDiN2o3YqaMYF5WPF0glXLg/HUyyilHKVNVZ7X8QTxeh5LSRkU2
zICPmK3XRmTxQVZvkBapClQYKamKBGTOQai7RMLU+jwsIJRgco7xShp8TJuY0SID
tMw1KRYKmrLXg49/9rU64FqjGn1ka3r6bEWTJSajw3VWGb6ZTCEcKjHAWzRHg2yy
FQvhgp2uawTFU1z/VG45K6eXQRcg+ST0kKWsVJXyE1bVULeCpkwWiLa2VbzHhCGX
pDTC9lY7W38Jp4vMSIIyeDVh0W9MurZ1VAAFB4FXDGZgS4F60SUilHNuiwGGGkta
dFGbi2/lFImlByOS5YdibHE3dlddM4BqHI4nMq+XwmgPUWZjMcTri7wEMcT5aDLa
8bPEVSj7oVP2x4scGYcClHzNM3cnpG+1O6Ed5ctBkTRoWVFstq1yQA888gmyNq7z
WlgKyH6z4w+v1mlzyop90mda9B96F7YUM80a+A93CIafZlSISXmAsawQoM3LY2oA
7YaBs15CkSTKgDUHJbhfg6Xqw6SjzBYAkD5lKTVgubM25a8NUp2sGgSBGTAst6m8
wRC5SFG/AhF/GZ3EhahSt0c/CbgxpoMdW1TAt5DSJc9ruS2UYqJs2zPdpRI8eq8O
JqC4NlXuoovzqAdHJQGP1rrktgHPYbqrcaej01GXo0PnS0onLBJdVAiWQm2Ft5WN
Ozimuph+w3Ilx7RM2xLd5FObSrCCNjaD8Ev3oJzFxB3+gwobFi4LMkM0Ni8IShRG
dyM0S63QAPjYxTfEj5mPBTB869Ht4LgcO8WaBlobbWOybILxAf9kgGOzduK7bFt0
VfZVpQwv6treFQ76Dg5vNlrqICEiIyQlJicoKSorLC0uLzAxMjM0NTY3ODk6Ozw9
Pj4=
-----END PRIVATE KEY-----
```

Acknowledgments

The authors wish to thank the following people for their contributions to this document: Corey Bonnell, Deirdre Connolly, Viktor Dukhovni, Alicja Kario, Russ Housley, Mike Ounsworth, Daniel Van Geest, Thom Wiggers, and Carl Wallace.

In addition, we would like to thank those who contributed to the private key format discussion: Tony Arcieri, Bob Beck, Dmitry Belyavskiy, David Benjamin, Daniel Bernstein, Uri Blumenthal, Theo Buehler, Stephen Farrell, Jean-Pierre Fiset, Scott Fluhrer, Alex Gaynor, John Gray, Peter Gutmann, David Hook, Tim Hudson, Paul Kehrer, John Kemp, Watson Ladd, Adam Langley, John Mattsson, Damien Miller, Robert Relyea, Michael Richardson, Markku-Juhani O. Saarinen, Rich Salz, Roland Shoemaker, Sophie Schmieg, Simo Sorce, Michael St. Johns, Falko Strenzke, Filippo Valsorda, and Wei-Jun Wang.

Authors' Addresses

Sean Turner
sn3rd
Email: sean@sn3rd.com

Panos Kampanakis
AWS
Email: kpanos@amazon.com

Jake Massimo
AWS
Email: jakemas@amazon.com

Bas Westerbaan
Cloudflare
Email: bas@westerbaan.name