

Internet Engineering Task Force (IETF)  
Request for Comments: 9881  
Category: Standards Track  
ISSN: 2070-1721

J. Massimo  
P. Kampanakis  
AWS  
S. Turner  
sn3rd  
B. E. Westerbaan  
Cloudflare  
October 2025

## Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)

### Abstract

Digital signatures are used within X.509 certificates and Certificate Revocation Lists (CRLs), and to sign messages. This document specifies the conventions for using FIPS 204, the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) in Internet X.509 certificates and CRLs. The conventions for the associated signatures, subject public keys, and private key are also described.

### 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/rfc9881>.

### Copyright Notice

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

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

### Table of Contents

1. Introduction
  - 1.1. Requirements Language
2. Identifiers
3. ML-DSA Signatures in PKIX
4. ML-DSA Public Keys in PKIX
5. Key Usage Bits
6. Private Key Format
7. IANA Considerations
8. Operational Considerations

8.1.	Private Key Format
8.2.	Private Key Consistency Testing
8.3.	Rationale for Disallowing HashML-DSA
9.	Security Considerations
10.	References
10.1.	Normative References
10.2.	Informative References
Appendix A.	ASN.1 Module
Appendix B.	Security Strengths
Appendix C.	Examples
C.1.	Example Private Keys
C.1.1.	ML-DSA-44 Private Key Examples
C.1.2.	ML-DSA-65 Private Key Examples
C.1.3.	ML-DSA-87 Private Key Examples
C.2.	Example Public Keys
C.3.	Example Certificates
C.4.	Example Inconsistent Seed and Expanded Private Keys
Appendix D.	Pre-Hashing (External $\mu$ -ML-DSA)
Acknowledgments	
Authors' Addresses	

## 1. Introduction

The Module-Lattice-Based Digital Signature Algorithm (ML-DSA) is a quantum-resistant digital signature scheme standardized by the US National Institute of Standards and Technology (NIST) PQC project [NIST-PQC] in [FIPS204]. This document specifies the use of the ML-DSA in Public Key Infrastructure X.509 (PKIX) certificates and Certificate Revocation Lists (CRLs) at three security levels: ML-DSA-44, ML-DSA-65, and ML-DSA-87.

[FIPS204] defines two variants of ML-DSA: pure and pre-hash. Only the former is specified in this document. See Section 8.3 for the rationale. The pure variant of ML-DSA supports the typical pre-hash flow. Refer to Appendix D for more details.

Prior to standardization, ML-DSA was known as Dilithium. ML-DSA and Dilithium are not compatible.

### 1.1. Requirements Language

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.

## 2. 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 object identifier (OID).

\* parameters, which are optional, are the associated parameters for the algorithm identifier in the algorithm field.

The NIST-registered OIDs [CSOR] are:

```
id-ml-dsa-44 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
    country(16) us(840) organization(1) gov(101) csor(3)
    nistAlgorithm(4) sigAlgs(3) id-ml-dsa-44(17) }

id-ml-dsa-65 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
    country(16) us(840) organization(1) gov(101) csor(3)
    nistAlgorithm(4) sigAlgs(3) id-ml-dsa-65(18) }

id-ml-dsa-87 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
    country(16) us(840) organization(1) gov(101) csor(3)
    nistAlgorithm(4) sigAlgs(3) id-ml-dsa-87(19) }
```

The contents of the parameters component for each algorithm MUST be absent.

### 3. ML-DSA Signatures in PKIX

ML-DSA is a digital signature scheme built upon the Fiat-Shamir-with-aborts framework [Fiat-Shamir]. The security is based upon the hardness of lattice problems over module lattices [Dilithium]. ML-DSA provides three parameter sets for the NIST PQC security categories 2, 3, and 5.

Signatures are used in a number of different ASN.1 structures. As shown in the ASN.1 equivalent to that in [RFC5280] below, in an X.509 certificate, a signature is encoded with an algorithm identifier in the signatureAlgorithm attribute and a signatureValue attribute that contains the actual signature.

```
Certificate ::= SIGNED{ TBSCertificate }

SIGNED{ToBeSigned} ::= SEQUENCE {
    toBeSigned          ToBeSigned,
    algorithmIdentifier SEQUENCE {
        algorithm      SIGNATURE-ALGORITHM.
                        &id({SignatureAlgorithms}),
        parameters     SIGNATURE-ALGORITHM.
                        &Params({SignatureAlgorithms}
                                {@algorithmIdentifier.algorithm})
                        OPTIONAL
    },
    signature BIT STRING (CONTAINING SIGNATURE-ALGORITHM.&Value(
                                {SignatureAlgorithms}
                                {@algorithmIdentifier.algorithm}))
}
```

Signatures are also used in the CRL list ASN.1; the representation below is equivalent to that in [RFC5280]. In an X.509 CRL, a signature is encoded with an algorithm identifier in the signatureAlgorithm attribute and a signatureValue attribute that contains the actual signature.

```
CertificateList ::= SIGNED{ TBSCertList }
```

The following SIGNATURE-ALGORITHM ASN.1 classes are for ML-DSA-44, ML-DSA-65, and ML-DSA-87:

```
sa-ml-dsa-44 SIGNATURE-ALGORITHM ::= {
    IDENTIFIER id-ml-dsa-44
    PARAMS ARE absent
}
```

```

PUBLIC-KEYS { pk-ml-dsa-44 }
SMIME-CAPS { IDENTIFIED BY id-ml-dsa-44 }
}

```

```

sa-ml-dsa-65 SIGNATURE-ALGORITHM ::= {
  IDENTIFIER id-ml-dsa-65
  PARAMS ARE absent
  PUBLIC-KEYS { pk-ml-dsa-65 }
  SMIME-CAPS { IDENTIFIED BY id-ml-dsa-65 }
}

```

```

sa-ml-dsa-87 SIGNATURE-ALGORITHM ::= {
  IDENTIFIER id-ml-dsa-87
  PARAMS ARE absent
  PUBLIC-KEYS { pk-ml-dsa-87 }
  SMIME-CAPS { IDENTIFIED BY id-ml-dsa-87 }
}

```

| NOTE: The above syntax is from [RFC5912] and is compatible with  
| the 2021 ASN.1 syntax [X680].

The identifiers defined in Section 2 can be used as the AlgorithmIdentifier in the signatureAlgorithm field in the sequence Certificate/CertificateList and in the signature field in the sequence TBSCertificate/TBSCertList in certificates and CRLs, respectively, [RFC5280]. The parameters of these signature algorithms MUST be absent, as explained in Section 2. That is, the AlgorithmIdentifier SHALL be a SEQUENCE of one component, the OID id-ml-dsa-\*, where \* is 44, 65, or 87 -- see Section 2.

The signatureValue field contains the corresponding ML-DSA signature computed upon the ASN.1 DER-encoded TBSCertificate/TBSCertList [RFC5280]. The optional context string (ctx) parameter as defined in Section 5.2 of [FIPS204] is left to its default value: the empty string.

Conforming Certification Authority (CA) implementations MUST specify the algorithms explicitly by using the OIDs specified in Section 2 when encoding ML-DSA signatures in certificates and CRLs. Conforming client implementations that process certificates and CRLs using ML-DSA MUST recognize the corresponding OIDs. Encoding rules for ML-DSA signature values are specified in Section 2.

#### 4. ML-DSA Public Keys in PKIX

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
}

```

| 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 SubjectPublicKeyInfo have the following meaning:

- \* algorithm is the algorithm identifier and parameters for the public key (see above).
- \* subjectPublicKey contains the public key.

Algorithm 22 in Section 7.2 of [FIPS204] defines the raw byte string encoding of an ML-DSA public key. When used in a

SubjectPublicKeyInfo type, the subjectPublicKey BIT STRING contains this raw byte string encoding of the public key. When an ML-DSA public key appears outside of a SubjectPublicKeyInfo type in an environment that uses ASN.1 encoding, it could be encoded as an OCTET STRING by using the ML-DSA-44-PublicKey, ML-DSA-65-PublicKey, and ML-DSA-87-PublicKey types corresponding to the correct key size defined below.

The PUBLIC-KEY ASN.1 types for ML-DSA are defined here:

```
pk-ml-dsa-44 PUBLIC-KEY ::= {
  IDENTIFIER id-ml-dsa-44
  -- KEY no ASN.1 wrapping --
  CERT-KEY-USAGE
  { digitalSignature, nonRepudiation, keyCertSign, cRLSign }
  PRIVATE-KEY ML-DSA-44-PrivateKey } -- defined in Section 6
```

```
pk-ml-dsa-65 PUBLIC-KEY ::= {
  IDENTIFIER id-ml-dsa-65
  -- KEY no ASN.1 wrapping --
  CERT-KEY-USAGE
  { digitalSignature, nonRepudiation, keyCertSign, cRLSign }
  PRIVATE-KEY ML-DSA-65-PrivateKey } -- defined in Section 6
```

```
pk-ml-dsa-87 PUBLIC-KEY ::= {
  IDENTIFIER id-ml-dsa-87
  -- KEY no ASN.1 wrapping --
  CERT-KEY-USAGE
  { digitalSignature, nonRepudiation, keyCertSign, cRLSign }
  PRIVATE-KEY ML-DSA-87-PrivateKey } -- defined in Section 6
```

```
ML-DSA-44-PublicKey ::= OCTET STRING (SIZE (1312))
```

```
ML-DSA-65-PublicKey ::= OCTET STRING (SIZE (1952))
```

```
ML-DSA-87-PublicKey ::= OCTET STRING (SIZE (2592))
```

```
| NOTE: The above syntax is from [RFC5912] and is compatible with
| the 2021 ASN.1 syntax [X680].
```

[RFC5958] specifies the Asymmetric Key Package's OneAsymmetricKey type for encoding asymmetric keypairs. When an ML-DSA private key or keypair is encoded as a OneAsymmetricKey, it follows the description in Section 6.

When the ML-DSA 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-DSA-PrivateKey CHOICE formats defined in Section 6. The seed format is RECOMMENDED as it efficiently stores both the private and public key.

Appendix C contains example ML-DSA 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 a certificate that includes id-ml-dsa-\* (where \* is 44, 65, or 87 -- see Section 2) in the SubjectPublicKeyInfo, then the subject public key can only be used for verifying digital signatures on certificates or CRLs, or those used in an entity authentication service, a data origin authentication service, an integrity service, and/or a non-repudiation service that protects against the signing entity falsely denying some action. This means that the keyUsage extension MUST

have at least one of the following bits set:

- \* digitalSignature
- \* nonRepudiation
- \* keyCertSign
- \* cRLSign

ML-DSA subject public keys cannot be used to establish keys or encrypt data, so the keyUsage extension MUST NOT have any of the following bits set:

- \* keyEncipherment
- \* dataEncipherment
- \* keyAgreement
- \* encipherOnly
- \* decipherOnly

Requirements about the keyUsage extension bits defined in [RFC5280] still apply.

## 6. Private Key Format

[FIPS204] specifies two formats for an ML-DSA private key: a 32-octet seed (  $\xi$  ) (GREEK SMALL LETTER XI, U+03BE) and an (expanded) private key. The expanded private key (and public key) is computed from the seed using ML-DSA.KeyGen\_internal( $\xi$ ) (algorithm 6).

"Asymmetric Key Packages" [RFC5958] specifies how to encode a private key in a structure that both identifies what 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 ]],
    ...
}
```

| NOTE: The above syntax is from [RFC5958] and is compatible with  
| the 2021 ASN.1 syntax [X680].

For ML-DSA private keys, the privateKey field in OneAsymmetricKey contains one of the following DER-encoded CHOICE structures. The seed format is a fixed 32-byte OCTET STRING (34 bytes total with the 0x8020 tag and length) for all security levels, while the expandedKey

and both formats vary in size by security level:

```
ML-DSA-44-PrivateKey ::= CHOICE {  
    seed [0] OCTET STRING (SIZE (32)),  
    expandedKey OCTET STRING (SIZE (2560)),  
    both SEQUENCE {  
        seed OCTET STRING (SIZE (32)),  
        expandedKey OCTET STRING (SIZE (2560))  
    }  
}
```

```
ML-DSA-65-PrivateKey ::= CHOICE {  
    seed [0] OCTET STRING (SIZE (32)),  
    expandedKey OCTET STRING (SIZE (4032)),  
    both SEQUENCE {  
        seed OCTET STRING (SIZE (32)),  
        expandedKey OCTET STRING (SIZE (4032))  
    }  
}
```

```
ML-DSA-87-PrivateKey ::= CHOICE {  
    seed [0] OCTET STRING (SIZE (32)),  
    expandedKey OCTET STRING (SIZE (4896)),  
    both SEQUENCE {  
        seed OCTET STRING (SIZE (32)),  
        expandedKey OCTET STRING (SIZE (4896))  
    }  
}
```

| NOTE: The above syntax is from [RFC5912] and is compatible with  
| the 2021 ASN.1 syntax [X680].

The CHOICE allows three representations of the private key:

1. The seed format (tag [0]) contains just the 32-byte seed value (ξ) from which both the expanded private key and public key can be derived using ML-DSA.KeyGen\_internal(ξ).
2. The expandedKey format contains the expanded private key that was derived from the seed.
3. 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.

When encoding an ML-DSA private key in a OneAsymmetricKey object, any of these three formats may be used, though the seed format is RECOMMENDED for storage efficiency.

The privateKeyAlgorithm field uses the AlgorithmIdentifier structure with the appropriate OID as defined in Section 2. If present, the publicKey field will hold the encoded public key as defined in Section 4.

| NOTE: 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-  
| DSA.KeyGen\_internal(ξ). Alternatively, the public key can be  
| generated from the private key. While the publicKey field and  
| expandedKey format are technically redundant when using the  
| seed-only format, they MAY be included to enable keypair  
| 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 contains example ML-DSA private keys encoded using the textual encoding defined in [RFC7468].

7. IANA Considerations

For the ASN.1 module in Appendix A, IANA has assigned the following object identifier (OID) in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0):

Decimal	Description	Reference
119	id-mod-x509-ml-dsa-2025	RFC 9881

Table 1: Registered ASN.1 Module

8. Operational Considerations

8.1. Private Key Format

An ML-DSA.KeyGen seed (  $\xi$  ) represents the RECOMMENDED format for storing and transmitting ML-DSA private keys. This format is explicitly permitted by [FIPS204] as an acceptable representation of a keypair. In particular, generating the seed in one cryptographic module and then importing or exporting it into another cryptographic module is allowed. The internal key-generation function ML-DSA.KeyGen\_internal(  $\xi$  ) can be accessed for this purpose.

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 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. ML-DSA seed extraction can be implemented by including the seed  $\xi$  that is randomly generated at line 1 of Algorithm 1 ML-DSA.KeyGen in the returned output.

When encoding an ML-DSA private key in a OneAsymmetricKey object, any of these three formats may be used, though the seed format is RECOMMENDED for storage efficiency.

8.2. 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 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.

The seed consistency check consists of regenerating the expanded form from the seed via ML-DSA.KeyGen\_internal, and ensuring it is bitwise equal to the value presented in the private key.

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

### 8.3. Rationale for Disallowing HashML-DSA

The HashML-DSA mode defined in Section 5.4 of [FIPS204] MUST NOT be used; in other words, public keys identified by id-hash-ml-dsa-44-with-sha512, id-hash-ml-dsa-65-with-sha512, and id-hash-ml-dsa-87-with-sha512 MUST NOT be in X.509 certificates used for CRLs, OCSP, certificate issuance, and related PKIX protocols. This restriction is primarily to increase interoperability.

ML-DSA and HashML-DSA are incompatible algorithms that require different Verify() routines. This introduces the complexity of informing the verifier whether to use ML-DSA.Verify() or HashML-DSA.Verify(). Additionally, since the same OIDs are used to identify the ML-DSA public keys and ML-DSA signature algorithms, an implementation would need to commit a given public key to be either of type ML-DSA or HashML-DSA at the time of certificate creation. This is anticipated to cause operational issues in contexts where the operator does not know whether the key will need to produce pure or pre-hashed signatures at key-generation time. The External " $\mu$ " (GREEK SMALL LETTER MU, U+03BC) mode described in Appendix D avoids all of these operational concerns.

A minor security reason for disallowing HashML-DSA is that the design of the ML-DSA algorithm provides enhanced resistance against collision attacks, compared with HashML-DSA or conventional RSA or ECDSA signature algorithms. Specifically, ML-DSA prepends the SHAKE256 hash of the public key (tr) to the message to-be-signed prior to hashing, as described in line 6 of Algorithm 7 of [FIPS204]. This means that in the unlikely discovery of a collision attack against the SHA-3 family, an attacker would have to perform a public-key-specific collision search in order to find message pairs such that  $H(\text{tr} || m_1) = H(\text{tr} || m_2)$ , because a direct hash collision  $H(m_1) = H(m_2)$  will not suffice. HashML-DSA removes this enhanced security property. In spite of its lack of targeted collision protection, the practical security risk of using HashML-DSA in X.509 signatures would be immaterial. This is because a hash of the issuing CA's public key is already included in the Authority Key Identifier (AKI) extension, which is signed as part of the TBSCertificate structure. Even when it is a SHA-1 hash, general second pre-images against the AKI hash of existing issuing CAs would be impractical.

## 9. Security Considerations

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

The ML-DSA signature scheme is strongly unforgeable under chosen message attacks (SUF-CMA). For the purpose of estimating security strength, it has been assumed that the attacker has access to signatures for no more than  $2^{64}$  chosen messages.

ML-DSA depends on high quality random numbers that are suitable for use in cryptography. The use of inadequate pseudo-random number generators (PRNGs) to generate such values can significantly undermine various security properties. For instance, using an inadequate PRNG for key generation might allow an attacker to efficiently recover the private key by trying a small set of possibilities, rather than brute-force searching the whole key space. The generation of random numbers of a sufficient level of quality for use in cryptography is difficult; see Section 3.6.1 of [FIPS204] for some additional information.

In the design of ML-DSA, care has been taken to make side-channel resilience easier to achieve. For instance, ML-DSA does not depend on Gaussian sampling. Implementations must still take great care not

to leak information via various side channels. While deliberate design decisions such as these can help to deliver a secure implementation with greater ease -- particularly against side-channel attacks -- it does not necessarily provide resistance to more powerful attacks such as differential power analysis. Some amount of side-channel leakage has been demonstrated in parts of the signing algorithm (specifically the bit-unpacking function), from which a demonstration of key recovery has been made over a large sample of signatures. Masking countermeasures exist for ML-DSA, but comes with performance overhead.

ML-DSA offers both deterministic and randomized signing. Signatures generated with either mode are compatible and a verifier cannot tell them apart. In the deterministic case, a signature only depends on the private key and the message to be signed. This makes the implementation easier to test and does not require a randomness source during signing. In the randomized case, signing mixes in a 256-bit random string from an approved random bit generator (RBG). When randomized, ML-DSA is easier to harden against fault and hardware side-channel attacks.

A security property that is also associated with digital signatures is non-repudiation. Non-repudiation refers to the assurance that the owner of a signature keypair that was capable of generating an existing signature corresponding to certain data cannot convincingly deny having signed the data, unless its private key was compromised. The digital signature scheme ML-DSA possesses three security properties beyond unforgeability, that are associated with non-repudiation. These are exclusive ownership, message-bound signatures, and non-resignability. These properties are based tightly on the assumed collision resistance of the hash function used (in this case SHAKE-256). A full discussion of these properties in ML-DSA can be found at [CDFFJ21].

## 10. References

### 10.1. Normative References

- [CSOR] NIST, "Computer Security Objects Register (CSOR)", 13 June 2025, <<https://csrc.nist.gov/projects/computer-security-objects-register/algorithm-registration>>.
- [FIPS204] NIST, "Module-Lattice-Based Digital Signature Standard", NIST FIPS 204, DOI 10.6028/NIST.FIPS.204, 13 August 2024, <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [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>>.
- [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>>.

## 10.2. Informative References

- [CDFJ21] Cremers, C., Dzl, S., Fiedler, R., Fischlin, M., and C. Janson, "BUFFing signature schemes beyond unforgeability and the case of post-quantum signatures", Cryptology ePrint Archive, Paper 2020/1525, October 2023, <<https://eprint.iacr.org/archive/2020/1525/20231023:114351>>.
- [Dilithium] Bai, S., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and D. Stehl, "CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (Version 3.1)", 8 February 2021, <<https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf>>.
- [Fiat-Shamir] Lyubashevsky, V., "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures", International Conference on the Theory and Application of Cryptology and Information Security, 2009, <<https://www.iacr.org/archive/asiacrypt2009/59120596/59120596.pdf>>.
- [FIPS204-ExternalMuFAQ] NIST, "FIPS 204 Section 6 FAQ", 2025, <<https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/faq/fips204-sec6-03192025.pdf>>.
- [NIST-PQC] NIST, "Post-Quantum Cryptography (PQC)", 28 July 2025, <<https://csrc.nist.gov/Projects/post-quantum-cryptography>>.
- [RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <<https://www.rfc-editor.org/info/rfc3647>>.
- [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>>.

## Appendix A. ASN.1 Module

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

<CODE BEGINS>

```

X509-ML-DSA-2025
{ iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-x509-ml-dsa-2025(119) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS

PUBLIC-KEY, SIGNATURE-ALGORITHM
  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) } ;

--
-- ML-DSA Identifiers
--

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

sigAlgs OBJECT IDENTIFIER ::= { nistAlgorithms 3 }

id-ml-dsa-44 OBJECT IDENTIFIER ::= { sigAlgs 17 }

id-ml-dsa-65 OBJECT IDENTIFIER ::= { sigAlgs 18 }

id-ml-dsa-87 OBJECT IDENTIFIER ::= { sigAlgs 19 }

--
-- Public Key Algorithms
--

PublicKeys PUBLIC-KEY ::= {
  -- This expands PublicKeys from [RFC 5912]
  pk-ml-dsa-44 |
  pk-ml-dsa-65 |
  pk-ml-dsa-87,
  ...
}

--
-- ML-DSA Public Keys
--

pk-ml-dsa-44 PUBLIC-KEY ::= {
  IDENTIFIER id-ml-dsa-44
  -- KEY no ASN.1 wrapping; 1312 octets --
  PARAMS ARE absent
  CERT-KEY-USAGE { digitalSignature, nonRepudiation,
    keyCertSign, cRLSign }
  PRIVATE-KEY ML-DSA-44-PrivateKey
}

ML-DSA-44-PrivateKey ::= CHOICE {
  seed [0] OCTET STRING (SIZE (32)),
  expandedKey OCTET STRING (SIZE (2560)),
  both SEQUENCE {
    seed OCTET STRING (SIZE (32)),
    expandedKey OCTET STRING (SIZE (2560))
  }
}

```

```

pk-ml-dsa-65 PUBLIC-KEY ::= {
    IDENTIFIER id-ml-dsa-65
    -- KEY no ASN.1 wrapping; 1952 octets --
    PARAMS ARE absent
    CERT-KEY-USAGE { digitalSignature, nonRepudiation,
                     keyCertSign, cRLSign }
    PRIVATE-KEY ML-DSA-65-PrivateKey
}

ML-DSA-65-PrivateKey ::= CHOICE {
    seed [0] OCTET STRING (SIZE (32)),
    expandedKey OCTET STRING (SIZE (4032)),
    both SEQUENCE {
        seed OCTET STRING (SIZE (32)),
        expandedKey OCTET STRING (SIZE (4032))
    }
}

pk-ml-dsa-87 PUBLIC-KEY ::= {
    IDENTIFIER id-ml-dsa-87
    -- KEY no ASN.1 wrapping; 2592 octets --
    PARAMS ARE absent
    CERT-KEY-USAGE { digitalSignature, nonRepudiation,
                     keyCertSign, cRLSign }
    PRIVATE-KEY ML-DSA-87-PrivateKey
}

ML-DSA-87-PrivateKey ::= CHOICE {
    seed [0] OCTET STRING (SIZE (32)),
    expandedKey OCTET STRING (SIZE (4896)),
    both SEQUENCE {
        seed OCTET STRING (SIZE (32)),
        expandedKey OCTET STRING (SIZE (4896))
    }
}

ML-DSA-44-PublicKey ::= OCTET STRING (SIZE (1312))

ML-DSA-65-PublicKey ::= OCTET STRING (SIZE (1952))

ML-DSA-87-PublicKey ::= OCTET STRING (SIZE (2602))

--
-- Signature Algorithms
--

SignatureAlgorithms SIGNATURE-ALGORITHM ::= {
    -- This expands SignatureAlgorithms from [RFC 5912]
    sa-ml-dsa-44 |
    sa-ml-dsa-65 |
    sa-ml-dsa-87,
    ... }

--
-- ML-DSA Signature Algorithm Identifiers
--

sa-ml-dsa-44 SIGNATURE-ALGORITHM ::= {
    IDENTIFIER id-ml-dsa-44
    PARAMS ARE absent
    PUBLIC-KEYS { pk-ml-dsa-44 }
    SMIME-CAPS { IDENTIFIED BY id-ml-dsa-44 }
}

sa-ml-dsa-65 SIGNATURE-ALGORITHM ::= {

```

```

IDENTIFIER id-ml-dsa-65
PARAMS ARE absent
PUBLIC-KEYS { pk-ml-dsa-65 }
SMIME-CAPS { IDENTIFIED BY id-ml-dsa-65 }
}

sa-ml-dsa-87 SIGNATURE-ALGORITHM ::= {
  IDENTIFIER id-ml-dsa-87
  PARAMS ARE absent
  PUBLIC-KEYS { pk-ml-dsa-87 }
  SMIME-CAPS { IDENTIFIED BY id-ml-dsa-87 }
}
END
<CODE ENDS>

```

## Appendix B. Security Strengths

Instead of defining the strength of a quantum algorithm using the common but imprecise notion of bits of security, NIST has instead elected to define security levels by picking a reference scheme, which NIST expects to offer notable levels of resistance to both quantum and classical attacks. To wit, an algorithm that achieves NIST PQC security level 1 must require computational resources to break the relevant security property, which are greater than those required for a brute-force key search on AES-128. Levels 3 and 5 use AES-192 and AES-256 as references, respectively. Levels 2 and 4 use collision search for SHA-256 and SHA-384 as references.

The parameter sets defined for NIST security levels 2, 3, and 5 are listed in Table 2, along with the resulting signature size, public key, and private key sizes in bytes. Note that these are the sizes of the raw keys, not including ASN.1 encoding overhead from `OneAsymmetricKey` and `SubjectPublicKeyInfo` wrappers. Private key sizes are shown for both the seed format and expanded format.

Level	(k,l)	eta	Sig. (B)	Public Key(B)	Private Seed(B)	Private Expand(B)
2	(4,4)	2	2420	1312	32	2560
3	(6,5)	4	3309	1952	32	4032
5	(8,7)	2	4627	2592	32	4896

Table 2: ML-DSA Parameters

## Appendix C. Examples

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

### C.1. Example Private Keys

The following examples show ML-DSA private keys in different formats, all derived from the same seed 000102...1elf. 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-DSA-44 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-----
MDQCAQAwCwYJYIZIAWUDBAMRBCAIAAABAgMEBQYHCAkKCwwNDg8QERITFBUWFxgZ
Ghschr4f
-----END PRIVATE KEY-----

SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
  }
  OCTET_STRING {
    [0 PRIMITIVE] { '000102030405060708090a0b0c0d0e0f10111213141
5161718191a1b1c1d1e1f' }
  }
}
```

#### C.1.1.2. Expanded Format

```
-----BEGIN PRIVATE KEY-----
MIIKGAIBADALBgIghkgBZQMEAxEEggoEBIIKANeytHJUquDbReeTDUqY0sl9jxOX
0Xidr6FwJLMW6b7J0c4Pf3f421ZE3No2a/5HNL2V9DX/mmE6pUqkHCxpTAQymgex
+rtI9SownxGhiY+EjiMi/+Yj7IENS77jNoWFSogmnaMglRIL/P6JoY4w9xFNg6pA
SmRrbJlziYYNEliu4ABuI4SBkYZhmyYNEYZklKYOIhhEgkAomBRhSKZhTEJIoZII
wjgpUSRICKElwgxCMRxIBQJFINSGKEAhBBuyCBwIrVkCLBhDacEmBJEUYhpWQBG
IpMgQQYuQrZMARZJFChMQahRgEYKURZRWgggAiJE3JhJ0TJR4TB108CFkqhREqFk
ADkiCUZiHMcM2Qht0AYmUkCFgEQwkQYsUMgJJMWEgPZtSpqsmQZtpEQyIKdkWjJu
EbVwIJJhJBOOBiUsCkhyYKBR0wgqmSCAWCQgJAdOWRSIEKRkYMBt4LKNGxkJIDQi
wCRBCUNxCiEgYaIBUiJSG4CAmJQAE5NN0zIpIhcKmJJPghRRICchnMAgYqKBSBhp
GoVNg0RpWyBBaxJCyxhGAakNDaiXg7AhWiJKyJIF2ZBpBDBqSwZK0rIBHEBAGUIy
UjJyKZAWhgQDDiSksKAUhJiXIIoC7RsA0KNuXAMFAEO4TZSiIQkkQIKY0YmIAYp
EcIo0CBIArNsojYJWoZiY7Rhi0ZixECCGokJEAJNjLJFIBILJmKfiCiMycBNWugi
CiduwTRkTJBgW0RQgoZJQ4gEQ7KMYDCAoogthKRtjKYp0MaEQgZGiYhRAKmaNAUmN
5DgNpAan05RxQrJsGoRhG6MoQrQoCKBxGsUx4KBMATdlJChiFCiQCRBh2UAiGzNg
CQKS0CSBIAQISRheoyItXiHefJgIpeZHAZVkcZkKDJRQykBq0rIgwDgBgjCOE7kI
kYCEFIgpbBiRejUNoCQi4gQG2cKFBCgSHMmJGAJy0kApwggS2AYqmZRxm7hoI4Qp
GiKJFEUR3IJEUJZFDESEwLIEmqYFQ4YsRDJuIEQhIKhMmjBw47gtYyaIAYVJA0OM
SKgJyhRyUzROEkMIG6cEWTAi2ZSA4jQigUISnDAqLDQmYQRFJCYoE0YJSjJtESgJ
GLglYigRE0ENQbIRKIRMixISosaIycAwIgyG0hiOhIYwKERSEogx2SBxE8UoQwYO
AzBgZkaEWCZSTIGBHvclYshf+kOs+kkhfysXLXu8FGIObZgKcaq73wxF6aIG7LFC
P+4V3swXYBMAFJ2SI8lubG4fqOQfx8ZJOKtokF/T3NpQ2HCC59DXHRVjsrhmV18
qp5srSlk340+FbEI/3IdDMh7w906dZAYS6EVmOpH8nhw8U6YdhnQgsE8J1lV108
ZaBjaPlBKV/QmSQTGL+r9nlkwUJnSnJcNDkUxM7PWMB0vK9FWML795EeB6ptCTjy
7iuzwajFldY16ENC/eoB3CSyEa0vwoHPd+WREMerxUvwyG1IC5vidkcdydYdzumM
/as+n8+3A3klYFSePEUPp7M/uRacRLTSX7nEV/SXkc09oD6slglYE8EFeyzNpOY+
SSKM0j2KHzeFbxQtk7kNsJ+Cr4kljGOquAR6gMA2yTV+ogRvjcy1TwxSlfNCu0F9
PP6wsf0zYiwp4Uy72S4TY8ZevUUEt1EjKblndjLhssZ6VOfxpV+Ln56gToyjpwXm
KjxeY3N0r7eut3qYSzeKPAaIC16pONHItJ90/m4mJTQGf1dTXEZ7+Ny07oQTLi7
CYHgdN46/iANqq6tgmxEXyRNv0Ma+rNO+994JHTS/VcRj2RiFJNO2Zy6OWA+jWej
g29vGfxBkQzlFj7jrpnrhNUU63YeY2hOpW+XkdLdSqxuYWi5SMgX9loiKssOjNwD
zEr+j2cVfho203+u/58XK5iRNnfFod0IXp7kwiBSwa9YGTEWZz3NO/xfNLhV3MbH
eIVknp5x9D1K6g9Lcsp+2gV4uhPTGmWNLQYKmmB/ae0b5516L7HScj04+b+r4Y+O
ezzakG5Om16ULI6uspYHDr/TZJR6lAzJeL7Wazd0nmldzXvoxJREDiueZs/vuYwL
7fs8QeMlnSzXGX++cgxIqmxrZGXB7mPjVpwq3HREkTcLf3gm/gt3odGdZBAaAyuR
gQa0LS73N0flYB/kulDyPt5SHwMagX0VKUpDci6DeHhLbbDPG6norpeDkgG5zpzD
AZxvXCfLmNomFetkIlp8kysw92Hnii1Zodi4PsY0Si9t1H52VwbQC/SnmngSbDup
HYEsjyx5erF5Zwnl0WhWd4KTUp8ChtAVw7U51hlkKjM+nlk9bj9TU51CCOnmozKF
HX91JSPkKLx4n4tbtUITff4uv6b7HGeybAJUuoAF9+vb4xWmjgotp2noqfQtPmAA
fHEzCSaywAetgru5P0e2HLM0ZciAdKwJ/NUwsLTDNeLwddA/sy8b8KgrGxuMOrF
HlppCYqilEfyCfOTkuSZmJpIdLeR4UYzQkM4meuotJ62lf9iLSXbYn7hDzc0mn
bKJnnmgBv6f7AxIW+1BilwS5kjk2ul3ThTERIcrfsRmV5ZtzA0z2ftA6uBOGdkjQ
```

JYKAh+lJqa/Ra5XXLZmx7colegwTL/t6BwmulanA/wX7Dyu/KECe7XtfWAG+lktz  
AZ4ct4UdOFHxApBnThn/sAizAcSs9kGiuxQhbhlpyr9Ste8idJaw8weZqFXRF/rT  
dEpvozUD6nmLUt3X7lQmYJ2/zT8ME7FklSBR9+lKEZcZpxLjinMoQCCB/xNUTVTS  
wjev7TsVHEuo6fS964SZowZuJrvGnorwid7HFzHR3FKeqxfvc3RzTA/kdULMg4Nr  
3TSgO5vImRRxYGG/uY7G5hw+lEOO3K8lJDxkcIa56nAYsNmooLAM7LAKveJJjWnC  
M2EBp3LL5PVxUj9RvQWILN8li4ScwUCqH68iQjoShRzg4z/UiXWklZ+lx5BjJOQ  
gZGrbnQbd7/gLLlpjueVxGbWFWGeZEE4LG6sAYNO6atzzqgLviNceNqRvXm2+C+J  
l4XWhwDTk+ZlwiJNa3oa0hMgSVZ5ra7XAWelCGZxOlMQnbe299gTBOzf2Dsxmx7y  
SDBrRa0p593Mhj2sVgSLXWnqF1AR92FMAKhqhjzeGHKokyh4uax+GsW9pJl7cgZP  
DNdfTIFOA03hGsuQE89+qSa05+qs4HDHuiGI760uQx4SI9Rd0FxNhAPC5FzuZBPs  
vnUn6HPkVcTmEKYYOarMC9VtJIPnjymLZqR46y9VjLr8qGvor7rrAsWyFsJNiP6k  
3ySbCeZwogcDq6wksKkavEpWRmAUQroQvs/TCZOIAFHQf1agWpN556jmvv7j8i+q  
EGOY93BgBuQum+HvidJcJy8RqVCVxYfXE3MihN6dvTxyF7BonihY6w/2lmg=  
-----END PRIVATE KEY-----

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
  }
  OCTET_STRING {
    OCTET_STRING { 'd7b2b47254aae0db45e7930d4a98d2c97d8f1397d178
9dafa17024b316e9bec939ce0f7f77f8db5644dcda366bfe4734bd95f435ff9a
613aa54aa41c2c694c04329a07b1fab48f52a309f11a1898f848e2322ffe623
ec810db3bee33685854a88269da320d5120bfcfe89a18e30f7114d83aa404a64
6b6c997389860d12522ee0006e2384819186619b260d118664d4a62822184482
402898146148a6614c4248a19208c2382951244808a125c2083108c471201409
14836c18a78084106ec9c07022b56408b0610c07049812445188695900462293
2041062e42b64c01164914284c41a85180460a5116515a0820022244dc9849d1
3251e13065d3c08592a85112a1640039220946621cc70cd9086dd00626524085
80443091062c50c80924c5841a966d4a982c99066da4443220a7645a326e11b5
7020926124138e04852c0a4872c8a051d3082a99208058242024074e59148810
a46460c06de0b28d1b1909203422c024410943710a212061a2015222521b8080
9a340013934dd3322922170a9892691a14512027219cc02062a2814818691a85
4d8344695b2041031242cb184601a90d0c023183b0215a224ac89205d9906904
306a4b064ad2b2011c404081423252327254a6405a18100c321292c280521262
5c82280bb46c03428d53100c14010ee1365288842491020a63462620062911c2
28d0204802b36ca236095a8648cbb4618b4662c440821a890910024d24b24520
122524c90588288cc9c04d5948220a276ec134644c90605b4450828649438804
43b28c603080a2882d84a46d8ca629d0c68442064689885100a98d01498de438
0da4068dd3947142b26c1a84611ba32842b42808a0711ac531e0a04c01376524
2862142890091061d940221b3360090292d02481200408491844a3222d5c8844
149808a446610195640b390a0c9450ca406ad2b220c0380182308e13b9089180
84148829c0189112350da02422e20406d9c2850428121cc989180272d24029c2
0812d8062a9994719bb8682384291a2289144511dc82445096450c4484c0b204
9aa60543862c44326e88442120a84c9a3070e3b82d63268803254903438c48a8
09ca147253344e1243081ba704593022d99480e234228142129c302a94342661
04542426281346094a326d11280918b28562281113410d41b21190844c8b1212
a2c688c9c030220606d218e848630904452128831d9207113c52843060e0330
60cca6845826524c88011ef72562c85ffa43acfa49217f2b172d7bbc14620e6d
980a71aabdbdf0c45e9a206ecb1423fee15decc17601300149d9223cd6e6c6e1f
a8e41fc7c64938ab68905fd3dcda50d87082e7d0d71d1bc9b2b84c85523ca8fe
6cad294adf83be15b108ff721d0cc87bc3dd3a7590184b0e845663a91fc9e1c3
c53a61d867420b04f092355753bc65a06368fd41295fd09924132c6f91f67964
c142674a725c343914c4cecf58c074bcfa4558c97bf7911e07aa6d0938f2ee2b
b3c1a8c595d635e84342fdea01dc24b211ad2fc281cf77e59110c7abc54bf0c8
6d480b9be276471dc9d603cee98cfdab3e9fcfb703793560549ea4450fa7b33f
b9169c44b4d25fb9c457f49791cd3da03eac96095813c105132ccda4e63e4922
8cd23d8a1f37856f142d93b90db09f82af89258c63aab8047a80c036c9357ea2
046f8dc6354f0c5295f342bb417d3cfef0b1fd33622c29e14cbbd92e1363c65e
bd4504b7512329b9670e32elb2c67a54e7f1a55f8b9f9ea04e8ca3a705e62a3c
5e637374afb7aeb6ddea612cde28f01a202d7aa4e34722d27dd3f9b89894d019
fd5d4d7119efe3723bba104cb8bb0981e074de3afe200daaaead826cc45f244d
bf431afab34efbdf782474d2fd57118f646214934ed99cba3b003e8d67a3836f
6f19fc41910ce5163ee3ae99eb84d514eb761e63684ea56f9791d2dd4aac6e61
68b948c817f75a222acb0e8cdc03cc4afe8f67157e1a363b7faeff9f172b9891
```

```
3677c5aldd085e9ee4c22052c1af58193116673dcd3bfc5f34b8555dcc6c77885
649e9e71f43d4aea0f4b72ca7eda0578ba13d31a658d2d060a9a66ff69ed1be7
997a2fbl1d2723d38f9bfabel18f8e7b3cda906e4e9b5e942c8eaeb296070ebfd3
64947a940cc978bed66b37749e6d5dcd7be8c494440e2b84cecfefb98c0bedfb
3c41e3359d2cd7197f7be720c48aa6c6b6465c1ee63e3569c2adc744491370b7f
7826fe0b77a1d19d64101d032b918106b42d2ef73747e5601fe4ba50f23ede52
1f031a817d15294a43722e8378784b6db0cf1ba9e8ae911d9201b9ce9cc3019c
6f5c27cb98da26144b64225a7c932b30f761e78a2d59a1d8b83ec6344a2f6dd4
7e765706d00bf4a79a6a926c3ba91d812c8f2c797ab1796709e5d16856778293
529f0286d015c3b5399619642a333e9e593d6e3f5353994208e9e6a332851d7f
652522a928b917e27e2d6d42137dfe2ebfa6fb1c67b26c0254528685f7ebdbe3
15a68aaa2da769e8a9f42d3e60007c71330926b2c0012d83ead4e4fdled872cc
d1972201d2b027f3545ac2d30cd78bc1d740fccc6c6fc2a0446c6e30eac51f5a
69098aa2d447f2085b4e4e4b92ccc26921d2de478518cd090ce267aea2d27ada
57fd88b4976d89fb843cdccf49a76ca2679e6801bfa7fb031896fb50629704b9
923936bb5dd385311121cadfb11995e59b73034cf67ed03ab813867648d02582
8087e949a9afd16b95d72d99bledca257aac132ffb7a0709aed5a9c0ff05fb0f
2bbf28409eed7b5f5801be964ced019e1cb7851d3851f10290674e19fffb008b3
01c4acf641a2bb14216e1d69cabf52b5ef227496b0f30799a855d117fad3744a
6fa33503ea798b52ddd7ee5426609dbfcd3f0c13b164d6c051f7ed4a119719a7
12e388d328402081ff1354b554d2c237afed3b151c4ba8e9f4bdeb8499a3066e
26bbc69e8af089dec71731d1dc529eab17ef7374734c0fe475494c83836bdd34
a03b9bc89914716061bfb98ec6e61c3ed4438edcaf25243c647086b9ea7018b0
d9a8a0b00cecb00abde2498d69c2336101a772cbe4f571523f51bd05882cdf35
8b849cc140aalfaf22423a12851ce0e33fd48975a4959fa5c5fe418c93908191
ab6e741b77bfe02cbd698ee795c466d615619e6441382c6eac01834ee9ab73ce
a80bbe235c78da91bd79b6f82f899785d68700d393e675c2224d6b7a1ad21320
495679adaed70167b50866713a53109db7b6f7d81304ecdf83b319b1ef24830
6b45ad29e7ddcc863dac56048b5d69ea175011f7614c00a86a863cde1872a893
2878b9ac7e1ac5bda4997b72064f0cd75f4c814e034de11acb9013cf7ea926b4
e7eaace070c7ba2188efad2e431e1223d45dd05c4d8403c2e45cee6413ecbe75
27e873e455c4e610a61839aacc0bd56d2483e78f298b66a478eb2f558cbafca8
6be847baeb02c5b216c8cd88fea4df249b09e670a20703abac24b0a91abc4a56
46601442ba10becfd30993880051d07f56a05a9379e7a8e6befee3f22faa1063
98f7706006e42e9bel9d25c272f11a95095c587d713732284de9dbd3c7217
b0689e21d8eb0ff69668' }
}
}
```

### C.1.1.3. Both Format

```
-----BEGIN PRIVATE KEY-----
MIIKPgIBADALBglghkgBZQMEAxEEggoqMIIKJgQgAAECAwQFBgcICQoLDA0ODxAR
EhMUFYRXGBkaGxwdHh8EggoA17K0c1Ssq4NtF55MNSpjSyX2PE5fReJ2voXAKsxbp
vsk5zg9/d/jbVktC2jZr/kc0vZX0Nf+aYTq1SqqcLGLMBDKaB7H6u0j1KjCfEaGJ
j4SOIyL/5iPsgQ2zvuM2hyVKiCadoyDVEgv8/omhjJd3EU2DqkBKZGtsmX0Jhg0S
Ui7gAG4jhIGRhmGbJg0RhmTUpigiGESQCciYFGFIpmFMQkihkgjCOC1RJEGIoSXC
CDEIxEHEgFAkUg2wYp4CEEg7JwHAitWQIsGEMBWsyEKRRIg1ZAEYikyBBBi5CtkwB
FkkUKExBqFGARgpRf1FaCCACIkTcmEnRMLHhMGXTwIWSqFESoWQAOSIJRmIcxwzZ
CG3QBiZSQIWARDCRBixQyAkKxYQalmlKmCyZBm2kRDIGp2RaMm4RtXAgkmEkE44E
hSwKSHLioFHTCCqZIIByJCAkB05ZFigQpGRgwG3gso0bGQkgNCLAJEEJQ3EKISBh
ogFSilIbgICaNAATk03TMikiFwqYkmkaFFegJyGcwCBiooFIGGkahU2DRG1bIEED
EkLLGEYBqQ0MAjGDsCFaIkrIkGZXZGkEMGpLBkrSsgEcQECBQjJSMnJUpkBaGBAM
MhKSwoBSEmJcgigLtGwDQo1TEAwUAQ7hNlKiHCSRAGpjRiYgBikRwiJQIEgCs2yi
NglahkJLtGGLRmLEQIIaiQkQAK0kskUgEiUkyQWIKIzJwE1ZSCIKJ27BNGRMkGBb
RFCChkLDiARDsoxgMICiic2EpG2MpinQxoRCBkaJiFEaQY0BSY3kOA2kBo3TlHFC
smwahGEboyhCtCgIoHEaxTHgoEwBN2UkKGIUKJAJEGHZQCIbM2AJApLQJIEgBAhJ
GESjiilciEQUMaIkRmEBLWQLOQomLFDKQGrSsiDAOAGCMI4TuQiRgIQUiCnAGJES
NQ2gJCLiBabZwoUEKBiCyYkYAnLSQCnCBBLYBiqlZHGbuGgjhCkaIokURRHcgkRQ
lkUMRITasgSapgvDhixEMm6IRCEgqEyaMHDjuCljJogDJUkDQ4xIqAnKFHJTNE4S
QwgbpwrZMCLZLIDiNCKBQhKcMCqUNCZhBEUkJigTRglKMm0RKakYuCViKBETQ1B
shGQhEyLEhKixojJwDAiBgbsGI6EhjCQRFISiDHZIHETxShDBg4DMGDMpoRYJlJM
iAEe9yViyF/6Q6z6SSF/Kxcte7wUYg5tmApxqrvfDEXpogbssUI/7hXezBdgEwAU
nZiJzW5sbh+o5B/Hxkk4q2iQX9Pc2lDYcILn0NcdG8myuEyFUjyo/mytKUrfg74V
sQj/ch0MyHvD3TPlkBhLDoRWY6kfyeHDxTph2GdCCwTwk jVXU7xloGNo/UEpX9CZ
JBMSb5H2eWTBQmdKclw0ORTEzs9YwHS8r0VYyXv3kr4Hqm0JOPLuK7PBqMWV1jXo
```

Q0L96gHcJLIRrS/Cgc935ZEQx6vFS/DibUgLm+J2Rx3J1gP06Yz9qz6fz7cDeTVg  
VJ6kRQ+nsz+5FpxEtNjFucRX9JeRzT2gPqyWCVgTwQUTLM2k5j5JIoZSPYofN4Vv  
FC2TuQ2wn4KviSWMY6q4BHqAwDbJNX6iBG+NxjVPDFKV80K7QX08/rCx/TNiLCnh  
TLvZLhNjxl69RQS3USMpuWcOMuGyxnpU5/GlX4ufnqBOjKOnBeYqPF5jc3Svt662  
3ephLN4o8BogLXqk40ci0n3T+biYlNAZ/VlNcRnv43I7uhBMuLsJgeB03jr+IA2q  
rq2CbMRfJE2/Qxr6s07733gkdNL9VxGPZGIUk07ZnLo7AD6NZ6ODb28Z/EGRDOUW  
PuOumeuElRTrdh5jaE6lb5eR0t1KrG5haLlIyBf3WiIqyw6M3APMSv6PZxV+GjY7  
f67/nxcrmjE2d8Wh3QhenuTCIFLBr1gZMRZnPc07/F80uFXcxsd4hWSennH0PURq  
D0tyyn7aBXi6E9MaZY0tBgqaZv9p7RvnmXovsdJyPTj5v6vhj457PNqQbk6bXpQs  
jq6ylgcOv9NklHqUDMl4vtZrN3SebV3Ne+jElEQOK4TOz++5jAvt+zxB4zWdLNCz  
f75yDEiqbGtKzCzHuY+NWnCrcdESRNwt/ecb+C3eh0Z1kEB0DK5GBBrQtLvc3R+Vg  
H+S6UPI+3lIfAxqBfRUpSkNyLoN4eEttsM8bqeiukR2SAbnOnMMBNg9cJ8uY2iYU  
S2QiWnyTKzD3YeeKLVmh2Lg+xjRKL23UfnZXBtAL9KeaapJsO6kdGsyPLHl6sXln  
CeXRaFZ3gpNSnwKG0BXDtTmWGWQqMz6eWTlUPlNTmUII6eajMoUdf2UliQkouRfi  
filitQhN9/i6/pvscZ7JsAlRShoX369vjFaaOqi2naeip9C0+YAB8cTMJJrLAAS2D  
6tTk/R7YcszRlyIB0rAn8lRawtMMl4vB10D+zLxvwqBEbG4w6sUfWmkJiqLUR/II  
W05OS5LMwmkh0t5HhRjNCQziZ66i0nraV/2ItJdtifuEPNzPSadsomeeaAG/p/sD  
GJb7UGKXBLmSOTa7XdOFMREhyt+xGZXlm3MDTPZ+0Dq4E4Z2SNAIgoCH6Ump9Fr  
ldctmbHtyiV6rBMv+3oHCa7VqcD/BfsPK78oQJ7tel9YAb6WTO0Bnhy3hr04UfEC  
kGdOGf+wCLMBxKz2QaK7FCFuHWnKv1K17yJ0lrDzB5moVdEX+tN0Sm+jNQpqeYtS  
3dfuVCZgnb/NPwwTsWTWwFH37UorlXmnEuOI0yhAIiH/E1S1VNLcN6/tOxUcS6jp  
9L3rhJmjBm4mu8aeivCJ3scXMDHcUp6rF+9zdHNMD+R1SUyDg2vdNKA7m8iZFHFg  
Yb+5jsbmHD7UQ47cryUkPGRwhrnqcBiw2aigsAzssAq94kmNacIzYQGncsvk9XFS  
PlG9BYgs3zWLhJzBQKofryJCOhKFHODjP9SJdaSVn6XF/kGMk5CBkatudBt3v+As  
vWmO55XEZtYVYZ5kQTgsbqwbG07pq3POqAu+Ilx42pG9ebb4L4mXhdaHANOT5nXC  
IklrehrSEyBJVnmtrtcBZ7UIZnE6UxCdt7b32BME7N/YOzGbHvJIMGtFrSnn3cyG  
PaxWBItdaeoXUBH3YUwAgGqGPN4YcqiTKHi5rH4axb2kmXtyBk8M119MgU4DTeEa  
y5ATz36pJrTn6qzgcMe6IYjvrS5DHhIj1f3QXE2EA8LkXO5kE+y+dSfoc+RVxOYQ  
phg5qswLlW0kg+ePKYtmpHjrLlWMuvyao+hHuusCxbIWym2I/qTfJJ5J5nCiBwOr  
rCSwqRq8SlZGYBRcuhC+z9MJk4gAuDB/VqBak3nnqOa+/uPyL6oQY5j3cGAG5C6b  
4e+J0lwnLxGpUJXFh9cTcyKE3p29PHIXSgieIdjrD/aWaa==  
-----END PRIVATE KEY-----

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
  }
  OCTET_STRING {
    SEQUENCE {
      OCTET_STRING { '000102030405060708090a0b0c0d0e0f1011121314
15161718191a1b1c1d1e1f' }
      OCTET_STRING { 'd7b2b47254aae0db45e7930d4a98d2c97d8f1397d1
789dafa17024b316e9bec939ce0f7f77f8db5644dcda366bfe4734bd95f435ff
9a613aa54aa41c2c694c04329a07b1fabbb48f52a309f11a1898f848e2322ffe6
23ec810db3bee33685854a88269da320d5120bfcfe89a18e30f7114d83aa404a
646b6c997389860d12522ee0006e2384819186619b260d118664d4a628221844
82402898146148a6614c4248a19208c238295124480a125c2083108c4712014
0914836c18a78084106ec9c07022b56408b0610c070498124451886959004622
932041062e42b64c01164914284c41a85180460a5116515a0820022244dc9849
d13251e13065d3c08592a85112a1640039220946621cc70cd9086dd006265240
8580443091062c50c80924c5841a966d4a982c99066da4443220a7645a326e11
b57020926124138e04852c0a4872c8a051d3082a99208058242024074e591488
10a46460c06de0b28d1b1909203422c024410943710a212061a2015222521b80
809a340013934dd3322922170a9892691a14512027219cc02062a2814818691a
854d8344695b2041031242cb184601a90d0c023183b0215a224ac89205d99069
04306a4b064ad2b2011c404081423252327254a6405a18100c321292c2805212
625c82280bb46c03428d53100c14010ee1365288842491020a63462620062911
c228d0204802b36ca236095a8648cbb4618b4662c440821a890910024d24b245
20122524c90588288cc9c04d5948220a276ec134644c90605b44508286494388
0443b28c603080a2882d84a46d8ca629d0c68442064689885100a98d01498de4
380da0468dd3947142b26c1a84611ba32842b42808a0711ac531e0a04c013765
242862142890091061d940221b3360090292d02481200408491844a3222d5c88
44149808a446610195640b390a0c9450ca406ad2b220c0380182308e13b90891
8084148829c0189112350da02422e20406d9c2850428121cc989180272d24029
c20812d8062a9994719bb8682384291a2289144511dc82445096450c4484c0b2
```

```

049aa60543862c44326e88442120a84c9a3070e3b82d63268803254903438c48
a809ca147253344e1243081ba704593022d99480e234228142129c302a943426
6104452426281346094a326d11280918b82562281113410d41b21190844c8b12
12a2c688c9c030220606d2188e848630904452128831d9207113c52843060e03
3060cca6845826524c88011ef72562c85ffa43acfa49217f2b172d7bbc14620e
6d980a71aabbdf0c45e9a206ecb1423fee15decc17601300149d9223cd6e6c6e
1fa8e41fc7c64938ab68905fd3dcda50d87082e7d0d71d1bc9b2b84c85523ca8
fe6cad294adf83be15b108ff721d0cc87bc3dd3a7590184b0e845663a91fc9e1
c3c53a61d867420b04f092355753bc65a06368fd41295fd09924132c6f91f679
64c142674a725c343914c4cecf58c074bcfa4558c97bf7911e07aa6d0938f2ee
2bb3c1a8c595d635e84342fdea01dc24b211ad2fc281cf77e59110c7abc54bf0
c86d480b9be276471dc9d603cee98cfdab3e9fcfb703793560549ea4450fa7b3
3fb9169c44b4d25fb9c457f49791cd3da03eac96095813c105132ccda4e63e49
228cd23d8a1f37856f142d93b90db09f82af89258c63aab8047a80c036c9357e
a2046f8dc6354f0c5295f342bb417d3cfefb0b1fd33622c29e14cbdd92e1363c6
5ebd4504b7512329b9670e32e1b2c67a54e7f1a55f8b9f9ea04e8ca3a705e62a
3c5e637374afb7aeb6ddea612cde28f01a202d7aa4e34722d27dd3f9b89894d0
19fd5d4d7119efe3723bba104cb8bb0981e074de3afe200daaaead826cc45f24
4dbf431afab34efbdf782474d2fd57118f646214934ed99cba3b003e8d67a383
6f6f19fc41910ce5163ee3ae99eb84d514eb761e63684ea56f9791d2dd4aac6e
6168b948c817f75a222acb0e8cdc03cc4afe8f67157e1a363b7faeff9f172b98
913677c5aldd085e9ee4c22052c1af58193116673dcd3bfc5f34b855dcc6c778
85649e9e71f43d4aea0f4b72ca7eda0578ba13d31a658d2d060a9a66ff69ed1b
e7997a2fbl1d2723d38f9bfabel18f8e7b3cda906e4e9b5e942c8eae296070ebf
d364947a940cc978bed66b37749e6d5dcd7be8c494440e2b84cecfefb98c0bed
fb3c41e3359d2cd7197f7be720c48aa6c6b6465c1ee63e3569c2adc744491370b
7f7826fe0b77a1d19d64101d032b918106b42d2ef73747e5601fe4ba50f23ede
521f031a817d15294a43722e8378784b6db0cf1ba9e8ae911d9201b9ce9cc301
9c6f5c27cb98da26144b64225a7c932b30f761e78a2d59a1d8b83ec6344a2f6d
d47e765706d00bf4a79a6a926c3ba91d812c8f2c797ab1796709e5d168567782
93529f0286d015c3b5399619642a333e9e593d6e3f5353994208e9e6a332851d
7f652522a928b917e27e2d6d42137dfe2ebfa6fb1c67b26c0254528685f7ebdb
e315a68eaa2da769e8a9f42d3e60007c71330926b2c0012d83ead4e4fd1ed872
ccd1972201d2b027f3545ac2d30cd78bcl1d740fecbc6fc2a0446c6e30eac51f
5a69098aa2d447f2085b4e4e4b92ccc26921d2de478518cd090ce267aea2d27a
da57fd88b4976d89fb843cdccf49a76ca2679e6801bfa7fb031896fb50629704
b9923936bb5dd385311121cadfb11995e59b73034cf67ed03ab813867648d025
828087e949a9afd16b95d72d99b1edca257aac132ffb7a0709aed5a9c0ff05fb
0f2bbf28409eed7b5f5801be964ced019e1cb7851d3851f10290674e19fffb008
b301c4acf641a2bb14216el1d69cabf52b5ef227496b0f30799a855d117fad374
4a6fa33503ea798b52ddd7ee5426609dbfcd3f0c13b164d6c051f7ed4a119719
a712e388d328402081ff1354b554d2c237afed3b151c4ba8e9f4bdeb8499a306
6e26bbbc69e8af089dec71731d1dc529eab17ef7374734c0fe475494c83836bdd
34a03b9bc89914716061bfb98ec6e61c3ed4438edcaf25243c647086b9ea7018
b0d9a8a0b00cecb00abde2498d69c2336101a772cbe4f571523f51bd05882cdf
358b849cc140aalfaf22423a12851ce0e33fd48975a4959fa5c5fe418c939081
91ab6e741b77bfe02cbd698ee795c466d615619e6441382c6eac01834ee9ab73
cea80bbe235c78da1bd79b6f82f899785d68700d393e675c2224d6b7a1ad213
20495679adaed70167b50866713a53109db7b6f7d81304ecd83b319b1ef248
306b45ad29e7ddcc863dac56048b5d69ea175011f7614c00a86a863cde1872a8
932878b9ac7elac5bda4997b72064f0cd75f4c814e034del1acb9013cf7ea926
b4e7eaace070c7ba2188efad2e431e1223d45dd05c4d8403c2e45cee6413ecbe
7527e873e455c4e610a61839aacc0bd56d2483e78f298b66a478eb2f558cbafc
a86be847baeb02c5b216c8cd88fea4df249b09e670a20703abac24b0a91abc4a
5646601442ba10becfd30993880051d07f56a05a9379e7a8e6befee3f22faa10
6398f7706006e42e9bele89d25c272f11a95095c587d713732284de9dbd3c72
17b0689e21d8eb0ff69668` }
    }
}
}

```

### C.1.2. ML-DSA-65 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-----
MDQCAQAwCwYJYIZIAWUDBAMSBCAIAABAgMEBQYHCAKCCwNDg8QERITFBUWFxgZ
Ghschr4f
-----END PRIVATE KEY-----

SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
  }
  OCTET_STRING {
    [0 PRIMITIVE] { '000102030405060708090a0b0c0d0e0f10111213141
5161718191a1b1c1d1e1f' }
  }
}
```

#### C.1.2.2. Expanded Format

```
-----BEGIN PRIVATE KEY-----
MIIP2AIBADALBgIghkgBZQMEAxIEgg/EBIIPwEhoPZGXjjHrPd24sEc0gtK4il9i
WUn9jl1lYeaWvUwn2FP6abgZkCPozWen2fq/kEdkb/0Ms8x/eVgFpx5w0jcbBWPj
zTNGFJyMnrzyOwpOWpAO6pxlYnkKfGPjhmPaot3bbkgNxAWh5wGui3SEHvXMHD8r
8yeXLPuQUQzVN17MCFVxdxGHIiGGI4EABCR3gGFHUAdQFxcDVQRRUSVHGDgEYXVy
IkQQiGhghkYBJ0dWcYCHBmaGQzJEQSIENjhmDQKCNjQkQyIFc2QQZFVUdyJ1VoFD
NhRiVQggZDdoVgh1Q1N1EGhxgzOAVHUFJYB1KBiEOBEIcmAgIAhYgwGDYROCghIG
FxFXh2h4iHhkN1RgFlcVUIRxiGYHJzKIBmR0GFZ2IYAxgnZkFXgkUCVkJkMRNQQ2
R4ASZnMUMBFmBlWGRxg2iGNQOEeGEQEgI1YRYTeGB4UyEkAHVHiCMENmYRZgQ1VB
goVgU2d4VjhDRDBjJhB3BzF4QnIUERZTA4UnaGdGAVCCNzUyB2YQdQROekgGZgMD
JlIxJEVAIAAaxgIh2chcwcYJHIVEngBF1RHSGYXIjM4CGYGRGg1IVhCA2gBGAIrgY
MxdzVFNigQBEhlNnQ3BXcliDNGA4QjKfABAGBCYEJYRWajVoIFGDhjhdJCEiQkVv
WFhncUVyhQR4hxcYBhiDYIaGQVZQgRZQJkZwBggmYic4MXJAclcwBycohiBmdYho
JgcGQCAzaA0NmMVVGQkU0VmcYc0Vlg3AiUIRoViiAcDZwhGI3FxAAGVxdYR3hwhlVT
eCI1FEZ3KFZzAyKHABQzIGfXWEVSZjJQJLEzR3c4A1UWQxNHNBRmJ1FlDAJGiFw
ZONGgyYBdlJfMfCHIQQ0NAEDIOdjUVUmUIEwd0VEQWgVQYNjZBEGQCaHMENndxKA
iEY1VFMAYkWBFBfZUSSEJ4A0UWZjWEN4VgFGURV0IyFDZoUir3cxNFAXg2JCBVAA
ZIRHEjRAiABgrZvAV4MzYwghBhUiUgckiFE0hjcGdiJYhXEmVnNHABZGRoQlhwgS
JwVQCDgyACMggGY0UzYAM0aFckcGNVQANXcSJ1IwcUJTahQ3RXAFZkMiRIKFIHIY
MzAgUzcZQHcngFULMGNSUEBnM0YTGAcoBxckg3djRXMYWFFgIzNENiUWQzgWCFh3
NGJCiDAHA2WFN1UADviXUDcCEyrjBDcIaAY2FQMDAENYy1cIAhEGZHNGNSJiAzBD
gCEIUodXgyEHIGdICFY0dDZzQoQFhGaEFdCAVRCHNCZEdyESc4RzZSZHJXcURwQX
hkQmAkkRh0CBIhZgWecXgTcGdoCBcfGYVYVHE2NCEHVYAWNynyUYRAOEcrAzH0Ji
gkd0E2VUQnBzrjV3dQBmJWJoQgISRoOGRhZkyDEiU4iEVACEVzRGR1RHJWBUYWae
ZjCIBjgnFWMocYOEB1IkdoEWBmITazAYaAKAE4RjBQVlcjh1g2VyMjBogEYSJgZl
FnVXBTJBMidnNRcIAVMAFiHGATSIdeRiBVXExVGQxFWrZKIKFY2gjRVUEGGJ2Vj
ERFodeQUQ1RBRCEfiHEXF4gVNoUVdEcWYlU2VYNjAlAoVXaHUycTcQNYnWVxR2Ff
NlGEEKI2ZERmQUNSBSEIUVCdM2OGAlhCZigUGRBuYmgXMDh1ZDMhZyHwhmNjKBNA
YlQBIECIZUEiYXfldiNyYjSGcdARURVjIFB1NQISIqhcZTFDvWcRFSVYAQAFNjAV
BVdYyFh4QxQxMnh4gIc4R4hjeIGBOHNCYXg4hSRmdzNQYCEVFGQjgJJoATVEB4NH
U4VTV1KDIzUYdgEVITQyV3MzNlUYhhWBYWgkGEIhIjCEFEgVEgEQMCR3ckJUQ2YG
dxdwdgMBRSVANQAYOHMjdzUmUIY1cRNzRIFgUndFZVNzAIWDD4UDUSERVIBiFAY
AmgThlIFNGgBMgckGAMhMAVYOGQHZCCrQQGDhSVRBjJgcQSGUXaDOChXJ2I1RRhz
UIMTKIY3ZmFCYxFnUDMRJVN2QXYDFDMXchIjRBioLk9cnqD6+Z6wTXinMycREXWz
8Y7KIffh0M3atpSGYBKftmlVX/NZ6NVCzpLjFiGKcAhR1+j1WldbpuxoJvaJrTeYi
3f8W2LyZsUJ4qK8ddr7RV2ct2cmJFvl+jare+NnaaVhnJVZ/uWtZmQ1L8LycGVuQ
t0KV9WdbJCV8JxDBdbAVPykRMowut6u5rUbnCotTw56mQs7ks8tCYg6GPOi2UM6K
3NkjchoWhwI8ZzqMu2sD1RzRl+jDRuutzpOVD4jO4gHbnjIIQ+KfMA2aGVANcKTK
8nLgnk7vafu4pV79fKK+2ZDS07WChI+cRcKrxUz8R9NPBsD/pW/Ndiq5y6kUbXcl
IYljskDXK20iyTFx+9R3iLducgQt7wh40j32MaGh5aYCdobeW0oQ6RBpyPK6Almw
TWQJ2pZWfKUTpJcCblg6Ds78HwHmuYjIH5dnorfhZy3rmh4qp8yGOqkVF8M0YgYB
tP55cw6TSTX0tvve4yaVFFwrX2oSf+zAondFhrw/1SNET57nycNFNPnw21RPwxwb
/ex2XHfqL3wurkxv668QQnHFZv1OuscceMLHSVKBeuZ1UE2VmbG3YrasoWioMkjJ
2a2wzrFVbldZSQu8DHkAeVrXISMDi2YvZPEGqZk2gaJdWa97yXojW+koTFvEWmyQ
yxwpmcZj2WtHjIMH+FVilX1ldA4mc+nr0TUoKQOPriuP07VoHaVcAlJSOFNSXqCt
ZH5xrCxiJpma6yX5WwEzrLyblxbS22Uq4ETgP0A8iCP6GU1CGrr/TXcKSBiTAT7
```

thE5KdnFVjUCU3ZsIJ/bqDyV/M00KigJk1XQC8hj9O711lusLQuvMfHlJHM6uIF6g  
uAWfu4pXJsWUnSsV5+KcUfybAu4aT8NXtFG++cStlGoqkgwvwwijfrFRS/oVEQPd  
kqdMbxPFDfz/2XUxCY180jtg6zXEPci0bFU4bhAQxLp/cOTH7LdXXzBjpx6E39zw  
mliyzbD5nyftN4YQ0ly6l17+muGlZGJz+iOq5tG1+bbAwfqvkGY6ZvXH3eatmWB4J  
Evx7HSWFJF6aEmh6l1zV6OHcwEXV+JHEXoXbB8+B53OJs2Pra9/jmyf/hM1+7+4W  
LjtFH+aRRxnLZDbYVZYP+RXXzqat6v38HAV4bEn5I6R0/9/DFTOG5u0LCtIglyUk  
Q01Sc8Cqtt3k6RR21YGiaVpg3m2fRNd6oIJm6TjutKlZfJtkmGBZ5JjipOqyRU4U  
AVrQU2xCczpdd9eZXCogRGAJ6/5WMsGMC0r1681BmSJ9ZfrGx8R8E9g4MkEAVnE  
SrPmDgoVIp0ZEii+0Xu8Osk5s8Z87hNfNSwnIWycMfcqPocEDF9hkwbrC2zKKpzn  
sioWlNAMqcBeMVEmRX8mzoT5YXJBhgeC+GS0c9hAF0kZArG9yM3FgA3UYSf7gKcc  
CVtHolYlKbOx5+Q34Vil9mZumXTQBbBijCebc6Y+bZYxuP5ohbVjIyRQr0cjIWP  
2ocuu/rT/qnZq6K2ja6PGcb/XwBYTUXa+dbJlp7QS42olocli3eAeSdhLFMERv6n  
aXrj+SZpiSm8alqM8+ICTA8MXuV7WGM/mBiByvnjZl/H9+/GeJKfh6VuqkLqTR/2  
aRgi3XmkcJa3dtHY8BRW5Yc7BzhAbDgsVzrpzeLZ5/IxtsxcZ2589DljNzATpYB1  
OB/wlJvghFRtcuT4o+X+SqUJGt0jTir+ADCxtmOunS0yQQmGuUAqqvJGW3S14tC8  
00OpK73dih/te5SMI8zm+MCP41aDW6ZbD5hAaGFu9IE479ib81elTS6783bL3Mac  
Xx9hXk0nllWgZLmr32biUIXYDDirjsP4PB6evi5MgvzQpcJl9Z9fBJZ0o+/reY1  
qsUwg6cCLEfV93pStXtZjak5KubYavxG/AZFUYG5xlpkbcIfgeS/ITdT3nN/0qFA  
AnkgrdNaIj+fX0RlZrYMA+0EVAzMzpcyDrb9D8fQsLMuDKMIcerf67Sshz63i2lUi  
Oqqyr5tBxzMjQXRjQbOaovQ4FWUPVIBRFCTPppAXecTRI2OMwCh6qvMWgDONILF8  
dEn9xqJ4qNlqgu5MTspAE14tZSkAcceu8b5qmRWY+5lZUSUjvNSzjFZrjoCnOuMz  
4TRBQyfvHYPEfEnf55Nt8TOKXiR3h4aPyE/cuVrInBhcS7X9V7IzisQrQcEKgj3z  
liTzaxWi8GdYTGbKLgJmr/Fhj+Ad0G3zUS4Lck3shQbaJCFayswsUbqg2NMCAC+0  
EGix2k+LsUeYezUWutXb3fATGP0/qbxDCrEmMcZ2V8uhBtiKl5ISKPFwmKVmZLq  
enlyoo2gcJ0l9+tkzVcuxu5eG0U/yz1kDF4SP1YVkJxEN2jblGSqBbOnIgWzHu/  
yATvxACFo4ULifHn/lZW26QQ+QapfDIzbBrn6Bc3qd4Ic1TkKNqFONlI2/XfrLWd  
0rX9O8gD9LpDLJpznfLPqe2UhDIPl+3/GkjGuGswAs+3ctleVivEw9aD7ZZLYZn6  
BRSweQ2VgJW3uFxr6HX7tVnhkwFGzOpjo4ihlP4Jw96gO+Ut4n6QEBev6AmvYwpz  
gr9cTNTRuPQVeftDSO3kygX0zT8TmjGyVE5Rbb5Ahrm7Syvtr+LSMJgtlRkkKdN3  
t8B0XMB04vWkqgTH/4cgntElmXag/Jsl6ehR1ONQLALIXW3/Ap4hHQHr8OnnGI1W  
j4Q32BOW8SLy+xdgO2k+2cOPF8/VC4FebZ38DtLM8Z9jmSdKFCdYNaWdi/ckNF4U  
5F2eS+iTTfw/qSZ422HXEYv1PLiilszX36uUOP5QSN2KNT22Oo493pyrzomyB/k  
NSOzNVNaxR23w480EIK7VzTQieiuMJz9o6C8tclbCXETyO35YWqk9uZjG5ElJ2+z  
9ocjQ0HD22aNXsrUX8k7JwJkKvdzcOc0/RkcUAidrVOYL92uAlmf+T4fIf85X8Ch  
KHTt8GtvklfpWnMkWGxx39kdkBliGFgZD+zQDM0RC7rFn5bLiEw8k5lHSKVvQSG7  
/EH7iQUhU6iUWIw8uQF/PWYybJhWN+VlrlgSNGNCZUAllgLeO6lAwZrBpjPf/al3  
tSm4AT4ZwdbQaA9NrmLJJEUK5mqrgvIUCwYdqz1iskf5B+NVGTmtPlRl6dCKgr/q  
F+6htrK5I3V0d/mTAAsvQ7cPKKqrH+miatH9M2FhbAsOJC/nZgS3AzofM0l+kPUM  
yJyID+K42dGwyf8YizHLnZdCWsq5shbZimrjVeWD2nHohk7j0WshWXlhkO9UXB5i  
v++Sr2yhR7EyRNbIkvyO8iOrP0P5JML0Zgl+6A==  
-----END PRIVATE KEY-----

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
  }
  OCTET_STRING {
    OCTET_STRING { '48683d91978e31eb3dddb8b0473482d2b88a5f625949
fd8f58a561e696bd4c27d853fa69b8199023e8cd678dd9fabf9047646ffdd0cb3
cc7f795805a71e70d2371b0563e3cd3346149c8c9ebcf23b0a4e5a900eea9c65
62790a7c63e38663daa2dddb6e480dc405a1e701948b74841ef5cc1c3f2bf327
972e9510510cd5375ecc08557177118722218623810004247780614750075017
1703550451512547183804617572224410886860864601274756718087066686
43324441122043638667502823634244322057364106455547722755681433614
6255082064376854687543537510687183338054750525807528188438110872
6020200858830183611382821206171157876878887864375460165715508471
8866072732880664741856762180318276641578245025646643113504364780
1266731430116606558647183688635038478611012023561161378607853212
4007547882304366611660425541828560536778563843443063261077073178
4272141116530385276867460150823735320766107504681248066603032652
3124454088003180887672173071824721512780116544748661722333808660
6446835215842036801180211818331773545348810044865367437057725883
3460384232856810060426042584560235682051838638432421224245645858
6771457285047887171806188360868641565081165026467006082662273831
7240725730072728862066758868260706402033034366315546424534566718
```

7345658370225084685628807036708462371710065717584778708655537822  
3514467728567303228700143320617158455266325026513347773803551643  
1347351066275175740246888170674346818601765245333087210434340103  
2287635155265081307745444168154183636411204026873043677712808846  
3554530062458104583651248427803451666358437856014651157423214366  
8522477731345017836242055000648447123440880060473540578333630821  
0615225207248851348637067622588571265673476816464684258708122705  
5008383200232080663453360033468572470635540035771227523071425368  
7437457005664322448285207218333020533733407727805525306352504067  
3346131807280717248377634573185851602333443625164338160858773462  
4288300703658537550075523150370213246304370868063615030300435863  
5708021106647346352262033043802108528757832107886748085634743673  
4284058466841437005510873426447721127384736526472577144704178644  
2602471187408122166058471781370676808170581855854713634210755801  
6358358518440384711033874262824774136554427073463577750066256268  
4202124683864616646031225388845400845734464754472560546166846630  
8806382715632871838406522476811606621303301868028013846305056572  
3875836572323068804612260665167557053241322767351708015300162846  
0134887701118815571315464311704732882856368234555041862765631111  
6875051042544144278522111717881536851574471662553655836302502855  
7687532713710372370571476171365184124236644466414352052108515703  
3363860258426628148110546268173038756433216588568663632813406254  
0120408865478861716576237262348670301151156320507535021221084265  
3143556711152572010685363015055758605878431431327878808738478863  
7881813873426178388524667733506021151464238232680135440783475385  
535752832335187601152134325773336551886158161682418422122308414  
4815120110302477724254436606771770760301452540350018387323773526  
5086357113734481605277456553730085837785035121115480628850180268  
1386520534680132072418032130057238640764271141018385255106326071  
0486517683382857276235451873508313288637666142631167503311255376  
4176031433177212234418a82e4f5c9ea0faf99eb04d78a7332711117c33f18e  
ca21f8743376ada5219804a7ed9a5557fcd67a3550b3a4b8c588629c021475fa  
3d56d5d6cfbb1a09bda8d14de622ddff16d8bc99b14278a8af1d76bed157672d  
d9c32316f97e8daadef8d9da69586725567fb96b59990d4bf0bc9c195b90b742  
95f5675b24257c2710c175b0153f2911328c2eb7abb9ad46e70a8b53c39ea642  
cee4b3cb42620e863ce8b650ce8adcd923721a1687023c673a8cbb6b03d51cd1  
97e8c346ebadce93950f88cee201db9e320843e29f300d9a19500d70a4caf272  
c69e4eef69fbb8a55efd7ca2bed990d2d3b582848f9c45c2abc54cfc47d34f06  
c0ffa56fcd762ab9cba9146d7725218963b240d72b6d22c93171fbd47788b76e  
72042def0878d23df631a1a1e5a6027686de5b4a10e91069c8f2ba0259b04d64  
09da96567ca52da497026e583a0ecefcl1f01e6b988e21f9767a2b7e1672deb9a  
1e2a3fcc863aa91517c334620601b4fe79730e934935f4b6fbc4e32695145c2b  
5f6a127fecc0a277451ebc3fd523444f9ee7c9c34534f356db544fc31c1bfde5  
f65c77ea2f7c2eae4c55ebaf104271c566fd4ebac71c7a62c74952817ae67550  
4d9599b1b762b6aca168a83248c9d9adb0ceb1556e5759490bbc0c7900795ad7  
2123038b662f64f106a9993681a25d59af7bc97a235be9284c5bc45a6c90cb1c  
2999c663d96b478e2307f85548957d65740e2673e9ebd1352829038f462b8fd3  
b5681da55c02523853525ea0ad647e71ac2c5a8893e603ac97e56c04ceb2f2  
6f5c5b4b6d94ab811380fd00f2208fe86535086aebfd35c29120624c04fbb611  
3929d9c556350253766c209fdb83c95fccd342a28099355d00bc863f4eef596  
eb0b42ebcc7c79491ccea205ea0b8059fbb8a5726c5949d2b15e7e29c51fc9b  
02eela4fc357b5f1bef9c4add46a2a920c2fbf08a37eb1514bfa15110a4392a7  
4c6f13c50c5cfff97531098d7cd23b60eb35c4a428b46c55386e1010c4ba7f70  
e4c7ecb7575f3063a71e84dfdcf09a58b2cdb0f99f27ed378610d25cbad7bfa6  
ba0d59189cfe88eab9b46d7e6db0307eabe4198e99bd71f779ab66581e0912fc  
7b1d2585245e9a12687a975cd5e8e1dcc045d5f891c4c685db07cf81e77389b3  
63eb6bdfc39b27ff84c97eefee162e3b451fe6914719cb6436d855960ff915d7  
cea6adeafdfcl1c05786c49f923a474ffdfc3153a06e6ed0b0ad220d72524434d  
5273c0aab6dde4e91476d581a2695a60de6d9f44d77aa08266e938eeb4a9597c  
9b64986059e49262a4eab2454e14015ad0536c42733a5d77d7995c2a20446009  
ebfe5632c80c08ed2b97af35066489f597eb1b1f11f04f60e0c9040159c44ab3  
e60e0a15229d191228bed17bbc3ac939b3c67ceel35f352c27216c9c31f72a3e  
87040c5f619306eb0b6cca2a9ce7b22a1694d00ca9c05e315126457f26ce84f9  
617241860782f864b473d84017491902b1bdc8cdc5800dd46127fb80a71c095b  
473a562529b3b1e7e437e158a5f6666e9974d005b062c2309e6dce98f9b658c6  
e3f9a216d58c8c9142bd1c8c85a9da872ebbfad3fea9d9aba2b68c0e8f19c6ff

```

5f00584d45daf9d6c9d69ed04b8da8d687258b77807927612c530446fea7697a
e3f926698929bc6a5a8cf3e2024c0f0c5ee57b5869bf981881caf9e3665fc7f7
efc678929f87a56eaa42ea4d1ff6691822dd79a47096b776d1d8f01456e5873b
0738406c382c573ae9cde2d9e7f231b6cc5c676e7cf43963373013a58075381f
f0949be084546d72e4f8a3e5fe4aa5091add234e2afe0030b1b663ae9d2d3241
0986b9402aaaf2465b74a5e2d0bc38e3a92bbddd8a1fed7b948c23cce6f8c08f
e356835ba65b0f984068616ef48138efd89bf357a54d2ebbf376cbdcc69c5f1f
61c64d2794bc06ccb9abdf66e25085d8c830e2ae3b0fe0f07a7af8b9320bf342
970997d67d7c12593a8fbfade635aac53083a7022c47d5f77a52b57b598da939
2ae6d86afc46fc06455181b9c75a646dc21f81e4bf213753de737fd2a1400279
20add35a223f9f5f4465ceb60c03ed0455a333a5cc83adbf43f1f42c2ccb8328
c21c7ab7faed2b21cfade2da55223aaab2af9b41c7332341746341b39aa2f438
15650f5480511424cfa6901779c4d18b638cc0287aaaf31680338d20b17c7449
fdc6a278a8d96a82ee4c4eca40125e2d65290071c7aef1be6a991598fb9d5951
2523bcd4b38c566b8e80a73ae333e134414327ef1d83c47c49dfe7936df1338a
5e247787868fc84fdcb95ac89c185c4bb5fd57b2338ac42b41c10a823df39624
f36b15a2f067584e06ca2e08ccaff1618fe01dd06df3512e0b724dec8506da24
215acacc2c51b82ad8d302002fb41068b1da4f8bb147987b3516bad5dbddf013
18fd3fa9bc43702ac498c719d95f2e841b622a5e4848a3c5c262959992ea7a7d
72ca8a368028f497dfad93355cbb1bb9786d14ff2cf590317848f95856427110
dda36f5192a816ce9c8816cc7b7bfc804efc40085a3850b89f1e7fe5656dba410
f906a97c32336c1ae7e81737a83e087354e428da8538d948dbf5dfacbf59dd2b5
fd3bc803f4ba432c9a739df2cfa9ed9484320f97edff1a48c6b86b3002cfb772
dd5e562bc4c3d683ed964b6199fa0514b0790d958095b7b85c6be875fbb559e1
930146ccea63a388a194fe09c3dea03be52de27e901017afe809af630a7382bf
5c4cd4d1b8f41579fb4348ede4ca05f4cd3f139a31b2544e516dbe4086b9bb4b
2bed47e2d230982dd5192429d377b7c0745cc068e2f5a4aa04c7ff87209ed125
9976a0fc9b25e9e851d4e3502c02c85d6dff029e211d01ebf0e9e7188d568f84
37d813b0f122f2fb17603b693ed9c38f17cfd50b815e6d9dfc0ed2ccf19f6399
274a1420f235a59d8bf724345e14e45d9e4be8934dfc3fa92678db61d7118bf5
3cb8a2225b335f7eae50e3f941237628db76d8ea38f77a72af3a26c81fe43523
b335535a5d1db7c38f341082bb5734d089e8ae309cfda3a0bcb5cd5b097113c8
edf9616aa4f6e6631b9125276fb3f680a34341c3db668dc6cad45fc93b2708ca
2af75ccce734fd191c50089dad53982fddae02531ff93e1f21ff395fc0a12874
edf06b6f9647e95a7324586c71dfd91d901d621858190fecdd0ccd110bbac59f
96cb884c3c93994748a56f41283bfc41fb89052153a894588c3cb9017f3d6632
6c985637e575acb812346342654025d602de3ba940c19ac1a633dffda977b529
b8013e19c1d6d0680f4dae62c924450ae66aab82f21473061dab3d62b247f907
e3551939ad3f5465e9d08a82bfea17eeal6b2b923757477f993000b2f43b70f
28aaab1fe9a26ad1fd3361616c0b0e242fe76604b7033a1f30e97e28f526ca3c
880fe2b8d9d1b0c9ff188b31cb9d97425acab9b216d98a6ae355e583da71e886
4ee3d16b0759796190ef545c1e62bfef92af6ca147b13244d6c892fc8ef223ab
3f43f924c2f466097ee8' }
}
}

```

#### C.1.2.3. Both Format

```

-----BEGIN PRIVATE KEY-----
MIIP/gIBADALBgIghkgBZQMEAxIEgg/qMIIP5gQgAAECAwQFBgcICQoLDA0ODxAR
EhMUFYRXGBkaGxwdHh8Egg/ASGg9kZeOMes93biwRzSC0riKX2JZSf2PWKVh5pa9
TCfYU/ppuBmQI+jNZ43Z+r+QR2Rv/QtyzH95WAWnHnDSNxsFY+PNM0YUnIyevPI7
Ck5akA7qnGVieQp8Y+OGY9qi3dtuSA3EBaHnAZSLdIQe9cwcPyvzJ5culRBRDNU3
XswIVXF3EYciIYYjgQAEJHeAYUdQB1AXFwNVBFJRJUCYOARhdXIiRBCIaGCGRGEn
R1ZxgICGZoZDMkRBIgQ2OGZ1AoI2NCRDIgVzZBBkVVR3InVWgUM2FGJVCCBkN2hU
aHVDU3UQAHGDM4BUDQUlGHUoGIQ4EQhyYCAgCFiDAYNhE4KCEgYXEVEHaHiIeGQ3
VGAWVxVQHGIzGcnMogGZHQYVnYhgDGCdmQVeCRQJWRmQxE1BDZHGjBjmcxQwEWYG
VYZHGDAiY1A4R4YRASAjVhFhN4YHhTISQAdUeIIwQ2ZhFmBCVUGChWBTZ3hWOENE
MGMmEHcHMxhCchQRfLMDhSdoZ0YBUiI3NTIHZhB1BGgSSAZmAwMmUjEkRUCIADGA
iHZyFzBxgkchUSEAEWVEDIZhCiMzgIZgZEAduhWEIDaAEYAhGBgzF3NUU0iBAESG
U2dDcFdyWIM0YDhCMoVoEAYEJgQlhfYCNWggUYOGOEMkISJCRWRYWGdxRXKFBHiH
FxxGGINGhoZBVLcBfLAmRnAGCCZiJzgxckByVzAHJyiGIGZliGgmBwZAIDMDQ2Yx
VUZCRTRWZxhzRWWDcCJQHghWKIBwNnCEYjcXEAZXFlhHeHCGVVN4IjUURncoVnMD
IocAFDMgYXFYRVJmMlAmUTNHdzgDVRZDE0c1EGYnUXV0AkaIgXBnQ0aBhgF2UkUz
MiChBDQ0AQMih2NRVSZQgTB3RURBaBVBg2NkESBAJocwQ2d3EoCIRjVUuwBiRYEE
WDZRJIQngDRRZmNYQ3hWAUZRFXQjiUNmhSJHdzE0UBeDYkIFUABkhEcSNECIAGBH

```

NUBXgzNjCCEGFSJSBySIUTSGNwZ2IliFcSZWc0doFkZGhCWHCBInBVAIODIAIyCA  
ZjRTNgAzRoVyRwYlVAAldxInUjBxQlNodDdFcAVmQyJEgoUgchgZMCBtNzNADyeA  
VSUwYlJQQGczRhMYBygHFySdd2NFcxhYUWAjM0Q2JRZDOBYIWHc0YkKIMAcDZYU3  
VQB1UjFQNWITJGMENwhoBjYVAwMAQ1hjVwgCEQZkc0YlImIDMEOAIQhShleDIQeI  
Z0gIVjR0NnNChAWEZoQUNwBVEIc0Jkr3IRJzhHNlJkclDxRHBBeGRCYCRxGHQIEi  
FmBYRxeBNwZ2gIFwWBhVhUcTY0IQdVgBYlglRhEA4RxEDOHQmKCR3QTZVRCcHNG  
NXdlAGYlYmhCAhJGg4ZGFmRgMSJTiIRUAIRXNEZHVEclYFRhZoRmMigGOCcVYyhx  
g4QGUir2gRYGYhMDMBhoAoATHGMFBWVyOHWDZXIyMGIARhImBmUwDvCFMkEyJ2c1  
FwgBUwAWKEYBNih3ARGIFVcTFUZDEXBHMogoVjaCNFVQQYyNzWMMREWh1BRBCVEFE  
J4UiERcXiBU2hRV0RxZiVTZVg2MCUCVhdodTJxNx3I3BXFHYXE2UYQSQjZkRGZB  
QlIFIQhRVwMzY4YCWEJmKBSBEFRiaBcwOHVkmYfLiFaGY2MoE0BiVAEgQIh1r4hh  
cWV2I3JiNiZwMBFRFWMGUHU1AhIhCEJlMUNVZxEVJXIBBoU2MBUFV1hgWHhDFDEy  
eHiAhzhHiGN4gYe4c0JheDiFJGZ3MlBgIRUUZCOCMmgBNUQHg0dThVNXUoMjJNRh2  
ARUHNdJXczM2VRiGfYfhaCQYQIEiMIQUSBUSARAwJHdyQlRDZgZ3F3B2AwFFJUA1  
ABg4cyN3NSZQhJvxE3NEGWBSd0VlU3MAhYN3hQNRIRFUgGKIUBgCaBOGUgU0aAEy  
ByQYAyEwBXI4ZAdkJxFBAYOFJVEGMmBxBIZRdoM4KfcNjYjVFGHNQgxMohjdmYUJj  
EWdQMxElU3ZBdgMUMxdyEiNEGKguTlyeOPr5nrBNeKczJxERfDPxjsOh+HQzdz2l  
IZgEp+2aVvf81nolULokuMWIYpwCFHX6PVbV1s+7Ggm9qNFN5iLd/xbYvJmxQnio  
rxl2vtFXZy3ZwyMW+X6Nqt742dppWGclVn+5aImZDUvWvJwZW5C3QpXlZlSkJXwn  
EMF1sBU/KREyJc63q7mtRucKi1PDnqZCzuSzy0JiDoY86LZQzorC2SNyGhaHAjxn  
Ooy7awPVHNGX6MNG663Ok5UPiM7iAdueMghD4p8wDZoZUALwPMrycsaeTu9p+7il  
Xv18or7ZkNLtTyKEj5xwFqvFTpxH008GwP+lb812KrnLqRRtdyUhiW0yQNCrbSLJ  
MXH71HeIt25yBC3vCHjSPfYxoaHlpgJ2ht5bShDpEGnI8roCWbBNZAnallZ8pS2k  
lwJuWDOUzvwfAea5iOifl2eit+FnLeuaHio/zIY6qRUXwzRiBgG0/nlzDpNjNfS2  
+8TjJpUUXCtfahJ/7MCid0UevD/VI0RPnufJw0U081bbVE/DHBv95fZcd+ovfC6u  
TFXrrxBCCcVm/U66xxx6YsdJUoF65nVQTZWZsbditqyhaKgySMnZrbD0sVVuV1lJ  
C7wMeQB5WtchIwOLZi9k8QapmTaBollZr3vJeiNb6ShMW8RabJDLHCmZxmPZa0e0  
Iwf4VUiVfWV0DiZz6evRNSgpA49GK4/TtWgdpVwCULI4U1JeoK1kfnGsLFqIk+YD  
rJflbATosvJvXFtLbZSrgROA/QDyII/oZTUIauv9NcKRIGJMBPu2ETkp2cVWNQJT  
dmwgn9uoPJX8zTQqKAmTVdALyGP07vWW6wtC68x8eUkcZq4gXqC4BZ+7ilcmxZSd  
KxXn4pxR/JSc7hpPwle18b75xK3UaiqSDC+/CKN+sVFL+hURCkOSp0xvE8UMXP/Z  
dTEJjXzSO2DrNcSkKLRSVThuEBDEun9w5MfstldfMGOnHoTf3PCaWLLNsPmfJ+03  
hhDSXLrXv6a6DVkYnPi6I6rm0bX5tsDB+q+QZjpm9cfd5q2ZYHgks/HsdJYUkXpoS  
aHqXXNXo4dzARdX4kcTGhdsHz4Hnc4mzY+tr3+ObJ/+EyX7v7hYu00Uf5pFHGctk  
NthVlg/5FdfOpq3q/fwcBXhsSfkjPHT/38MVOgbm7QsK0iDXJSRDTVJzwKq23eTp  
FhbVgaJpWmDebZ9E13qggmbp0060qVl8m2SYFfnkkmKk6rJfThQBwtBTbEJzO1l3  
15lcbKiBEYAnr/lYyyAInI7SuXrzUGZInll+sbHxHwT2DgyQQBwCRks+YOChUinRks  
KL7Re7w6yTmzxznzuE18lLCchbJwx9yo+hwQMX2GTBusLbMoqnOeyKhaU0AypwF4x  
USZFfybOhPlhckGGB4L4ZLRz2EAXSRkCsb3IzcWADdRhJ/uApxwJW0c6ViUps7Hn  
5DfhWXX2Zm6ZdNAFSGLCMJ5tzpj5tljG4/miFtWMjJfCvRyMhanahy67+tp+qdmr  
oraMDo8Zxv9fAFhNRdr5lSnWntBLjaJWhyWld4B5J2EsUwRG/qdpeuP5JmmJKbxq  
Wozz4gJMDwxe5XtYab+YGIHK+eNmX8f378Z4kp+HpW6qQupNH/ZpGCLdearWlrd2  
0djwFFblhzSHOEBsOCxXOunN4tnn8jG2zFxnbnz0OWM3MBolGHU4H/CUM+CEVGly  
5PiJj5f5KpQka3SNOKv4AMLG2Y66dLTJBCYa5QCqg8kZbdKXi0Lw446krvd2KH+17  
lIwJzOb4wI/jVoNbplsPmEBoYW70gtjv2JvzV6VNLrvzdsvcxpxfH2HGTSeUvAbm  
uavfZuJQhdjIMOKuOw/g8Hp6+LkyC/NClwmX1n18Elk6j7+tsjWqxTCDpwIsR9X3  
elK1elmNqTKq5zhq/Eb8BkVRgbnHwMrtwh+B5L8hN1Pec3/SoUAcESct0loiP59f  
RGX0etgwD7QRvotOlzIotv0Px9Cwsy4Mowhx6t/rtKyHPReLaVSI6qrKvm0HHMYNB  
dGNBs5qi9DgVZQ9UGfEUJM+mkBd5xNGLY4zAKHqq8xaAM40gsXx0Sf3Gonio2WqC  
7kxOykASXi1lKQBxx67xvmqZFZj7nVlRJS081LOMVmuOgKc64zPhNEFDJ+8dg8R8  
Sd/nk23xM4peJHeHho/IT9y5WsicGFxLtf1XsjOKxCTBwQqCPfOWJPNrFaLwZ1h0  
BsouCMYv8WGP4B3QbfNRLgtyTeyFBtokIVrKzCxRuCrY0wIAL7QQA1HaT4uxR5h7  
NRa6ldvd8BMY/T+pvENwKsSYxxnZXy6EG2IqXkhIo8XCYPWZkup6fXLKiJaAKPSX  
362TNVY7G714bRT/LPQWQMXhI+VhWQnEQ3aNVUZKofS6ciBbMe7/IBO/EAIWjhQuJ  
8ef+VlbbpBD5Bql8MjNsGufoFzeoPghzVOQo2oU42Ujb9d+stZ3Stf07yAP0ukMs  
mnOd8s+p7ZSEMG+X7f8aSMa4azACz7dy3V5WK8TD1oPt1kthmfoFFLB5DZWAlbe4  
XGvodfulWeGTAUBm6mOjIKGU/gnD3qA75S3ifpAQF6/oCa9jCnOCv1xM1NG49BV5  
+0NI7eTKBfTNPxOaMbJUTlFtvkCGubtLK+1H4tIwmC3VGSQp03e3wHRcwGji9aSq  
BMf/hyCe0SWZdqD8myXp6FHU41AsAshdbf8CniEdAevw6ecYjVaPhDfYE7DxIvL7  
F2A7at7Zw48Xz9ULgV5ntfw00szxn2OZJoUIPIlpZ2L9yQ0XhTkXZ5L6JNN/D+p  
JnjbYdcRi/U8uKIiWzffq5Q4/1BI3Yo23bY6jj3enKvOibIH+Q1I7M1UlpdHbFD  
jzQQgrtXNNCJ6K4wnP2joLy1zVsJcRPI7flhaqT25mMbkSunb7P2gKNDQcPbZo3G  
ytRfyTsnCMoq91zm5zT9GRxQCJ2tU5gv3a4CUx/5Ph8h/zlfwKEod03wa2+WR+la  
cyRYbHHf2R2QHWIYWBkP7NAMzRELusWflsuITDyTmUdIpW9BKDv8QfuJBSFTqJRY  
jDy5AX89ZjJsmFY35XwsuBI0Y0JlQCXWAt47qUDBmsGmM9/9qXe1KbgBPhnBltBo  
D02uYskkRQrmaquC8hRzBh2rPWKyR/kH41UZoa0/VGXp0IqCv+oX7qG2srkjDXR3

+ZMACy9Dtw8oqqsf6aJq0f0zYWFsCw4kL+dmBLcDOh8w6X4o9SbKPIgP4rjZ0bDJ  
/xiLMcudl0JayrmyFtmKauNV5YPaceiGTuPRawdZeWGQ7lRcHmK/75KvbKFHsTJE  
lsis/I7yI6s/Q/kkwwRmCX7o  
-----END PRIVATE KEY-----

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
  }
  OCTET_STRING {
    SEQUENCE {
      OCTET_STRING { '000102030405060708090a0b0c0d0e0f1011121314
15161718191a1b1c1d1e1f' }
      OCTET_STRING { '48683d91978e31eb3dddb8b0473482d2b88a5f6259
49fd8f58a561e696bd4c27d853fa69b8199023e8cd678dd9fabf9047646ffd0c
b3cc7f795805a71e70d2371b0563e3cd3346149c8c9ebcf23b0a4e5a900eea9c
6562790a7c63e38663daa2dddb6e480dc405a1e701948b74841ef5cc1c3f2bf3
27972e9510510cd5375ecc085571771187222186238100042477806147500750
1717035504515125471838046175722244108868608646012747567180870666
8643324441220436386675028236342443220573641064555477227556814336
1462550820643768546875435375106871833380547505258075281884381108
7260202008588301836113828212061711578768788878643754601657155084
7188660727328806647418567621803182766415782450256466431135043647
8012667314301166065586471836886350384786110120235611613786078532
1240075478823043666116604255418285605367785638434430632610770731
7842721411165303852768674601508237353207661075046812480666030326
5231244540880031808876721730718247215127801165447486617223338086
6064468352158420368011802118183317735453488100448653674370577258
8334603842328568100604260425845602356820518386384324212242456458
5867714572850478871718061883608686415650811650264670060826622738
3172407257300727288620667588682607064020330343663155464245345667
1873456583702250846856288070367084623717100657175847787086555378
2235144677285673032287001433206171584552663250265133477738035516
4313473510662751757402468881706743468186017652453330872104343401
0322876351552650813077454441681541836364112040268730436777128088
4635545300624581045836512484278034516663584378560146511574232143
6685224777313450178362420550006484471234408800604735405783336308
2106152252072488513486370676225885712656734768164646842587081227
0550083832002320806634533600334685724706355400357712275230714253
6874374570056643224482852072183330205337334077278055253063525040
6733461318072807172483776345731858516023334436251643381608587734
6242883007036585375500755231503702132463043708680636150303004358
6357080211066473463522620330438021085287578321078867480856347436
7342840584668414370055108734264477211273847365264725771447041786
4426024711874081221660584717813706768081705818558547136342107558
0163583585184403847110338742628247741365544270734635777500662562
6842021246838646166460312253888454008457344647544725605461668466
3088063827156328718384065224768116066213033018680280138463050565
7238758365723230688046122606651675570532413227673517080153001628
4601348877011188155713154643117047328828563682345550418627656311
1168750510425441442785221117178815368515744716625536558363025028
5576875327137103723705714761713651841242366444664143520521085157
0333638602584266281481105462681730387564332165885686636328134062
5401204088654788617165762372623486703011511563205075350212210842
6531435567111525720106853630150557586058784314313278788087384788
6378818138734261783885246677335060211514642382326801354407834753
8553575283233518760115213432577333365518861581616824184221223084
1448151201103024777242544366067717707603014525403500183873237735
2650863571137344816052774565537300858377850351211154806288501802
6813865205346801320724180321300572386407642711410183852551063260
7104865176833828572762354518735083132886376661426311675033112553
764176031433177212234418a82e4f5c9ea0faf99eb04d78a7332711117c33f1
8eca21f8743376ada5219804a7ed9a5557fcd67a3550b3a4b8c588629c021475
fa3d56d5d6cfbbl1a09bda8d14de622ddff16d8bc99b14278a8af1d76bed15767
2dd9c32316f97e8daaef8d9da69586725567fb96b59990d4bf0bc9c195b90b7
```

4295f5675b24257c2710c175b0153f2911328c2eb7abb9ad46e70a8b53c39ea6  
42cee4b3cb42620e863ce8b650ce8adcd923721a1687023c673a8cbb6b03d51c  
d197e8c346ebadce93950f88cee201db9e320843e29f300d9a19500d70a4caf2  
72c69e4eef69fbb8a55efd7ca2bed990d2d3b582848f9c45c2abc54cfc47d34f  
06c0ffa56fcd762ab9cba9146d7725218963b240d72b6d22c93171fbd47788b7  
6e72042def0878d23df631a1a1e5a6027686de5b4a10e91069c8f2ba0259b04d  
6409da96567ca52da497026e583a0ecefcl1f01e6b988e21f9767a2b7e1672deb  
9a1e2a3fcc863aa91517c334620601b4fe79730e934935f4b6fbc4e32695145c  
2b5f6a127fecc0a277451ebc3fd523444f9ee7c9c34534f356db544fc31c1bfd  
e5f65c77ea2f7c2eae4c55ebaf104271c566fd4ebac71c7a62c74952817ae675  
504d9599b1b762b6aca168a83248c9d9adb0ceb1556e5759490bbc0c7900795a  
d72123038b662f64f106a9993681a25d59af7bc97a235be9284c5bc45a6c90cb  
1c2999c663d96b478e2307f85548957d65740e2673e9ebd1352829038f462b8f  
d3b5681da55c0252523853525ea0ad647e71ac2c5a8893e603ac97e56c04ceb2  
f26f5c5b4b6d94ab811380fd00f2208fe86535086aebfd35c29120624c04fbb6  
113929d9c556350253766c209fdb83c95fccd342a28099355d00bc863f4eef5  
96eb0b42ebcc7c79491cceae205ea0b8059fbb8a5726c5949d2b15e7e29c51fc  
9b02ee1a4fc357b5f1bef9c4add46a2a920c2fbf08a37eb1514bfa15110a4392  
a74c6f13c50c5cffd97531098d7cd23b60eb35c4a428b46c55386e1010c4ba7f  
70e4c7ecb7575f3063a71e84dfdcf09a58b2cdb0f99f27ed378610d25cbad7bf  
a6ba0d59189cfe88eab9b46d7e6db0307eabe4198e99bd71f779ab66581e0912  
fc7b1d2585245e9a12687a975cd5e8eldcc045d5f891c4c685db07cf81e77389  
b363eb6bdfc39b27ff84c97eefee162e3b451fe6914719cb6436d855960ff915  
d7cea6adeafdfclc05786c49f923a474ffdfc3153a06e6ed0b0ad220d7252443  
4d5273c0aab6dde4e91476d581a2695a60de6d9f44d77aa08266e938eeb4a959  
7c9b64986059e49262a4eab2454e14015ad0536c42733a5d77d7995c2a204460  
09ebfe5632c80c08ed2b97af35066489f597eb1b1f11f04f60e0c9040159c44a  
b3e60e0a15229d191228bed17bbc3ac939b3c67ceel35f352c27216c9c31f72a  
3e87040c5f619306eb0b6cca2a9ce7b22a1694d00ca9c05e315126457f26ce84  
f9617241860782f864b473d84017491902b1bdc8cdc5800dd46127fb80a71c09  
5b473a562529b3b1e7e437e158a5f6666e9974d005b062c2309e6dce98f9b658  
c6e3f9a216d58c8c9142bd1c8c85a9da872ebbfad3fea9d9aba2b68c0e8f19c6  
ff5f00584d45daf9d6c9d69ed04b8da8d687258b77807927612c530446fea769  
7ae3f926698929bc6a5a8cf3e2024c0f0c5ee57b5869bf981881caf9e3665fc7  
f7efc678929f87a56eaa42ea4d1ff6691822dd79a47096b776d1d8f01456e587  
3b0738406c382c573ae9cde2d9e7f231b6cc5c676e7cf43963373013a5807538  
1ff0949be084546d72e4f8a3e5fe4aa5091add234e2afe0030b1b663ae9d2d32  
410986b9402aaaf2465b74a5e2d0bc38e3a92bbddd8a1fed7b948c23cce6f8c0  
8fe356835ba65b0f984068616ef48138efd89bf357a54d2ebbf376cbdcc69c5f  
1f61c64d2794bc06ccb9abdf66e25085d8c830e2ae3b0fe0f07a7af8b9320bf3  
42970997d67d7c12593a8fbfade635aac53083a7022c47d5f77a52b57b598da9  
392ae6d86afc46fc06455181b9c75a646dc21f81e4bf213753de737fd2a14002  
7920add35a223f9f5f4465ceb60c03ed0455a333a5cc83adbf43f1f42c2ccb83  
28c21c7ab7faed2b21cfade2da55223aaab2af9b41c7332341746341b39aa2f4  
3815650f5480511424cfa6901779c4d18b638cc0287aaaf31680338d20b17c74  
49fdc6a278a8d96a82ee4c4eca40125e2d65290071c7aef1be6a991598fb9d59  
512523bcd48c566bdc80a73ae333e134414327ef1d83c47c49dfe7936df133  
8a5e247787868f8c564fbc89c185c44bb5fd57b2338ac42b41c10a823df396  
24f36b15a2f067584e06ca2e08ccaff1618fe01dd06df3512e0b724dec8506da  
24215acacc2c51b82ad8d302002fb41068b1da4f8bb147987b3516bad5dbddf0  
1318fd3fa9bc43702ac498c719d95f2e841b622a5e4848a3c5c262959992ea7a  
7d72ca8a368028f497dfad93355cbb1bb9786d14ff2cf590317848f958564271  
10dda36f5192a816ce9c8816cc7bbfc804efc40085a3850b89f1e7fe5656dba4  
10f906a97c32336clae7e81737a83e087354e428da8538d948dbf5dfacbf59dd2  
b5fd3bc803f4ba432c9a739df2cfa9ed9484320f97edff1a48c6b86b3002cfb7  
72dd5e562bc4c3d683ed964b6199fa0514b0790d958095b7b85c6be875fbb559  
e1930146ccea63a388a194fe09c3dea03be52de27e901017afe809af630a7382  
bf5c4cd4d1b8f41579fb4348ede4ca05f4cd3f139a31b2544e516dbe4086b9bb  
4b2bed47e2d30982dd5192429d377b7c0745cc068e2f5a4aa04c7ff87209ed1  
259976a0fc9b259e851d4e3502c02c85d6dff029e211d01ebf0e9e7188d568f  
8437d813b0f122f2fb17603b693ed9c38f17cfd50b815e6d9dfc0ed2ccf19f63  
99274a1420f235a59d8bf724345e14e45d9e4be8934dfc3fa92678db61d7118b  
f53cb8a2225b335f7eae50e3f941237628db76d8ea38f77a72af3a26c81fe435  
23b335535a5d1db7c38f341082bb5734d089e8ae309cfda3a0bcb5cd5b097113  
c8edf9616aa4f6e6631b9125276fb3f680a34341c3db668dc6cad45fc93b2708  
ca2af75ccce734fd191c50089dad53982fddae02531ff93e1f21ff395fc0a128

```

74edf06b6f9647e95a7324586c71dfd91d901d621858190fec00ccd110bbac5
9f96cb884c3c93994748a56f41283bfc41fb89052153a894588c3cb9017f3d66
326c985637e575acb812346342654025d602de3ba940c19ac1a633dffda977b5
29b8013e19c1d6d0680f4dae62c924450ae66aab82f21473061dab3d62b247f9
07e3551939ad3f5465e9d08a82bfea17eea1b6b2b923757477f993000b2f43b7
0f28aaab1fe9a26ad1fd3361616c0b0e242fe76604b7033a1f30e97e28f526ca
3c880fe2b8d9d1b0c9ff188b31cb9d97425acab9b216d98a6ae355e583da71e8
864ee3d16b0759796190ef545c1e62bfef92af6ca147b13244d6c892fc8ef223
ab3f43f924c2f466097ee8` }
    }
}
}

```

### C.1.3. ML-DSA-87 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-----
MDQCAQAwCwYJYIZIAWUDBAMTBCKAIAABAgMEBQYHCAKcKcwNDg8QERITFBUWFxgZ
Ghschr4f
-----END PRIVATE KEY-----

SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
  }
  OCTET_STRING {
    [0 PRIMITIVE] { `000102030405060708090a0b0c0d0e0f10111213141
5161718191a1b1c1d1e1f` }
  }
}

```

#### C.1.3.2. Expanded Format

```

-----BEGIN PRIVATE KEY-----
MIITOAIBADALBgIghkgBZQMEAxMEghMkBIITIJeSvOwvJDBaoL8zzwvX/Z153HX
q0G5AljPp+kOyXEk2OnuTpChbGAvXsm8OFF9ww4ynVqydn09hftTJsDAPd2OJiGdQ
tXwk2z/AEuYe3l1lMzc3T6cSSZFUmVJDSW0GN8s74FpZSCNb95h1+JbY/gyrMMhJ
SntNYxWqrxYKxiQ2ZCIBSBYRCReslAKJIKUsYrhFAEUqCJZwkBJuFJNwLEYQhERR
WJaRDkKpgrJByQhxxChoBJaJSECFmyJtHChkWRJBnLiRhASJRJAfyzRioIaQQCaS
IJkpEwVpXDRopDKOGSAsWUYQCaRJI0JNEjZhWBBLASiQGjNMmYYx06JJCyiLQxQo
wDiBaxVNWyIGCidIiZfSLCilw8BNpJghmEAg0UKGy0BwW7BxnJYswRIGU0YJDEUC
FEZukbQhVLCM5EZCmicMASEle0EFWkAiE8kMoBhAUswIwyzQsS8hoG6RgSYSEYzAp
SqBpW4AE0jgKFCZM4rJei6IRJEZJxBRSc0JxA7IQkiiAASSI4wgrCgUoGcSBACai
3ERoQhIiRAAQySZqDlCcx4MBEmRSEGDYNETdCIhiMY7KRDJgIoaABCJJEbBMkXJhx
goRxhDJSUBAxnEIuGqgoAgIRAcCJC8cfiirLIsJkTIiRXIJoE6VkUCCGIQQCkZRE
SCIwIjlkApieCaKIGRkpREiMIpUMoQRYBiDwEieEQGgaEG0mFiQZK0zYI28BAWLZR
DKcJjCRhmZBkjmKQWysQEKNJAYVhQzKKEZhEyLIgBDhBEEcsGcZEHCUsbIgw2UZp
myAAG0aCWqSAW6BJGJAlACaC8IxWkByVMYgwbAxJLFNEJUoFAAKoMhNVKKII5iB
YJAEAhYsEyFAkYaNCMKRkRQm0LQMCCzGUUQuBBEmACkRk8IIY6QxIgAowRQIDEAs
QRQGNcByVCIGiwhNoUhpEDBBHChJRBiOzJZI2UJQGwZJDEWIiWQNIDAuI4UsFAcw
QLaFTMAgRIYgGQBsvAJIzIhswQYySRSEBMDQE0ko5AYJ08YQyChMIzLEUqRkzKhJ
RDgyComEADQsIoWNEDEJCTJlHImMQEApIYUACaFthMBk4gItSARAEgm04EIuk0QI
EhBqAYQFkjCKyzSOoiYuXIYRCzUIGBAAAJmJCOJ0YQAJEzge7JJJChGGAJxoDiQ
irRE05YtoxAiYchwBhQQ8gEQUKNXCZBRKJtSBIOQDilCxSCckguy4KIA6NgGyUm
jLggJLCfMAJhCKcsgzhkVdKJAQQBI0mEApVp0arNE6QMkUYNYZSAkDhFXMZQARcg
U8YomxgQQRJokBIhwBCEQhasU4IpgSZJ2KQFmiYkJAMP4EAm0gJIESRoEZmJmBSF
ySANUBKMHAGQAAAAJUowSiQWbSF0xRlCkBuESllGMJMITRl2DBpEDBSGTFmjBiK
yMAITJgwo6YgQRYiGAUuIiUqZLglCrMBYyCECYAJGSgOAheBo5QR45hsWCAhCUEQ
YDYiCAZxESKFwqCFwMaEXDgGy7ZpFISEUyKCoaZAZIYAXCYioKgImDyrlCBBQ8SQ
SBZoGxZSGjccUCBCSEiKIBFB4gBswMIMFAZJETFNGQYKiUYJG4FlRMgAggZwABZy
zCRQikKJnJaQZChwkrJomCZiYZRAWaRaJ2EJkGiFOYpBkIcgkiyhtXEKSOMZNDIWA

```

zIhN1EKNQjSKCwRRwyaGJCWBEjUGoEQEyJSBW7QxHAGGXCQIAydaqIMIL4YCQGbRt  
o0YMSxhgUMYSg5ItERUEogAEIUgu2BYG0hCKg6ILCDENCThr2UhJCxZMIz1LGRkC  
SkQJ0bIhC4MsIyWfKxaFRKBEG4NQAIjYsSwSAmxR1IZNgGBMK2UYNIkVhyLRAoUit  
ArgJABREm7YRC5eMQBBKghRq2pAFHAKODBlyo7SNJDBQEYcJZMYo5BiSmLRsYRZR  
QEYOHDJI2iBRiDaKi7EhgpAoGhUy4hhhkgsOE7aQExNoyYRoTEBtCzMAgUZn0jgM  
BJaBpIhQApCFIrAE06Rx0oAQypZAUaZBPIQo4AhSCzCM0jgKDClRw4IJyiCR2DaS  
o6YokkIiohYBGjSGN9mmWRaYgewhz0gRhp0dfxOfBTfpxGEWFQF/ReAivHgYjnt  
s05ayovxNpZ3tEescYrEfYUMTXewvjHcn1COOXjyQnSrAYX3J6vf9Z9EkDcb8EYQ  
42TmTsh1750g3JQHfh4WYyeobirUWFGsqP3dDe5s8x9F66t3ITbYnRqNawJb3gv  
YqfwGqbWat3uyQsJxmmFoCMH4KHK5ZimcyTboPUvIkMidikyVwZc035eHP4d/U0N  
8IbfISQ0FKLSfiAjCoKb50tMgsFtnFeLDl4ZgzLgAHS7ZGEvqxfUyJccto5e2rA2  
nxFXs0aavYOE4tlVPxt454bh7p0LmNOfg8zs830evTqdY67HZhZKEBcaT9jGPa8Y  
LEISWMXlKapVy3664uFlIxXh9x6KdBMUENayR+3hHTTbkfbwiqJHj9eJZ5wElJ9x  
vAFx4H46i7VlPbvapBGMNq0bu+/hvxVHCnv5M3XZh1c9sPbItDO3eWZhURZ2X8g  
33RVvfNwOzjQ9+ttNBEfyUCyXAVDt4jt2p0mgQ6sPWzJxRMnws+D6IfUCJ4ZaV4R  
rdg39vRAZDYPk/Mv7oqWY3Esa704yEq3tUgj7DY++QutZ/B/OYPvVUwez7IX9na  
8yBte0s5F/HIT6kuPGfYmID98uR/WgyZRZXbFwr0G6v1oltNwcQt1qnbJx52TeL7  
AVpJqFDHkZvkcaAjNuLjJf3lOsWZVU0KfeTvRexAw5lrr/MRvu512J4CrTH0vkvs  
CukZT17d2qZlB3YRbp8nD3dxSteo6JrO90t/99jb7Cf4AgqYUkfiazvSJSklouj  
fKkSlr5zUByZUYHlt3cJnQs2Mdo3AOE/02bhMb8Gs262sDRQkyCfCnv+uH92HWW  
BofBFjw1PX0qyQk3s06XjPL4Ia3JZiIC70iaF+e7Za4X2DuQ275qUBpOE0W+50Wl  
tTry5bo9HvP04FrFczPM8uUwNg/uZJKZArVx9v0uMFZSPmsBD3n4FeGPK7uMyJ+m  
/Hb3fInik88XWgsZWAD+ctLM3X115b2QvGrENDakQO+FLpocjFPeA78ZM2XXNary  
nFFiphfjZOf5RbaND7SP70BVj0VCL8w91QhmLPI/uI4ZVKpF0cXhFbzDbwWz4JjV  
VSIPQL4mKbNFB7hGTFTCel3seNqPImUFFHl6+GolEry34pIzee9tc8E3AGwbOPue  
N/kIheKQQApk469GAHzh04tfeXfV1119VmjkJ7y+fsHXxAjAVKSMGueXv5msvI0m  
BlIpNflmXqeCLZMPI+q/9407I2l1aeIEuUMUHgDAiBCVa+BSU2XbqlTtSMT2lkzN  
9cvTrucoLUoAANJ4TXuPqxay9/DVilcyse+8TrHP7etD/eebaezA++qh5rQHKGc7  
1LLpig1KjwL4U5UHMPKNnesS/MeXaLjhjkvaDliJMaL3HXZMLUUbMrHGXDqz0fu  
UTshlUxBwAyHOHLulM8U9GA3QlNh9L21SCH3EUYM666MB1CKkhn4j6a+2qZ47tUB  
lEoWrm97W7ei4eNX5w17mEYALHHLd6d1lq2YJAgdN/KS/UvouEw2EQ3HRDYCAB7r  
4LlsnQXoaSVtL/P5lRe379KjN3QFbLVnFnWotJLp9fJiDrjvk4HT0d8Zk4t7X/qs  
WbyBEPqHuol6PQF1+OQd0PgE8Rud7Q81K114NdBjB6jgxu9NIZBD0eHPRYkjo+ie  
Al2UU0c2bALz3WNo1OR+hdPSqXBb1XlhhS5aV5+TscUUxTn0nqEWOipJOw78tH9H  
SPapnhC/chGoLkrOGBNuKos+4KOA3NOz7z514bgVconWJGetSIugOSSukKht7cvc  
kx3Bcpjm73ZkXH0zCgXCzkD4m4VGjzV6IXdr4VRjEwTsTgS7RbNniQnHSvUc43A2  
TY9PfrHmHgAomCnJlh3MoMiypomKbEwnYAOkrdwxQVdzHl/M4ZusM/YlJALDuJ/yo  
Ai9JKQ4tU3YWL7qpgtFkU8gls19lFWNeqSvqcjZ7qlTeP56uppVCqBpBJ/ccuqJX  
8yT+/vFPCPvWWgSc0vs2JZSo4j/xomF9tbFY9vAc9Qqw7ZXG5wmEEWQQiwbhtAqw  
qxHECDAdPZ2Opp6WipYAs9F/OAEc4oB04sLhC/YZfGAtjQzn06PvLYli08nxLqM4  
er6SZrum4CsSTGx5KbrqatJECYRUoIDrdSPH07G3xbZ3X6urq76Qdf5Wh6pFE5e7  
nPzNBRJD6b9a7yQGLTnd5fziTp3b3hGRBS2Aw235+ENIcvJ37U9aHOjr07lggkpO  
TxABSEy2hfm+5NDdsMVxWYrCAhpmBv0jNFxvu4TwzgX+UnNFibewfGOI0605kxi/  
ATFQSQnfuvVI+dMqnNTGiTUKsRMwotOq0+0QWJZuuWE0Rl1UP9d5evVJ9Wjq6+lx  
9k/shUZ0kCuXVYdWmGLG6jQ3olHLvqEaaHvUP10L2JzSyrph1SGDDJk06LkiGe0l  
3KARxoqXV8ATvYN7Ldc043UfZPy0s3j3Na8V+pWflcW4XNnJEDr4ja7IqlT53J1aV  
bnZAE//SwySQDuQipXJSNuyS8euxnx2tTQNVl98xypEBvfga6pSK7c8heqj8zXoH  
caonU+GoI79BjVN3ov+mGyJlE4FTzobSYH3Qeksy0n9fKHJkFDHOMhilaqrv2a/F  
sNE81GwlfjJmnh7pRa3RmSkypbHlxWkcn0j3ZhT2gB4fJ14+5JVU78HpQ3Vudkl  
hTQg5NGnGuYv+Qyhk83WwvS+0mNBWq+aNQLLwqIuKmY8dkUAHNGQt7wXx1/q346H  
zlwkt202WE7TLnGwJoFC6j7WiYFXv5I76/AZLRv17jCn01FjSmC1BN3jii4RT3rp  
vxdtShi6KJWnu0tHREqbqNu0wSTNQbuzL0vLHeSMSrtRBgegAbWgALukNhi2wZ5D  
UXtFtCQFkotnxxOIGFi606QlEcJxb/nNMyA0tnK1L/FmEIBc2+dUSoqEtm4cdFpz  
wba82lt3uVHzbA96U3Lenl0fm7zeiEPGkJAC3aSHXmdXGvC+xYGFbDLAnCQOZk52  
HlfNDY3Ipxy5GKV2LREShc2LVhPdvQygisA0Kyve44+W+nVLSrCHF5wRPJOYaoED  
VuuUVAuTy53sSqkpD/EuwaouZWYb49WQdT2bGAUBsBhvCIDOh/R9OERHQObiB05  
g8tQbD6n/zBXmD6L8BaC+7APQwBTE8gsE5KRimFloTM4/+EamSwfs9EDKqZ5pBjI  
uk+KC8GZ4Qz2vXehT9lqBgk1FDSOOl0Q0roo2djaca+LpK0Zys0P84ErGsi4M9H  
VovEXXCmjmjGSaSDCuIYWQwaQ356I6VO/kT2cIbraXufpXgl8Lj3DwqSkibvszba  
4hgzoCghjNY3MgKpHfmLRQduoGFT3DaaNr/SoTLbed5JU6Kl+c1ZtdK9Akq8Fy9  
ZlSv/ly8K4jJpXLZmjQ/sxAab2Qu1KLg++i+829k7KJkpYh7XTYCHOPwQPUSQVR  
CFH8kxnxceoM7QuXtbn7XvmFGGvFIJj560dvZ7fMdmXUDYeXXLRaUPxkEAcZv3Y0  
Xw/fHgnv6fuADcEU5Gvgh5oZXMBocOI9JjHa5xw5lEgch2HEDQfFv8qV5xi3siWF  
rwPtNBdaRtV681GOMqf8GqRIJzKoGof3JPjS54Czo51FGjgPdcLWgMxyE+qx1KWd  
OUrjgQockIGNUvk/sGPi2LG1+o9gstWF2RNdZihG8Ti4aVMkLSux8uzfOJtn52UY  
F7jk5ksZPxqsUjqt8nSKndj/vCn01Fe2+XgbCKZ6GXXQMczXFUXAA3Q0BWwkNNE+

bEvuv0b8EiIsCy7MlhWdWuqOVU16CWUrBr98ppmnGZ5xbQXdTBBqPKzA9I2qbq6  
r7n6Uo8oosoqp4C5QDg8CZqmWgB0uD/R8Lxbe15Gwl5Ug4s8vPyV+H8dRxs7qJRD  
T6WJUv3Ld/FhNyaTMG26To8hbRyOxK/w/oNgpRxgdjZEFp/caoJn8uP5CaYbKmeL  
zmrpBAOoNrGnt+jNi1TDcIep4URG2V5pCNLU2/zGU+Av33cfcBp5ueWibtCpR4Qg  
cPO1cBdCIRIZ52F2LDfw0KHRuXUP7ld+EggRXGasB+wJHmo/xKpqJTvLqGjt0xVN  
yvUWL2FehUkKbKNC80xDrGGj6mv+79hQ4ZDrHY2k0otezusWeMAkM+zV1IslNkBC  
V+jKe+9YVfK4E+0vTECURaMxfJvholri+00rh5IbkEvYwU21FM7gRSUC/CdjdNsV  
yZ3qFazeGXxutSSYjjm2Moe+uGdoZaqjutG004yrFcvyekmHWeMgOr82npckLwsB  
VBSfFKwjPNTzoit/uPCTJb8qzo07a124oSgitoIUmmkTHMzliImECxE/x7C8xYQF  
v+h/H5X/wulvxVllZ+lDZN+qbZlabrma5N30JA==  
-----END PRIVATE KEY-----

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
  }
  OCTET_STRING {
    OCTET_STRING { '9792bcec2f2430686a82fccf3c2f5ff665e771d7ab41
b90258cfa7e90ec97124d8e9ee4e90a16c602f5ec9bc38517dc30e329d5ab276
73bd85f4c9b0300f776389886750b57c24db3fc012e61ede59753337374fa712
4991549af243496d0637cb3be05a5948235bf79875f896d8fe0cab30c84948db
4d6315aaaf160ac6243664220148161109112c94028922452c62b84500452a08
967090126e149370d446108444515896910ca92982b241c90871c42868049689
4840859b226d1c28645912419cb891840489449005cb3462a086904026922099
291305695c3468a4328e19269259461009a44923424d1236615810650128901a
334c998631d3a249098225431428c0388103154d5b2886088748233152942225
c3c04da49821984020d14286cb40705bb0719c962cc112065346090c45021446
6e91b42154b08ce446429a208c0121251341055a402213c90ca0184052c230cb
342c4bc8681ba4604984846330294aa0695b8004d2380a14264ce2b2448ba211
244649c414520b427103b210922880012488e308110a052819c481002022dc44
6842122244002ac9266a0c8731e0c04499148418360d11374222188c63b2910c
9808a1a0010892440413245c987182847184325251b0319c422e1aa828020891
01c0890bc7058a246522c2644c88915c826813a5645020862104029194444822
3022394a02988409a28819192944488c22950ca104720487701221104206841b
498589064ad33608dbc04058b6510ca7098c24619990648cc2905b249010a349
03256143328a119844c8b22004384110472c19c6441c252c048830d946699b20
001b46825aa4805ba0491890250026800bc2315a407254c620c1b03124b14d10
952814000aa0c84d54a28823988160900402162c13214091868d08c291911426
d0b40c09c66051442e04112600291193c20863a431220028c114080c402c4114
069c20725422068b084da148691030411c284944188ecc9648d942501b06490c
458823040d20302e23852c14073040b6854cc02044862019006c540248cc886c
59063249148404c750134928e40609d3c610c8284c23394452a464cca8494438
320a898400342c22858d1031090932651c898c40402921850009a16d84c064e2
022d48044012098ee0422e93440812106a01840592308acb348ea2262e5c8611
0b3508181000023426242389d1840024466013b249242846180271a038908914
44d3962da31840232721c0185043c80441428d5c264144a26d48120e4032250b
14820a482ecb828803a3601b25268c802024b08598042108a72c833864543289
010401234984029569d1a44d13a40c91460d6194809038455cc65001172053c6
289b1810411268901221c01084421692538229812649d8a4059a2624240329e0
4026d20248112468119989981485c9200d50128c1c0810021000009528c12890
59b485d314650a406e11296518c24c213465d830691030521931668c188ac8c0
084c9830a3a62041162218052e22252a64b8250ab30163208409800919280e02
1101a39411e3986c58202109411060362208067112c2855aa085c0c6845c3806
cbb669148484532282a1a640cc8600c42622a0a808983472d4204143c4904816
681b16521a370250204248488a201141e2006cc0c20c14064911314d19060a89
46091b816544c800820670001672cc24508a42899c969064287092b268982662
619440c11689d842641a214e62906421c8248b286d5c4292a0c64d0c8580cc88
4dd4428d24348a0b0451c32686242581123506a04404c894815bb4311c08065c
240803276a20c225e1809019b46da3460c4b186050c62c1b922d111504a20004
21482ed81606d2108a83a22508310d093851d948490b164c2332251919024a44
09d1b2210b832c23258593168544a0441b83500222724b04809b146521936018
130ad9460d224561c8b440a1422d02b8090014449bb6110b978c40104a82146a
da90051c028e0c1972a3b48d24305011870964c628e4189298b46c6116514046
0e1c3248da205188368a23b1218290281a1532e2186192048e13b690131368c9
84684c406d0b330081464dd2380c049681a4885002908522b004d3a471d28010
```

ca964051a641a48428e008520b308cd2380a0c2951c38209ca2091d83692a3a6  
28924222a216011a348637d9a659169881ec21cf4811869d1d7f139f0537e96f  
1184585405fd17808af1e06239d3b34e5aca8bf1369677b447ac718ac47d850c  
4d77b0be31dc9f508e3978f24274ab0185f727abdf59f4490371bf04610e364  
e64ec875ef9d20dc94077e1e166327a879b8ab516160b2a3f77437b9b3cc7d17  
aeaddc84db62746a35ac096f782f62a7f01aa6d6693deec90b23c66985a02307  
e0a1cae598a67324dba0f52f22432275e93257065c3b7e5e1cfeldfd4d0df086  
df21243414a2d27e20230a829be4eb4c82c16d35f78b0e5e198332e00074bb64  
612fab17d4c8971cb68e5edab0369f1157b3469abd8384e2d9553f1b78e786e1  
ee9d0b98d39f83ccecf37d1ebd3a9d63aec766164a10171a4fd8c63daf182c42  
1258c5f529aa55cb7ebae2e1652315e1f71e8a74131410d03247ede11d34db91  
f6f08aa2478fd789679c04949f71bc0171e07e3a8bb5753dbbdaa411a6350ab4  
6eefbf86fc551c29efe4cdd7661d5cf6c3db22d0cedde599854459d97f20df74  
55bdf356a198d0f7eb6d34111fc940b25c0543b788edda9d26810eac3d6cc9c5  
1327c2cf83e887d4089e19695e11add837f6f440cc360f93f32fee8a9663712c  
6bbd38c84ab7b54823ec363eb7e42eb59fc1fce60fbd55307b3ec85fd9daf320  
6d7b4b3917f1c8b7a92e3c67d89880fdf2e47f5a0c994595db170af41babf5a2  
5b4dc1c42dd6a9db271e764de2fb015a49a850c7919be47006a336e2e325fde5  
3ac599554d0a7de4ef45ec40c39d6baff311beee75d89e02ad31f4be4bd20ae9  
194f5edddaa6650776116e9f270f77714ad7a8e89acef74b7ff7d8dbec27f802  
0a985247e2cdacef4894a4d68ba37ca912d6be73501c995181e5b77723350b36  
31da3700e13fd366e131bf06b36eb6b0345093209f0a7beffae1fdd875b00687  
c1163c353d7d2ac90937b34e978e92f821adc9662202ece89a17e7bb65ae17d8  
3b90dbbe6a501a4e1345bee4e5a5b53af2e5ba3d1ef3f4e05adf0b3a4cf2e530  
360fee64929902b571f6fd2e305652a4cb010f79f815e18f2bbb8cc89fa6fc76  
f77c89e293cf175a0b195800fe72d2ccdd7d75e5bd90bc6ac435d6a440ef852e  
9alc8c53de03bf193365d735aaf29c5162a617e364e7f944168d0fb48fef4055  
8f454297cc3dd508662cf23fb88e1954aa45d1c5e115bcc36f05b3e098d55522  
0f40be2629b34507b8464c54c27b5dec78da8f22650514797af86a2512bcb7e2  
923379ef6d73c137006c1b38f51e37f93585e29041a3e4e3af46007ce13b8b5f  
7b17d5d65d7d5668e427bcbe7ec1d7c408c054a48clae797bf99acbc8d260752  
2935fd665ea7822d930f23eabff783bb23697569e204b943141e00c08810956b  
e0525365dbab54ed48cb76964ccdf5cbdb3aee7282d4a0000d2784d7b8fab16b2  
f7f0d5225732b1efbc4eb1cfedeb43fde79b69ecc0fbaea1e6b40728673bd4b2  
e98a0d4a8f02f853950730f28d35eb12fcc79768b8e18e4bda0e58a331a2f71d  
7ccc2d451b32b1c65c312acf47ee513b21954c41c00c873872ee94cf14f46037  
425361f4b5b54821f711460cebae8c07508a9219f88fa6bedaa678eed501944a  
16ae6f7b5bb7a2e1e357e70d7b98461a2c71cb0fa762d6ad9824081d37f292fd  
4be8b84c36110dc744360201beebe0bd6c9d05e869256d2ff3f99517b7efd2a3  
3774056cb5671675a8b492e9f5f2620eb8ef9381d3d1df19938b7b5ffaac59bc  
8110fa87ba8d7a3d0165f8e41dd0f804f11b9ded0f352a597835d06307a8e0c6  
ef4d21904339e1cf458923a3e89e025d945347366c02f3dd6368d4e47e85d3d2  
a9705bd57961852e5a579f93b1c514c539f49ea1163a2a493b0efcb47f4748f6  
a99e10bf7078282e4ace18136e2a8b3ee0a380dcd3b3ef3e65e1b8157289d624  
67ad488ba0392b2e90alededcbdc931dc17298ccecf76645c7d330a05c2ce40f8  
9b85468f357a217751e154631304ec4e04bb45b3678909c74af51ce370364d8f  
4f7eb1e61e00d87429c9961de8322ca9a2629b1309d800e92bcldc5055dccc797  
f33866eb0cf028d40250d48ffca8022f49290e2d5376162fbaa982d16453c825  
b35f6515635ea92bea72367baa54de3f9eaea69542a81a4127f71cbaa257f324  
fefef14f08fbd65a049cd2fb362594a8e23ff1a2617db5b158f6f01cf50ab0ed  
95c6e709841164108b06e1b40ab0ab11c408301d3d9d8ea69e968a9600b3d17f  
38011ce28074e2c2e10bf6197c602d8d0ce7d3a3ef2d89623bc9f12ea338791e  
9266bb8ce02b124c6c7929baea693244098454a080eb7523e13bb1b7c5b6775f  
abababbe9075fe5687aa451397bb9cfcccd051243e9bf5aef24062d335de5fce2  
4e9dddbde1191052d80c36df9f8434872f277ed4f5a1ce8ebd3b960824a4e4f10  
01b04cb685f9bee4d0ddb0c571598ac2021a6606fd23345c6fbb84f0ce05fe52  
734521b7b07c6388d3a3b99318bf0131504aa9dfbaf548f9d32a9cd4c6893524  
b11330a2d3aad3ed2a58966ebb0134465d543fd7797af549f568eaebe957f64f  
ec854674902b97558756986946ea3ab7a251cbbbea11a687bd43f5d0bd89cd2ca  
ba61d5218374990ee8b92219ed25dca011c68a9757c013bd837b2dd734e3751f  
64fcb4b23dcd6bc57ea567f5716e17367244751e2303b22a953e772756956cdc  
c013ffd2c32490754422a572529d4c92f1ebbb19f1dad4d036f2fdf31ca9101bd  
f81aea948aedcf217aa8fccd7a0771aa2753e1a823bf41c95377a2ffa61b2265  
138153ce86d2c87dd07a4b32d27f5f2872641431ce9a18a502aaefd9afc5b0d1  
3cd46c357e38e69elee945add1992932a5b1e5c5629c9f48f7661853da00787c  
9d78fb925553bf07a50dd5b9d935853420e4d1a71ae62ff90ca193cdd6c2f4be

```
d263415aaf9a35094bc2a22e2a663c7645001cd190b7bc17c75feadf8e87ce5c
24b763b6584ed32e71b0268142ea3ed6898157bf923bebf0192d1bf5ee30a7d3
51634a60b504dde38a2e114f7ae9bf176d4a18ba2895a7bb4b47444a9ba8dbb4
c124cd41bbb32f4bcb1de48c4abb510607a001b5a000bba43618b6c19e43517b
45b42405928b67c713881858bad3a42511c2716ff9cd332034b672b52ff16610
805cdbe7544a8a84b66e1c745a73c1b6bcd5b77b951f36c0f7a5372de9e5d1f
9bbcd8843c6909002dda4875e67571af0bec581856c32c09c240e664e761e57
cd0d8dc8a71cb918a5762d111285cd8b5613ddb0ca08ac0342b2bdee38f96fa
754bb2b087179c113c93986a810356eb94540b93cb9dec4aa9290ff12ec1aa2e
656c9be3d590753c366c601406c061bc22033a1fd1f4e1111d039b8813b983cb
506c3ea7ff3057983e8bf01682fbb00f43005313c82c1392918a6165a13338ff
e11a992c1fb3d1032aa679a418c8ba4f8a0bc199e10cf6bd77a14fdd6a060935
14348e3a8974434ae8a3676369c6be2cf90e672b343f3ce04ac6b22e0cf47568b
c45d70a68e68c649a4830ae218590c1a437e7a23a54efe44f67086eb697b9fa5
7835f0b8f70f0a929226efb336c0e21833a028218cd63732c80aa477e62d141d
ba81854f70da68daff4a84cb6de779254e8a97e73565374af4092af05cbd6654
afc3fd72f0ae232695cb6668eafecc4069bd90bb528b83efa2fbcd93b28992
9621ed74d808738fc103eeb105510851fc9319f171ea0ced0b97b5b9fb5ef985
186bc52098f9eb476f67b7cc7665d47587975cb45a50fc64100719bf76345f0f
df1e09efe9fb800dc114e46be0879a195cc06870e23d2631dae71c3994481c87
61c40d07c5bfca95e718b7b22585af03ed34175a46d57af3518e32a7fc1aa448
2732a81a87f724f8d2e780b3a39d451a380f75c2d680cc7213eab1d4a59d394a
e3810alc90818d52f93fb203e2d8b1b5fa8f60b2d585d9135d648846f138b869
53242d2bb1f2ecdf389b4de7651817b8e4e64b333flaac523a93f2748a9c38ff
bc29ced457b6f9781b08a67a1975d031ccd71545c0037434056c2434d13e6c4b
eebf46fc1222c0b2eccd6159d5aea8e554d7a09652b06bf7ca699a7199e716d
05dd553041a8f2b303d236a9babaafbf9fa528f28a2ca2aa780b940383c099aa6
5a0074b83fd1f0bc5b7b5e46c25e54838b3cbcf95f87f1d471b3ba894434fa5
8952fdcb77f161372693306dba4e8f216d1c8e5caff0fe8360a51c6076364416
9fdc6a8267f2e3f909a61b2a678bce6ae90403a836b1a7b7e8cd8b54c37087a9
e14446d95e6908d2eedbfcc653e02fdf771f701a79b9e5a26ed0a947842070f3
b5701742211219e761762c37f0d0a1d1b9750fee577e1208115c66ac07ec091e
6a3fc4aa6a253bcba868edd3154dcdf5162f615e85490a6ca342f34c43ac61a3
ea6bfeefd850e190eb1d8da4d28b5ecee1678c02433ecd5d48b2536404257e8
ca7bef5855f2b813ed2f4c409445a3317c9bel1a35ae2fb4d2b87921b904bf2c1
4db514cee045251cfc276374db15c99dea15acde197c6eb524988e39b63287be
b8676865aaa3bad1b43b8cab15cbf27a498759e3203abf369e97242f0b015414
9f14ac233cdb73a22b7fb8f09325bf2ace83bb6b5db8a121a2b682149a69131c
cce52229840b113fc7b0bcc58405bfe87f1f95ffc2e96fc5596567e94364dfaa
6d9d5a6eb99ae4ddf424' }
}
}
```

#### C.1.3.3. Both Format

```
-----BEGIN PRIVATE KEY-----
MIITXgIBADALBgIghkgBZQMEAxMEghNKMIIITRgQgAAECAwQFBgcICQoLDA0ODxAR
EhMUFRYXGBkaGxwdHh8EghMgl5K87C8kMGHqgvzPPC9f9mXncderQbkCWM+n6Q7J
cSTY6e5OkKFYSYC9eybw4UX3DDjKdWrJ2c72F9MmwMA93Y4mIZ1ClfCTbP8AS5h7e
WXUzNzdPpxJJKVsa8kNJBQY3yzvgWllII1v3mHX4ltj+DKswyElI201jFaqvFgrG
JDZkIgFIFhEJESyUAokiRSxiuEUARSoIlncQEm4Uk3DURhCERFFYlpEMqSmCskHJ
CHHEKGgElolIQIwBIm0cKGRZEKGuJGEBIEkAXLNGKghpBAJpIgmSkTBWlcNGik
Mo4ZJpJZRhAJpEkjQk0SNmFYEGUBKJAaM0yZhjHTokkKgIvDFCjAOIEDFU1bKIYI
h0gjMVKUiiXDWe2kmCGYQCDRQobLQHbbsHGclizBEgZTRgkMRQIURm6RtCFUsIzk
RkKaIIwBISUTQQVaQCITyQygGEBSWjDLNCxLyGgbpGBJhIRjMClKoGlbGATSOAoU
JkziskSLOhEkRknEFFILQnEDshCSKIABJIjCBEBKSgZxIEAICLcRGHCEiJEACrJ
JmoMhzHgwESZFIQYNg0RN0IiGIXjSpEMMaIhoAEIkkQEEyRcmHGCHGEMlJRSdGc
Qi4aqCgCCJEBWIkLxwWKGJGuiwRMiJfCgmgTpWRQIIYhBAKRlERIIjAiOUoCmIQJ
oogZGS1ESIwilQyhBHIEh3ASIRBCBoQbSYWJBkrTNgjbwEBytLEmpwmMJGGZkGSM
wpBbJJAQo0kDJWFDMMoRmETIisIAEOEEQRYwZxkQcJSWEiDDZRmmBIAAbRoJapIBb
oEkYkCUAJoALWjFaQHJUXiDBsDEksU0QlSgUAAqgyElUoogjmIFgkAQCFiwTIUCR
ho0IwpGRFCbQtAwJxmBRRc4EESYAKRGTwghjpDEiACjBFAgMQCxBFAacIHJUIgaL
CE2hSGkQMEECkELEGI7MlkjZQlAbBkkmRYgjBA0gMC4jhSwUBzBAtVMwCBEhiAZ
AGxUakjMiGxZBjJFFIQEXlATSSjkBgnTxdIKewjOURSpGTMqELEODIKiYQANCwi
hY0QMqKJMMUciYxAcQckhQAJoW2EWGTiAi1IBEASCY7gQi6TRAgSEGoBhAWSMIRL
NI6iJi5chhELNQgYEAACNCYki4nRhAAkRmATskkkKEYYAnGgOJCJFETtli2jGEAj
```

JyHAGFBDyARBQo1cJkFEom1IEg5AMiULFIKSC7LgogDo2AbJSaMuCAksIWYBCEI  
pyyDOGRUMokBBAEjSYQCLWnRpE0TpAyRRg1hlICQOEvcxLABFyBTxiibGBBBEmiQ  
EiHAEIRCFpJTgimBJknYpAWaJiQkAyngQCBSakgRJGgRmYmYFIxJIA1QEowcCBAC  
EAAALsJBKJBZtIXTFGUKQG4RKWUYwkwhNGXYMGkQMFIZMwAMGIRIwAhMmDCjpiBB  
FiIYBS4iJSpkuCUKswfJIIQJgAkZKA4CEQGjLBHjmGxYICEJQRBgNiIIBnESwoVa  
oIXAxoRcOABltmkUhIRTIOKhpkDMhgDEJiKggAiYNHLUIEFdXJBIFmgfFlIaNwJQ  
IEJISIOgEUHiAGzAwgUBkkRMU0ZBgqJRgkbgWVEyACCBnAAFnLMJFCKQomclpBk  
KHCSsmiYJmJhLEDBFonYQmQaIU5ikGQhyCSLKG1cQpKgXk0MhYDMiE3UQo1CNIoL  
BFHDJoYkJYESNQagRATILfBtDEcCAZcJAgDJ2ogwiXhgJAZtG2jRgxLGGBQxiwb  
ki0RFQSiAAQhSC7YFgbSEIqDoiUIMQ0JOFHZSEkLFkwjMiUZGQJKRANrsiELgywj  
JYWTFoVEoEQbg1ACInJLBICbFGUhk2AYEwrZRg0iRWHiTEChQioCuAkAFESbthEL  
l4xAEEqCGFrakAUcAo4MGXKjtI0kMFARhwlkxiJkGJKYtGxhFlFARg4cMkjaIFGI  
NoosSGCKCgaFTLiGGGSBI4TtpATE2jJhGhMQG0LMwCBRk3SOAwElOGkiFACKiFui  
sATTpHHSgBDKlkBRpkGkhCjgCFILMIzSOAoMKVHDggNKiJHYNpKjpiiSQiKiFgEa  
NIY32aZZFpiB7CHPSBGGnR1/E58FN+lvEYRYVAX9F4CK8eBiOdOzTlrKi/E2lne0  
R6xxisR9hQxNd7C+MdyfUI45ePJCDksBhfcNq9/1n0SQNxxvRhDjZozOyHXvnSDc  
lAd+HhZjJ6h5uKtRYWCyo/d0N7mzzH0Xrq3chNtidGolrAlveC9ip/AaptZpPe7J  
CyPGaYWgIwfgocrlmKZzJNug9S8iQyJ16TJXBW7f14c/h39TQ3wht8hJDQUotJ+  
ICMKgpkv60yCwW0194sOXhMDmuAAdLtkYS+rF9Tilxy2j17asDafEVEzRpq9g4Ti  
2VU/G3jnhuHunQuY05+DzOzzfR69Op1jrSDmFkoQFxpP2MY9rxgsQhJYxfUpqlXL  
frri4WUjFeH3Hop0ExQQ0DJH7eEdNNuR9vCKokeP14lnnASUN3G8AXHgFjQltXU9  
u9qkEaY1CrRu77+G/FUCke/kzddmHVz2w9si0M7d5ZmFRFnZfyDfdFW981ahmND3  
6200ER/JQLJcBUO3iO3anSaBDqW9bMnFEyfcZ4Poh9QInhlpXhGt2Df29EDMNg+T  
8y/uiPzjcSxrvTjISrelSCPsNj635C61n8H85g+9VTB7Pshf2drzIG17SzkX8ci3  
qS48Z9iYgP3y5H9aDj1FlDsXCvQbq/WiW03BxC3WqdsnHnZN4vsBWkmoUMeRm+Rw  
BqM24uM1/eU6xZ1VTQp9509F7EDDnWuv8xG+7nXYngKtMfS+S9IK6R1Pxt3apmUH  
dhFunycPd3FK16joms73S3/32NvsJ/gCCphSR+LNr09IlKTwi6N8qRLWvnNQHJ1R  
geW3dyM1CzYx2jca4T/TZuExvwazbrawNFCTIJ8Ke+/64f3YdbAGh8EWPDU9fSrJ  
CTezTpeOkvghrcImIgLS6JoX57t1rhfyO5DbvmpQGk4TRb7k5aW1OvLluj0e8/Tg  
Wt8Lokzy5TA2D+5kkpkCtXH2/S4wVlKkywEPefgV4Y8ru4zIn6b8dvd8ieKTzxda  
Cx1YAP5y0szdfXX1vZC8asQ11qRA74UumhyMU94DvxkzZdc1qvKcUWKmF+Nk5/1E  
Fo0PtI/vQFWPRUKXzD3VCGYs8j+4jhlUqkXRxeEVVMNvBbPgmNVVig9AviYps0UH  
uEZMVMJ7Xex42o8iZQUUEXr4aiUSvLfikjN5721zwTcAbBs49R43+TWF4pBB0+Tj  
r0YAfoE7i197F9XWXX1WaoQnvL5+wdfecMBUpIwa55e/may8jSYHUiK1/WZep4It  
kw8j6r/3g7sjaXVp4gS5QxQeAMCIEJvr4FJTZdurVO1Iy3aWTM31y9Ou5ygtSgAA  
0nhNe4+rFrL38NUiVzKX77xOsc/t60P955tp7MD76qHmtAcoZzvUsumKDUqPAvhT  
lQcw8016xL8x5douOGOS9oOWKMxovcdfMwtRRsyscZcMSrPR+5ROyGVTEHADiC4  
cu6UzxT0YDDCU2H0vbVIIffcRRgzrrowHUIqSGfiPpr7apnJulQGUShaub3tbt6Lh  
41fnDXuYRhosccsPp2LWrZgkCB038pL9S+i4TDYRDcdENgIBvuvgvWydBehpJW0v  
8/mVF7fv0qM3dAVstWcWdai0kun18mIOuO+TgdPR3xmTi3tf+qxZvIEQ+oe6jXo9  
AWX45B3Q+ATxG53tdZuqWXg10GMHqODG700hkEM54c9FiSOj6J4CXZRTRzZsAvPd  
Y2jU5H6F09KpcFvVeWGFLlpXn5OxxRTFOfSeoRY6Kkk7Dvy0f0dI9qmeEL9weCgu  
Ss4YE24qiz7go4Dc07PvPmXhuBvyidYkZ61Ii6A5Ky6Qoe3ty9yTHcFymMzvdmRc  
fTMKBcLOQPibhuAPNXohd1HhVGMTB0xOBLtFs2eJCcdK9RzjcDZNj09+seYeAch0  
KcmWHegyLKmiYpsTCdgA6SvB3FBV3MeX8zhm6wz9jUkCUNSP/KgCL0kpDi1TdhYv  
uqmC0WRTyCWzX2UVY16pK+pyNnuqVN4/nq6mlUKoGkEn9xy6olfzJP7+8U8I+9Za  
BJzS+zYllKjiP/GiYX21sVj28Bz1CrDtlcbnCYQRZBCLBuG0CrCrEcQIMB09nY6m  
npaKlgCz0X84ARzigtIwUEL9hl8YC2NDOfTo+8tiWI7yfeUozh5HpJmu4zgKxJM  
bHkpuuppMkQJhFsggOtlI+E7sbFftndfQ6urvpB1/laHqkUTL7uc/M0FEkPpvlrv  
JAYtM13l/OJondveEZEFLYDDbfn4Q0hy8nftTloc6OvTuWCCSk5PEAGwTLaf+b7k  
0N2wxXFZisICGmYG/SM0XG+7hPDOBf5Sc0Uht7B8Y4jTo7mTGL8BMVBKqd+69Uj5  
0yqc1MaJNSSxEzCi06rT7SpYlm67ATRGXVQ/13169UnlaOrr6Vf2T+yFRnSQK5dV  
hlaYaUbqOreiUcu+oRpoe9Q/XQvYnNLKumHVIYN0mQ7ouSiZ7SXcoBHGipdXwBO9  
g3st1zTjdr9k/LSyPclrxX61Z/Vxbhc2ckR1HiMdsiqVPncnVpVs3MAT/9LDJJB1  
RCKlclKdTLx67GfHa1NA28v3zHKkQG9+BrqlIrtzyF6qPzNegdxqidT4agjv0HJ  
U3ei/6YbImUTgVPOhtLifdB6SzLSf18ocmQUMc6aGKUCqu/Zr8Ww0TzUbDV+00ae  
HulFrdGZKTKlseXFYpyfSPdmGFPAAh8nXj7klVTvwelDdW52TWFNCDk0aca5i/5  
DKGTzdbc9L7SY0Far5o1CUvCoi4qZjx2RQAc0ZC3vBfHX+rfjofOXCS3Y7ZYTtMu  
cbAmgULqPtaJgVe/kjvr8BktG/XuMKfITUWNKYLUe3eOKLhFPeum/F21KGLoolae7  
S0deSPuo27TBJM1Bu7MvS8sd5IxKulEGB6ABtaAu6Q2GLbBnkNRE0W0JAWSi2fH  
E4gYWLrTpCURwnFv+c0zIDS2crUv8WYQgFzb51RKioS2bhx0WnPbtrzaW3e5UfNs  
D3pTct6eXR+bvN6IQ8aQkALdpIdeZ1ca8L7FgYVsMsCcJA5mTnYeV80NjcinHLkY  
pXYtERKFzYtWE929DKCKwDQRK97jj5b6dUuysIcXnBE8k5hqqQNW65RUC5PLnexK  
qSkp8S7Bqi51bJvj1ZB1PDZsYBQGwGG8IgM6H9H04REdA5uIE7mDy1BsPqf/MFeY  
PovwFoL7sa9DAFMTyCwTkpgKYWWhMzj/4RqZLB+z0QMqpnmkGmi6T4oLwZnhDPa9  
d6FP3WoGCTUUNI46iXRDSuijZ2Npxr4s+Q5nKzQ/zgSsayLgz0dWi8RdcKaOamZJ

pIMK4hhZDBpDfnojpU7+RPZwhutpe5+leDXwuPcPCpKSJu+zNsDiGDogKCGM1jcy  
yAqkd+YtFB26gYVPcNpo2v9KhMtt53klToqX5zVlN0r0CSrwXLlmVK/D/XLwriMm  
lctmaOr+zEBpvZC7UouD76L7zb2TsomSliHtdNgIc4/BA+6xBVEIUfyTGfFx6gzt  
C5elufte+YUYa8UgmPnrR29nt8x2ZdR1h5dctFpQ/GQQBxm/djRfD98eCe/p+4AN  
wRTka+CHmhlcwGhw4j0mMdrnHDmUSByHYcQNB8W/ypXnGLeyJYWvA+00F1pG1Xrz  
UY4yp/wapEgnMggah/ck+NLngLOjnUUaOA91wtaAzHIT6rHUpZ05SuOBChyQgY1S  
+T+yA+LYsbX6j2CylYXZE11kiEbxOLhpUyQtK7Hy7N84m03nZRgXuOTmSzM/GqxS  
OpPydIqcOP+8Kc7UV7b5eBsIpnoZddAxzNcVRcADdDQFbCQ00T5sS+6/RvwSiwL  
LszWFZla6o5VTXoJZSSGv3ymmacZnnFtBd1VMEGo8rMD0japurqvufpSjyiyiqn  
gLlAODwJmqZaAHS4P9HwvFt7XkbCXlSDizy8/JX4fxlHGzuolENPpY1S/ct38WE3  
JpMwbbpOjyFtHI5cr/D+g2ClHGB2NkQWn9xqgmfy4/kJphsqZ4vOaukEA6g2sae3  
6M2LVMNwh6nhREBZXmkIOu7b/MZT4C/fdx9wGnm55aJu0KlHhCBw87VwF0IhEhnn  
YXYsN/DQodG5dQ/uV34SCBfcZqwh7Akeaj/EqmolO8uoaO3TFU3K9RYvYV6FSQps  
o0LzTEOsYaPqa/7v2FDhkOsdjaTSi17O6xZ4wCQz7NXUiYU2QEJX6Mp771hV8rgT  
7S9MQJRfFozF8m+GjWuL7TSuHkhuQS/LBTbUUzuBFJRz8J2N02xXJneoVrN4ZfG61  
JJiOObYyh764Z2hlqqO60bQ7jKsVy/J6SYdZ4yA6vzaelyQvCwFUFJ8UrcM823Oi  
K3+48JmlvyroG7trXbihIaK2ghSaarmczOUiKYQLET/HsLzFhAW/6H8flf/C6W/F  
WWVn6UNk36ptnVpuuZrk3fQk  
-----END PRIVATE KEY-----

```
SEQUENCE {
  INTEGER { 0 }
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
  }
  OCTET_STRING {
    SEQUENCE {
      OCTET_STRING { '000102030405060708090a0b0c0d0e0f1011121314
15161718191a1b1c1d1e1f' }
      OCTET_STRING { '9792bcec2f2430686a82fccf3c2f5fff665e771d7ab
41b90258cfa7e90ec97124d8e9ee4e90a16c602f5ec9bc38517dc30e329d5ab2
7673bd85f4c9b0300f776389886750b57c24db3fc012e61ede59753337374fa7
124991549af243496d0637cb3be05a5948235bf79875f896d8fe0cab30c84948
db4d6315aaaf160ac6243664220148161109112c94028922452c62b84500452a
08967090126e149370d44610844515896910ca92982b241c90871c428680496
894840859b226d1c28645912419cb891840489449005cb3462a0869040269220
99291305695c3468a4328e19269259461009a44923424d123661581065012890
1a334c998631d3a249098225431428c0388103154d5b28860887482331529422
25c3c04da49821984020d14286cb40705bb0719c962cc112065346090c450214
466e91b42154b08ce446429a208c0121251341055a402213c90ca0184052c230
cb342c4bc8681ba4604984846330294aa0695b8004d2380a14264ce2b2448ba2
11244649c414520b427103b210922880012488e308110a052819c481002022dc
446842122244002ac9266a0c8731e0c04499148418360d11374222188c63b291
0c9808a1a0010892440413245c987182847184325251b0319c422e1aa8280208
9101c0890bc7058a246522c2644c88915c826813a56450208621040291944448
223022394a02988409a28819192944488c22950ca10472048770122110420684
1b498589064ad33608dbc04058b6510ca7098c24619990648cc2905b249010a3
4903256143328a119844c8b22004384110472c19c6441c252c048830d946699b
20001b46825aa4805ba0491890250026800bc2315a407254c620c1b03124b14d
10952814000aa0c84d54a28823988160900402162c13214091868d08c2919114
26d0b40c09c66051442e04112600291193c20863a431220028c114080c402c41
14069c20725422068b084da148691030411c284944188ecc9648d942501b0649
0c458823040d20302e23852c14073040b6854cc02044862019006c540248cc88
6c59063249148404c750134928e40609d3c610c8284c23394452a464cca84944
38320a898400342c22858d1031090932651c898c40402921850009a16d84c064
e2022d48044012098ee0422e93440812106a01840592308acb348ea2262e5c86
110b3508181000023426242389d1840024466013b249242846180271a0389089
1444d3962da31840232721c0185043c80441428d5c264144a26d48120e403225
0b14820a482ecb828803a3601b25268cb82024b08598042108a72c8338645432
89010401234984029569d1a44d13a40c91460d6194809038455cc65001172053
c6289b1810411268901221c01084421692538229812649d8a4059a2624240329
e04026d20248112468119989981485c9200d50128c1c0810021000009528c128
9059b485d314650a406e11296518c24c213465d830691030521931668c188ac8
c0084c9830a3a62041162218052e22252a64b8250ab30163208409800919280e
021101a39411e3986c58202109411060362208067112c2855aa085c0c6845c38
06cbb669148484532282a1a640cc8600c42622a0a808983472d4204143c49048
```

16681b16521a370250204248488a201141e2006cc0c20c14064911314d19060a  
8946091b816544c800820670001672cc24508a42899c969064287092b2689826  
62619440c11689d842641a214e62906421c8248b286d5c4292a0c64d0c8580cc  
884dd4428d42348a0b0451c32686242581123506a04404c894815bb4311c0806  
5c240803276a20c225e1809019b46da3460c4b186050c62c1b922d111504a200  
0421482ed81606d2108a83a22508310d093851d948490b164c2332251919024a  
4409d1b2210b832c23258593168544a0441b83500222724b04809b1465219360  
18130ad9460d224561c8b440a1422d02b8090014449bb6110b978c40104a8214  
6ada90051c028e0c1972a3b48d24305011870964c628e4189298b46c61165140  
460e1c3248da205188368a23b1218290281a1532e2186192048e13b690131368  
c984684c406d0b330081464dd2380c049681a4885002908522b004d3a471d280  
10ca964051a641a48428e008520b308cd2380a0c2951c38209ca2091d83692a3  
a628924222a216011a348637d9a659169881ec21cf4811869d1d7f139f0537e9  
6f1184585405fd17808af1e06239d3b34e5aca8bf1369677b447ac718ac47d85  
0c4d77b0be31dc9f508e3978f24274ab0185f727abddf59f4490371bf04610e3  
64e64ec875ef9d20dc94077e1e166327a879b8ab516160b2a3f77437b9b3cc7d  
17aeaddc84db62746a35ac096f782f62a7f01aa6d6693deec90b23c66985a023  
07e0a1cae598a67324dba0f52f22432275e93257065c3b7e5e1cfe1dfd4d0df0  
86df21243414a2d27e20230a829be4eb4c82c16d35f78b0e5e198332e00074bb  
64612fab17d4c8971cb68e5edab0369f1157b3469abd8384e2d9553f1b78e786  
e1ee9d0b98d39f83ccecf37d1ebd3a9d63aec766164a10171a4fd8c63daf182c  
421258c5f529aa55cb7ebae2e1652315e1f71e8a74131410d03247ede11d34db  
91f6f08aa2478fd789679c04949f71bc0171e07e3a8bb5753dbbdaa411a6350a  
b46eefbf86fc551c29efe4cdd7661d5cf6c3db22d0cedde599854459d97f20df  
7455bdf356a198d0f7eb6d34111fc940b25c0543b788edda9d26810eac3d6cc9  
c51327c2cf83e887d4089e19695e11add837f6f440cc360f93f32fee8a966371  
2c6bbd38c84ab7b54823ec363eb7e42eb59fc1fce60fbd55307b3ec85fd9daf3  
206d7b4b3917f1c8b7a92e3c67d89880fdf2e47f5a0c994595db170af41babf5  
a25b4dc1c42dd6a9db271e764de2fb015a49a850c7919be47006a336e2e325fd  
e53ac599554d0a7de4ef45ec40c39d6baff311beee75d89e02ad31f4be4bd20a  
e9194f5edddaa6650776116e9f270f77714ad7a8e89acef74b7ff7d8dbec27f8  
020a985247e2cdacef4894a4d68ba37ca912d6be73501c995181e5b77723350b  
3631da3700e13fd366e131bf06b36eb6b0345093209f0a7beffae1fdd875b006  
87c1163c353d7d2ac90937b34e978e92f821adc9662202ece89a17e7bb65ae17  
d83b90dbbe6a501a4e1345bee4e5a5b53af2e5ba3d1ef3f4e05adf0b3a4cf2e5  
30360f7ee64929902b571f6fd2e305652a4cb010f79f815e18f2bbb8cc89fa6fc  
76f7fc89e293cf175a0b195800fe72d2ccdd7d75e5bd90bc6ac435d6a440ef85  
2e9a1c8c53de03bf193365d735aaf29c5162a617e364e7f944168d0fb48fef40  
558f454297cc3dd508662cf23fb88e1954aa45d1c5e115bcc36f05b3e098d555  
220f40be2629b34507b8464c54c27b5dec78da8f22650514797af86a2512bcb7  
e2923379ef6d73c137006c1b38f51e37f93585e29041a3e4e3af46007ce13b8b  
5f7b17d5d65d7d5668e427bcbe7ec1d7c408c054a48clae797bf99acbc8d2607  
522935fd665ea7822d930f23eabff783bb23697569e204b943141e00c0881095  
6be0525365dbab54ed48cb76964ccdf5cbd3aee7282d4a0000d2784d7b8fab16  
b2f7f0d5225732b1efbc4eb1cfedeb43fde79b69ecc0fbeaa1e6b40728673bd4  
b2e98a0d4a8f02f853950730f28d35eb12fcc79768b8e18e4bda0e58a331a2f7  
1d7ccc2d451b32b1c65c312acf47ee513b21954c41c00c873872ee94cf14f460  
37425361f4b5b54821f711460cebae8c07508a9219f88fa6bedaa678eed50194  
4a16ae6f7b5bb7a2e1e357e70d7b98461a2c71cb0fa762d6ad9824081d37f292  
fd4be8b84c36110dc744360201beebe0bd6c9d05e869256d2ff3f99517b7efd2  
a33774056cb5671675a8b492e9f5f2620eb8ef9381d3d1df19938b7b5ffaac59  
bc8110fa87ba8d7a3d0165f8e41dd0f804f11b9ded0f352a597835d06307a8e0  
c6ef4d21904339e1cf458923a3e89e025d945347366c02f3dd6368d4e47e85d3  
d2a9705bd57961852e5a579f93b1c514c539f49ea1163a2a493b0efcb47f4748  
f6a99e10bf7078282e4ace18136e2a8b3ee0a380dcd3b3ef3e65e1b8157289d6  
2467ad488ba0392b2e90alededcbdc931dc17298ccecf76645c7d330a05c2ce40  
f89b85468f357a217751e154631304ec4e04bb45b3678909c74af51ce370364d  
8f4f7eb1e61e00287429c9961de8322ca9a2629b1309d800e92bcldc5055dcc7  
97f33866eb0cfd8d490250d48ffca8022f49290e2d5376162fbaa982d16453c8  
25b35f6515635ea92bea72367baa54de3f9eaea69542a81a4127f71cbaa257f3  
24fefef14f08fbd65a049cd2fb362594a8e23ffa2617db5b158f6f01cf50ab0  
ed95c6e709841164108b06e1b40ab0ab11c408301d3d9d8ea69e968a9600b3d1  
7f38011ce28074e2c2e10bf6197c602d8d0ce7d3a3ef2d89623bc9f12ea33879  
1e9266bb8ce02b124c6c7929baea693244098454a080eb7523e13bb1b7c5b677  
5fabababbe9075fe5687aa451397bb9cfcccd051243e9bf5aef24062d335de5fc  
e24e9ddbde1191052d80c36df9f8434872f277ed4f5a1ce8ebd3b960824a4e4f

```

1001b04cb685f9bee4d0ddb0c571598ac2021a6606fd23345c6fbb84f0ce05fe
52734521b7b07c6388d3a3b99318bf0131504aa9dfbaf548f9d32a9cd4c68935
24b11330a2d3aad3ed2a58966ebb0134465d543fd7797af549f568eaebe957f6
4fec854674902b97558756986946ea3ab7a251cbbea11a687bd43f5d0bd89cd2
caba61d5218374990ee8b92219ed25dca011c68a9757c013bd837b2dd734e375
1f64fcb4b23dcd6bc57ea567f5716e17367244751e2303b22a953e772756956c
dcc013ffd2c32490754422a572529d4c92f1ebbb19f1dad4d036f2fdf31ca9101
bdf81aea948aedcf217aa8fccd7a0771aa2753e1a823bf41c95377a2ffa61b22
65138153ce86d2c87dd07a4b32d27f5f2872641431ce9a18a502aaefd9afc5b0
d13cd46c357e38e69e1ee945add1992932a5b1e5c5629c9f48f7661853da0078
7c9d78fb925553bf07a50dd5b9d935853420e4d1a71ae62ff90ca193cdd6c2f4
bed263415aaf9a35094bc2a22e2a663c7645001cd190b7bc17c75feadf8e87ce
5c24b763b6584ed32e71b0268142ea3ed6898157bf923bebf0192d1bf5ee30a7
d351634a60b504dde38a2e114f7ae9bf176d4a18ba2895a7bb4b47444a9ba8db
b4c124cd41bbb32f4bcb1de48c4abb510607a001b5a000bba43618b6c19e4351
7b45b42405928b67c713881858bad3a42511c2716ff9cd332034b672b52ff166
10805cdbe7544a8a84b66e1c745a73c1b6bcd5b77b951f36c0f7a5372de9e5d
1f9bbcd8e8843c6909002dda4875e67571af0bec581856c32c09c240e664e761e
57cd0d8dc8a71cb918a5762d111285cd8b5613ddbd0ca08ac0342b2bdee38f96
fa754bb2b087179c113c93986a810356eb94540b93cb9dec4aa9290ff12ec1aa
2e656c9be3d590753c366c601406c061bc22033a1fd1f4e1111d039b8813b983
cb506c3ea7ff3057983e8bf01682fbb00f43005313c82c1392918a6165a13338
ffe11a992c1fb3d1032aa679a418c8ba4f8a0bc199e10cf6bd77a14fdd6a0609
3514348e3a8974434ae8a3676369c6be2cf90e672b343fce04ac6b22e0cf4756
8bc45d70a68e68c649a4830ae218590c1a437e7a23a54efe44f67086eb697b9f
a57835f0b8f70f0a929226efb336c0e21833a028218cd63732c80aa477e62d14
1dba81854f70da68daff4a84cb6de779254e8a97e73565374af4092af05cbd66
54afc3fd72f0ae232695cb6668eafecc4069bd90bb528b83efa2fbcd93b289
929621ed74d808738fc103eeb105510851fc9319f171ea0ced0b97b5b9fb5ef9
85186bc52098f9eb476f67b7cc7665d47587975cb45a50fc64100719bf76345f
0fdf1e09efe9fb800dc114e46be0879a195cc06870e23d2631dae71c3994481c
8761c40d07c5bfca95e718b7b22585af03ed34175a46d57af3518e32a7fclaa4
482732a81a87f724f8d2e780b3a39d451a380f75c2d680cc7213eab1d4a59d39
4ae3810alc90818d52f93fb203e2d8b1b5fa8f60b2d585d9135d648846f138b8
6953242d2bb1f2ecdf389b4de7651817b8e4e64b333f1aac523a93f2748a9c38
ffbc29ced457b6f9781b08a67a1975d031ccd71545c0037434056c2434d13e6c
4beebf46fc12222c0b2eccd6159d5aea8e554d7a09652b06bf7ca699a7199e71
6d05dd553041a8f2b303d236a9babaafb9fa528f28a2ca2aa780b940383c099a
a65a0074b83fd1f0bc5b7b5e46c25e54838b3cbcf95f87f1d471b3ba894434f
a58952fdcb77f161372693306dba4e8f216d1c8e5caff0fe8360a51c60763644
169fdc6a8267f2e3f909a61b2a678bce6ae90403a836b1a7b7e8cd8b54c37087
a9e14446d95e6908d2eedbfcc653e02fdf771f701a79b9e5a26ed0a947842070
f3b5701742211219e761762c37f0d0ald1b9750fee577e1208115c66ac07ec09
1e6a3fc4aa6a253bcba868edd3154dcaf5162f615e85490a6ca342f34c43ac61
a3ea6bfeefd850e190eb1d8da4d28b5ecee1678c02433ecd5d48b2536404257
e8ca7bef5855f2b813ed2f4c409445a3317c9bel1a35ae2fb4d2b87921b904bf2
c14db514cee045251cfc276374db15c99dea15acde197c6eb524988e39b63287
beb8676865aaa3bad1b43b8cab15bcbf27a498759e3203abf369e97242f0b0154
149f14ac233cdb73a22b7fb8f09325bf2ace83bb6b5db8a121a2b682149a6913
1ccce52229840b113fc7b0bcc58405bfe87f1f95ffc2e96fc5596567e94364df
aa6d9d5a6eb99ae4ddf424` }
    }
}

```

## C.2. Example Public Keys

The following is the ML-DSA-44 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-----
MIIFMjALBgIghkgBZQMEAxEDggUhANeytHJUquDbReeTDUqY0sl9jxOX0Xidr6Fw
JLMW6b7JT8mUULxm3mnQTu6oz5xSctC7VEVaTrAQfrLmIretf4OHYYxGEMVtZLD
19IpTi4U+QqkFLo4JomaxD9MzKy8JumoMr1RGNXLQzy++WYLABOOCBf2HnYsonTD

```

atVU6yKqWRyUsrAay6Hjje79j4C2WzM9D3LlXf5xzpweu5iJ58VhBsD9c4A6Kuz+  
r97XqjyyztpU0SvYzTanjPl1lDtHq9JeiArEUuV0LtHo0agq+oblkMdYwVrk0oQN  
kryhpQkPQE111/yn2LlRPxob2m6VCqqY3kZlB9Sk9aTwWZlWWCw1cvYu2okFqzWB  
ZwxKAnd6M+DKcpX9j0/20aCjp2g9ZfX19/xg2gI+gmxfkhRMAvfRuhB1mHVT6pNn  
/NdtmQt/qZzUWv24g21D5Fn1GH3wWEeXCaAepoNZNfpwRgmQzT3BukAbqUurHd5B  
rGerMxncrKBgSNTE7vJ+4TqcF9BTj0MPLWQtwkFWYN54h32NirxyUjl4wELkKF9D  
GYRsRBjiQpdorMEOVWuiFbWnGeWdDGsqtOYWQcf3MLN51JKe+2uVOhbMY6FTo/i  
svPt+slxkSgnCq/R5QRMok/a/Z/zH5B4S46ORZYUSg2vWGUR09mWK56pWvGXtOX8  
YPKx7RXeOlvvX4m9x52RBR2bKBbnT6VFMe/cHL501EiFf0drzVjyHATlOzt2pOB2  
plWaMCcYVVzGP3SFmqurkl8COGHKjND3utsocfZ9VTJtdFETWtRfShumkrj7ssiJ  
DuyTku8/13Bmya3VxxDMZHsVFNIX2VjHAXw+kP0gWE5nS5BIbpNwoxoAHTL0c5ee  
SQZ0nn5Hf6C3RQj4pfi3gxK4PCW9OIygsP/3R4uvQrcWZ+2qyXxGsSlkPlhuWwVa  
DCEZRTTzobdb7Vhg+gQqMV2YJhZNapI3wlpfv0lUkKW9TfJIuVxKrneEtgVnMWas  
QkWltLCCoJ6TI+YvIHjFt2eDRG3v1zatOjcClJsImESQCMGDM5e8RBmzDXqXoLoH  
wZEUDMTUG1PjKpd6y28Op122W7OeWecB52lX3vbylEVZwxp3EitSB00lwhnxaIsU  
7QvAuAGz5ugtZUPpwOn0F0TNmBW9G8iCDYuxI/BPrNGxtoXdWisbjbvz7ZM2cPCV  
oYC08ZLQixC4+rvfzCskUY4y7qCl4MkEyoRHgAg/OwzS0Li2r2e8NVuU1AJdx7Cn  
j6gOOi2/61EyiFHWB4GY6Uk2Ua54fsAlH5Irow6fUd9iptcnhM890gU5MXbfoysl  
Er2Ulw023TSlFKhnkfDrNvAUWwmrZGUbSgMTsplhGiocSIkWJlHAKMRQGC6RENI  
bfUVIqHOiLMJhcIW+ObtF43VZ7MEoNTK+6iCooNC8XqaomrljbYwCD0sNY/fVmw/  
XWKkKFZ7yeqM6VyqDzVHSwv6jzOaJQq0388gg76077wQVeGP4VNw7ssmBWbYP/Br  
IRquxDyim1TM0A+IFaJGXvC0ZRXmfkHZEK8J7/9zkwmrWLKaFFmgC85Q00k4yWeP  
cusOTuX9quZtn4Vz/Jf8QrSVn0v4th14Qz6GSNDnbpGRxNi/SHs5BcEiz9asJLDO  
t9y3z1H4TQ7Wh7lerrHFM8BvDZcCPZKnCCWDelm6bLfU5WsKh8IDhiro8xW6WSXo  
7e+meTaaIgJ2YVHxapZfn4Hs52zAcLVYaeTb14TPBcgwsyQsgxI=  
-----END PUBLIC KEY-----

```
SEQUENCE {
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
  }
  BIT_STRING { '00' 'd7b2b47254aae0db45e7930d4a98d2c97d8f1397d17
89dafa17024b316e9bec94fc9946d42f19b79a7413bbaa33e7149cb42ed51156
93ac041facb988adeb5fe0e1d8631184995b592c397d2294e2e14f90aa414ba3
826899ac43f4cccacbc26e9a832b95118d5cb433cbef9660b00138e0817f61e7
62ca274c36ad554eb22aac1162e4ab01acba1e38c4efd8f80b65b333d0f72e55
dfe719c9c1ebb9889e7c56106c0fd73803a2aecfeafded7aa3cb2ceda54d12bd
8cd36a78cf975943b47abd25e880ac452e5742ed1e8d1a82afa86e590c758c15
ae4d2840d92bca1a5090f40496597fca7d8b9513f1a1bda6e950aaa98de46750
7d4a4f5a4f0599216582c3572f62eda8905ab3581670c4a02777a33e0ca7295f
d8f4ff6d1a0a3a7683d65f5f5f7fc60da023e826c5f92144c02f7d1ba1075987
553ea9367fcd76d990b7fa99cd45afdb8836d43e459f5187df058479709a01ea
6835935fa70460990cd3dc1ba401ba94bab1dde41ac67ab3319dcaca06048d4c
4eef27ee13a9c17d0538f430f2d642dc2415660de78877d8d8abc72523978c04
2e4285f4319846c44126242976844c10e556ba215b5a719e59d0c6b2a96d3985
9071fdcc2cde7524a7bedae54e85b318e854e8fe2b2f3edfac9719128270aafd
1e5044c3a4fdaf9ff31f90784b8e8e4596144a0daf586511d3d9962b9ea95af
197b4e45fc60d2b1ed15de3a5bef5f89bdc79d91051d9b2816e74fa54531efdc1
cbe74d448857f476bcd58f21c0b653b3b76a4e076a6559a302718555cc63f748
59aabab925f023861ca8cd0f7badb2871f67d55326d7451135ad45f4a1ba6911
8fbb2c8a30eec9392ef3f977066c9add5c710cc647b1514d217d958c7017c3e9
0fd20c04e674b90486e9370a31a001d32f473979e4906749e7e477fa0b74508f
8a5f2378312b83c25bd388ca0b0fff7478baf42b71667edaac97c46b129643e5
86e5b055a0c211946d4f36e675bed5860fa042a315d9826164d6a9237c35a5fb
f495490a5bd4df248b95c4aae7784b605673166ac4245b5b4b082a09e9323e62
f2078c5b76783446defd736ad3a3702d49b089844900a61833397bc4419b30d7
a97a0b387c1911474c4d41b53e32a977acb6f0ea75db65bb39e59e701e76957d
ef6f2d44559c31a77122b5204e3b5c219f1688b14ed0bc0b801b3e6e82dcd43e
9c0e9f41744cd9815bd1bc8820d8bb123f04facd1b1b685dd5a2b1b8dbbf3ed9
33670f095a180b4f192d08b10b8fabdbfcc2b24518e32eea0a5e0c904ca84478
0083f3b0cd2d0b8b6af67bc355b9494025dc7b0a78fa80e3a2dbfeb51328851d
6078198e9493651ae787ec0251f922ba30e9f51df62a6d72784cf3dd20539317
6dfa324a512bd94970a36dd34a514a86791f0eb36f0145b09ab64651b4a0313b
299611a2a1c48891627598768a3114060ba4443486df51522a1ce88b30985c21
6f8e6ed178dd567b304a0d4cafba882a28342f17a9aa26ae58db630083d2c358
fdf566c3f5d62a428567bc9ea8ce95caa0f35474b0bfa8f339a250ab4dfcf208
```

```

3be8eefbc1055e18fe15370eecb260566d83ff06b211aaec43ca29b54ccd00f8
815a2465ef0b46515cc7e41f3124f09efff739309ab58b29a1459a00bce5038e
938c9678f72eb0e4ee5fdaae66d9f8573fc97fc42b4959f4bf8b61d78433e86b
0335d6e9191c4d8bf487b3905c108cfd6ac24b0ceb7dcb7cf51f84d0ed687b95
eaeblc533c06f0d97023d92a70825837b59ba6cb7d4e56b0a87c203862ae8f31
5ba5925e8edefa679369a2202766151f16a965f9f81ece76cc070b55869e4db9
784cf05c830b3242c8312' }
}

```

The following is the ML-DSA-65 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-----
MIIHsjALBglghkgBZQMEAxIDggehAEhoPZGXjjHrPd24sEc0gtK4il9iWUn9j1il
YeaWvUwn0Fs427Lt8B5mTv2Bvh6ok2iM5oqilRxZWPi7xutOie5n0sAyCVTVchLK
xyKf8dbq8DkovVFRH42I2EdzbH3icwlZeOVBBxMWCXiGdxG/VTmgv8TDUMK+Vyuv
DuLi+xbM/qCAKNmaxJrrtlk33c4RHNq2L/886ouiIz0eVvvFxaHnJt5j+t0q8Bax
GRd/o9lxotkncXP85VtndFrwt8IdWX2+uT5qMvNBxJpai+noJQiNHYqkUVXWYK4V
Nn50sAO4/feFEHGULzn5//CQI+r0UQTSqEpFkG7tRnGkTcKNJ5h7tV32np6FYfYa
gKcmmVA4Zf7Zt+5yqOF6GcQIFE9LKa/vcDHDpthXFhC0LJ9CEkWoJxl+FoErAxFZ
tluWh+Wz6TTfIlrpinm6c9Kzmdc1EO/60Z5TuEUPC6j84QEv2Y0mCnSqghP64kmg
BrHDTluguILyY3giL7NvIoPCQ/D/618btBSgpw1V49QKVrbLyIrh8Dt7KILZje6i
jhRcne39jq8c7y7ZSofD41k9G0eoNDCpD4N2mGCrB9PbtF1tnQiv4Wb8i86QX7P
H52JMXteU51YevFrnhMT4EUU/6ZLqLP/K4Mh+IEcs/sCLi9kTnCkuAovv+5gSrtz
eQkeqObF038AoNma0DAeThwAoIEoTa/XalWjreY00kDi9sMEeA0ReeEfLUGnHXP
KKxgHHeZ2VghDdvLIm5Rr++fHeR7Bzhz1tP5dFa+3ghQgudKKYss1I9LMJMVXzZs
j6YBxq+FjfoywISRsQKYh/kDNZSaXW7apnmIKjqVlr9tlwioH0udPYy/OEr4GqyV
4rMpTgR4msg3J6XcBFwflq9B2KBTUW/u7rxSdG62qygZ4JEIcQ2DXwEfpjBlhyrT
NNXN/7KyMQUH6S/Jk64xfal/TzCc2vD2ftmdkCFVdgg4SflTskbX/ts/22dnmFC1
rUBOZBR/t89Pau3dBa+0uDSWjR/ogBSWdc5dlCI2Um4SpHjWnl++aXAcZCMBORQ
GM/HsqtDChOmsax7sCzMuz2RGsLxEghhP74Cm/30As9c04lQ7XLIOUTt+8dWFa+H
+GTAufPFVfBFQShjpAwG0dq1Yr3/BXG408ORE70wCIC7pemYI5uV+pg31kFtTzmL
OtvNMJg+01krTZ731CNv0A9Q2YqloINaxBcnIPd9lhcmcpGM/o/3pacCeD7cK6Mb
IlkBWhEvx/RoqcL5RkA5AC0w72eLTLeYvBfiFr96mnwYug03tY/QdRXTEVBj02FL
56B+dEMAdQ3x0sWHUziQWer8PXhczdMcB2SL7cA6XDUK1G0GTvNBpVc3Ryn8Tilt
YuKlGRIEUwQovBUir6KP9f4WVeMEylvIwnrQ4MaJndTfKJVsFLOMyTaCzv5AK71e
gtKcRk5E6103ti/FaN/gzG6OFrrqBeUTVZDxkpTnPoNnsCFtu4FQMLneVZE/CAOc
QjUcWeVRXdWvjgiaFeYl6Pbe5jk4bEZJfXomMoh3TeWBp96WKbQbRCQUH5ePuDMS
CO/ew8bg3jm8VwY/PclsrWnZwiR6inLx8xtZIO4iJCDrOhqp7UbHCz+birRjZfO
NvvFbqQvrpfpmp6wRSGRHjDzt8eux57EakJhQT9WXW98fSdxwActjwXOanSY/utQH
P2qfbCuK9LTDMqEDoM/6Xe6y0GLKPCFF02ACa+FFfK9KRCTvdJSIBNZvRkh3Msgg
LHlUEGR7TqcdYnwiYCTMo1SkHwh3s48Zs3dK0glcjaU7Bp4hx2ri0gB+FngelACA
0zt321Lp9aWZBDnK8IOpW4M/Aq0QoIwabQ8mDABYhb1KL0dwOlrvRlKH01OxisIl
FDFiEP9WaBSx4eik9bxmdPdlZmQ0MEMi09Q1fn877vyN70MKLGbgtZ110HxTxC/
uyG7oSq2IKojlvVsBoa06pAXmQikIwsv6K12xKkUju+ahqNjWmqne8Hc+2+6Wad9
/am3Uw3AyoZiYnlzc44Burjwi0kf6EqkZBvWakEM2XUgJl8vIx8rNeFesvoE0r2U
lad6uvHg4WEBcPkAh/W0bqmIsrwFEv2g+pi9rdbEXFMB0JSDZzJltasuEPS6Ug9r
utVkpCPV4nvBCA99IOEylqMYGVTdNGScld6+F99ch3quCo/hJsR3WfPdTWSKDQCL
avXozTG+aakpbU8/0l7YbyIeS5P2X1kplnUzYkuSNXUMHB1ULWFNtEJpxMcWlu+
SlcVVnwSU0rsdmB2Huu5+uKJHHdFibgOVmrVV93vc2cZa3In6phw7wnd/seda5MZ
poebUgXXa/erpazzOvtZ0X/FTmg4PWvloI6bZtpT3N4Ai7KUuFgr0TLNzEmVn9vC
HlJyGIDIRQNSx58DpDu9hMTN/cbFKQBeHnzZo0mnFoolVpul3qgYlolakUZrluZO
IL9iQXGYr8ToHCjdd+1AKCMjmLUvvehryE9HW5AWcQziqrwRoGtNuskB7BbPNlyj
8tU4E5SKaToPk+ecRspdWm3KPSjKUK0YvRP8pVBZ3ZsYX3n5xHGWPogbIQS8RgoF
HgLy6ERP
-----END PUBLIC KEY-----

```

```

SEQUENCE {
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
  }
  BIT_STRING { '00' '48683d91978e31eb3dddb8b0473482d2b88a5f62594
9fd8f58a561e696bd4c27d05b38dbb2edf01e664efd81be1ea893688ce68aa2d
51c5958f8bbcb6eb4e89ee67d2c0320954d57212cac7229ff1d6eaf03928bd515

```

```
11f8d88d847736c7de2730d5978e5410713160978867711bf5539a0bfc4c350c
2be572baf0ee2efb16ccfea08028d99ac49aebb75937ddce111cdab62fff3ce
a8ba2233d1e56fbc5c5a1e726de63fadd2af016b119177fa3d971a2d9277173f
ce55b67745af0b7c21d597dbeb93e6a32f341c49a5a8be9e825088d1f2aa4515
5d6c8ae15367e4eb003b8fdf7851071949739f9fff09023eaf45104d2a84a459
06eed4671a44dc28d27987bb55df69e9e8561f61a80a72699503865fed9b7ee7
2a8e17a19c408144f4b29afef7031c3a6d8571610b42c9f421245a88f197e168
12b031159b65b9687e5b3e934c5225ae98a79ba73d2b399d73510effad19e53b
8450f0ba8fcel012fd98d260a74aaaa13fae249a006b1c34f5ba0b882f263782
22fb36f2283c243f0ffeb5f1bb414a0a70d55e3d40a56b6cbc88aelf03b7b288
2d98deea28e145c9dedfd8eaf1cef2ed94a8b050f8964f46d1ea0d0c2a43e0dd
a6182adbf4f6ed175b6742257859bf22f3a417ecf1f9d89317b5e539d587af16
b9e1313e04514ffa64ba8b3ff2b8321f8811cb3fb022c8f644e70a4b80a2fbfe
e604abb7379091ea8e6c5c74dfc0283666b40c0793870028204a136bf5da9568
eb798d349038bdb0c11e03445e7847cb5069c75cf28ac601c7799d958210ddbc
b226e51afef9f1de47b073873d6d3f97456bede085082e74a298b2cd48f4b309
3155f366c8fa601c6af858dfa32c08491b2a29887f90335949a5d6edaa679882
a3a95d6bf6d970a221f4b9d3d8cbf384af81aac95e2b3294e04789ac83727a5d
c04559f96af41d8a053516feeeebc52746eb6ab2819e09108710d835f011fa63
065872ad334d5cdfb2b2310507e92fc993ae317da97f4f309cdaf0f67ed99d9
0215576083849f953b246d7fedb3fdb67679850a5ad404e64147fb7cf4f6aedd
d05afb4b834968d1fe88014960dce5d942236526e12a478d69e5fbeb6970310b3
08c06845018cfc7b2ab430a13a6b1ac7bb02cccb3d911ac2f11068613fbc029
bfdce02cf5cd38950ed72c83944edfbc75615af87f864c051f3c55456c541286
3a40c06d1dab562bdf0571b8d3c3917bbd300880bba5e998239b95fa91b7d64
16d4f398b3adbcd30983ed3592b4d9ef7d4236fd00f50d98aa53a235ac417272
0f77d96172672980cfe8ff7a5a702783edc2ba31b2259015a112fc7f468a9c2f
9464039002d30ef678b4cb798bc116216bf7a9a7c18ba03b7b58fd07515d3115
049d3614be7a07e744300750df1d2c58753389059eafc3d785ccdd31c07648be
dc03a5c3b8ad46d064d59c13d57374729fc4e295362e2a5191204530428bc152
2afa28ff5fel655e304ca5bc8c27ad0e0c6a39dd4df28956c14b38cc93682cef
e402bbd5e82d29c464e44eb5d37b48fc568dfe0cc6e8e16baea05e5135590f19
294e73e8367b0216dbb815030b9de55913f08039c42351c59e5515dd5af8e089
a15e625e8f6dee639386c46497d7a263288774de581a7de9629b41b4424141f9
78fb8331208efdec3c6e0de39bc57063f3dcd6c470373c08891ea29cbc7cc6d6
483b8889083ace86aa7b51b1c2cfe6e2ad18d97ce36fbc56ea42fae97e6a7ac1
14864478c366dfllebb1e7b11a9098504fd5975bdf1f49dc70002b63c1739a9d2
63fbad4073f6a9f6c2b8af4b4c332a103a0cffa5deeb2d062ca3c215fd360026
be7c5164f4a4424ef74948804d66f46487732c8202c795478647b4ea71d627c0
86024cca354a41f0877b38f19b3774ad2095c8da53b069e21c76ae2d2007e167
19ed40080d334f7da52e9f5a5990439caf083a95b833f02ad10a08c1a6d0f260
c007285bd4a2f47703a5aef465287d253b18ac22514316210ff566814b10f87a
293d6f199d3c3959990d0c1268b4f50d5f9fcefbbf237bd0c28b80182d665974
1f14f10bfbb21bba12ab620aa2396f56c0686b4ea9017990224216b2fe8ad76c
4a9148eef9a86a3635a6aa77bc1dcfb6fba59a77dfda9b7530dc0ca8648c8d97
3738e01bab8f08b4905e84aa4641bd602410cd97520265f2f231f2b35e15eb2f
a04d2bd94d5a77abaf1e0e161010a990087f5b46ea988b2bc0512fda0fa923da
dd6c45c5301d09843673265b5ab2e10f4ba520f6bbad564a5c3d5e27bdb08f7
d20e13296a3181954c39c649c943ebe17df5c1f7aae0a8fe126c477585a5d4d6
48a0d008b6af5e8cd31be69a9296d4f3fd25ed86f221e4b93f65f59299675336
24b9235750c30707550b58536d109a7131c5a5bbe4a5715567c12534aec76607
61eebb9fae2891c774589b80e566ad557ddef7367196b7227ea9870ef09ddfec
79d6b9319a6879b5205d76bf7aba5acf33afb59d17fc54e68383d6be5a08e9b6
6da53dcde008bb294b8582bd132cdcc49959fdbc21e52721880c8ad0352c79f0
3a43bbd84c4cdfdc6c529005e1e7cd9a349a7168a35569ba5dea818968d5a914
66bd6e64e20bf62417198afc4e81c28dd77ed4028232398b52fbde86bc84f475
b9016710ce2aabc11a06b4dbac901ec16cf365ca3f2d53813948a693a0f93e79
c46ca5d5a6dca3d28ca50ad18bd13fca55059dd9b185f79f9c47196a4e81b210
4bc460a051e02f2e8444f' }
}
```

The following is the ML-DSA-87 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-----

MIiKmjALBgIghkgBZQMEAxMDggohAJeSvOwvJDBoaoL8zzwvX/Zl53HXq0G5AljP  
p+kOyXEkpzsY05uiGrZNDnxDP1pSHv/hj4bkahiJUsRGfgSLcp5/xNEV5+SNOYlt  
X+EzS3N3vYssweVQHS0IzblKDbEYdQUH4036misgQb6vhkHBNmvYAhTcSD3B504  
6pZa5ue3tMmlx0IcYPJEUboekz2xou4Wx5VZ8hs9G4MFhQqkKvuxPx9NW59INfnY  
ffzrFi009Kf9xMuhdDzRyHu0ln2hbMh2S2Vp3471vcv/6aTgV0jm/filr55063dz  
ti6Phfmla1SJRVUYRPvYmAakrDab7S01YQD2iKatXgpwmCbcRENpHiPFUG5kI2Hv  
WjE3EvebxLMyAGHKhaS6sX5/LD0biJM6o6584WtEDWAY+eBNr1clx/GpP60aWie2  
eJW9JJqpFoXeIK8yyLfiaMf5aHfQyFABElpPCo8bgmT6br5aNJ2K7K0aFimczy/Z  
x7hbrOLO06oSdrph7njtfllyltznzDRYqTVAM0aru6vlagojFv7J26g7UdQv0xZ/Hg  
+QhV1cZlCbIQJl3B5U7ES006fPmu8Ri0TYCRL0DRZqZlHhFs6+SSKacGLAMTH3Gr  
0ik/dvfvwyFbqXgAA35Y5HC9u7Q8GwQ56vecVNk7RkrJ7+n74VGHTPSqZMvuKMxM  
D+d3Xl2HDxwC5bLjxQBMMV8kybd5y3U6J300cf1CXra8LKV54SnbUfchQPMey5dr  
UMcxLpeXl4xbGsJKX6NHZJFuCoPlw7Z1zTC4Hj+hC5NETgc5dXHM6Yso2lHbKFa8  
coxbCxGB4vvTh7THmrGl/v7ONxZ693LdrRTrTDMc2lpZ0OnrFz7GMVCRFwAno6te  
9qoSnLhYVye5NYooUB1xOnLz8dsxcUKG+bZAgBOvBgRddVkvwLfdR8c+2cdbEenX  
xp98rfwygKkGLFJzxDvhw0+HRIhkzqelyXltMvWb1fJThGU7tcT6pFvqi4lAKEPm  
Rba5Jp4r2YjdrLazMo/7BgRQ998IAFPmlpslHodezsMs/FkoQNaatpp14Gs3nFNd  
lSZrCC9PCckxYrM7DZ9zB6TqqLIQRDF+1m+O4+q71FlnslqBM/SWRotSuv/b+tk+  
7xqYGLXkLscieIo9jTUp/Hd9K6VwgB364B7IgwKDFB+54DVXJ2Re4QRsP5Ffaugt  
rU+2sDVqRlGP/INBVcO0/m2vpsyKXM9TxxoISdJUT33PcnVOcOG337RHu070nRpx  
j2Fxu84gCVDGzpjHBrFRo+hxlC5JcxvWZQqbDKly2hxfE21Egg6mODwI87OEzyM4  
54nFE/YYzFaUpvDO4QRRHh7XxfI6Hr/YoNuEJFUyQBVtv2IoMbDGQ9HFUbbz96mN  
KbhCLBaZfphXu4WSVvZBzdnIRWlPpHF2QAozz8ak5U6FT3l00QITpzP9rc2aTkm  
2u/rstd6palom5LzFoZmnfFtFxxMWPeiz7ct0aUekvglmTp0Aivn6etgVGVEVw1N  
FJKPICFeeyIqxWtRrb7I2L22mDl5p+OiG0S10VGMqX0LUZXlHtaiQlDl10fh7epR  
tEjj6RRwVM6SeHPJDbOU2GiI4H3/F3WTlveeFSMCIErrA74jhq8+JAeL0CixaJ9e  
FHyfRSyM6wLsWcydtjoDV2zur+mCOQI4l9oCnmMKU8Def0NaGYaXkvqzbnueYldg  
8JBp5kMucAA1rCoCh5//Ch4b7FIgRxx9l0td8e/VPuORRMp4lAhS9eyXJ5BLNm7e  
Tl4tMx+tX8KC6ixH6SMUJ3HD3XWocldife+Z5fGOnZ7WI8F10CiIxr+CwHqAlUcW  
s8PCvb4unwqbuq6+tNupNodkBvXADo5LvQPewFeX5iB8WrbIjxpohCG9BaEU9Nfe  
KsJB+g6L7f9H92Ldy+qpEAT40x6FCVYBBUmUrTgm40S6lgQIEPwLktheSM+t4ALG  
LlpJoHMas4NEvBY23xa/YHlWhV5WlOQAPHGOS62eWgmZefzd7rHEP3ds03o0F8sO  
GE4p75vA6HRlumY74J4Aq1Yut8D3Fl+WmptCQUGYzPG/8qLl1omkFOznZiknZlaJ  
6U25YeuuxWFcvBp4lcaFGslhQy/xEYlGB9Mu+dxzLVEzO+S00OMN3qeE7Ki+R+dB  
vpwZYx3EcKuU9NwTPNjP9Q014fBcJd7QX31mOHQ3eUGu3HW8LwX7HDjsDzcGWXL  
Npk/YzsEcuUNCSosbG98dPmRZzBifd1+U0J6dvPXWkOIym40KC6y3xjJRsmKQw  
jNfxtovRjTtHaZypu2FqNeMKG+1b0qz0hSXUoBFxjJiyKQq8vmALF03u4viJnJ+C1  
zkX7t6GvGjsoqNlLeJdjyILjm8mOnwrXYCW/DdLwApjnFBoiazl87kFPYE0eC6VN  
EdX+WLzOpq13rS6MHKRPmkWQFLe5EAGx76itFypSP7jjZbV3Ehv5/Yiixgwh6CHX  
tqy0elqZXkDKztXCI7j+beXhjp0uWJOU/rt6rn/xoUYmDi8RDpOVKCE6ACWjjsea  
q8hhs168UJpGdMEyqqy34BRvFO/RHPyvTKpPd1pxbOMl4KQlPNNJlyC88TdfCvxF  
BG/Bofg6nTKXd6cITkqtrnEizpcAWTBSjrPH9/ESmzcoh6NxFVo7ogGiXL8dy2Tn  
ze4JLDFB+1VQ/j0N2C6HDleLK0ZQCBGR049laXc8Z30ftppCt33Lp6z/2V/URS4j  
qqHTfh2iFR6mWNQKNZayesn4Ep3GzwZDdyYktZ9PRhIw30ccomCHw5QtXGAh32CC  
glk1o/h8t2Kww7HQ3aSmUzllvvG3uCUkJUwBTQkP7YV8RMGDnGLMCMtj+tkKEfU0  
citu4VdPlhSdVdde3kiHak4IURQxwGJlDhbHSrnzJC8ts/+xKolhb/qikdb2NzsH  
8205MrO9sEWZ3WTq3X+Tw8VkwlihyB3PHJwx5bBlaPl1RMF9wVaYxcs4mDqa/EJ4  
P6p3OlLJ2CYGkL6eMVAqW8FQneo/aVh21clv8XK6g+am2KfWu+u7zaNnJzGYP4m8  
WDHcN8PzxcVvrMaX88sgvV2629c5UHERC9iaQH+FZ25Pf1Hc9j+c1YrhGwfyFbR  
gCdiha68cteYi951y8pw0xnTLODMA107KtRVcj7gx/RzbObmZlxayjKkgcU4Obwl  
kWeWE9BCM5Xuuaqu4yBhSafVUNZ/xf3+SopcNdJRC2ZDeauPcoVaKvR6vOKmMgSO  
r4nly0qi3rxTpZUQOszk8c/xis/wev4etXFqoeQLYxNMOjrpV5+of1Fb4JPC0p22  
lrZck2YeAGNRWScE0JPMZxbCNC6xhTlIyFxrIooVEYse3fn470erFvKKP+qALXT  
SfilR62HW5aowrKRDJMBMJo/kTilaTER9Vs8AJypR8Od/ILZjrHKpKnL6IX3hVqG  
5VvgYiIvi6kKl0BzmmsxISrs4KNKYA==

-----END PUBLIC KEY-----

```
SEQUENCE {
  SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
  }
  BIT_STRING { '00' '9792bcec2f2430686a82fccf3c2f5ff665e771d7ab4
1b90258cfa7e90ec97124a73b323b9ba21ab64d767c433f5a521effe18f86e46
a188952c4467e048b729e7fc4d115e7e48da1896d5fe119b10dcddef62cb3079
54074b42336e52836de61da941f8d37ea68ac8106fabe19070679af600853712
```

0f70793b8ea9cc0e6e7b7b4c9a5c7421c60f24451bale933db1a2eel6c79559f  
21b3d1b8305850aa42afbb13f1f4d5b9f4835f9d87dfceb162d0ef4a7fdc4cba  
1743cd1c87bb4967da16cc8764b6569df8ee5bdcbbffe9a4e05748e6fdf225af9  
e4eeb7773b62e8f85f9b56b548945551844fbd89806a4ac369bed2d256100f68  
8a6ad5e0a709826dc4449e91e23c5506e642361ef5a313712f79bc4b3186861c  
a85a4bab17e7f943d1b8a333aa3ae7ce16b440d6018f9e04daf5725c7f1a93fa  
d1a5a27b67895bd249aa91685de20af32c8b7e268c7f96877d0c85001135a4f0  
a8f1b8264fa6ebe5a349d8aecad1a16299ccf2fd9c7b85bace2ced3aa1276ba6  
1ee78ed7e5ca5b67cdd458a9354030e6abbbabf56a0a2316fec9dba83b51d42f  
d3167f1e0f90855d5c66509b210265dc1e54ec44b43ba7cf9aef118b44d80912  
ce75166a6651e116cebe49229a7062c09931f71abd2293f76f7efc3215ba9780  
0037e58e470bdbbb43c1b0439eaf79c54d93b44aac9efe9fbe151874cfb2a64c  
bee28cc4c0fe7775e5d870f1c02e5b2e3c5004c995f24c9b779cb753a277d0e7  
1fd425eb6bc2ca56ce129db51f70740f31e63976b50c7312e9797d78c5b1ac24  
a5fa347cc916e0a83f5c3b675cd30b81e3fa10b93444e07397571cce98b28da5  
1db9056bc728c5b0b1181e2fbd387b4c79ab1a5fefece37167af772ddad14eb4  
c3982da5a59d0e9eb173ec6315091170027a3ab5ef6aa129cb8585727b9358a2  
8501d713a72f3f1db31714286f9b6408013af06045d75592fc0b7dd47c73ed9c  
75b11e9d7c69f7cadfc3280a9062c5273c43belc34f87448864cea7b5c97d6d3  
2f59bd5f25384653bb5c4faa45bea8b89402843e645b6b9269e2bd988ddacb03  
3328fffb060450f7df080053e6969b251e875ecec32cfc592840d69ab69a75e06  
b379c535d95266b082f4f09c93162b33b0d9f7307a4eaaa52104437fed66f8ee  
3eabbd45d67b25a8133f496468b52baffdbfad93eef1a9818b5e42ec722788a3  
d8d3529fc777d2ba570801dfae01ec88302837c1fb9e0355727645ee1046c3f9  
15f6ae82dad4fb6b0356a46518fffc834155c3b4fe6dafa6cc8a5ccf53c73a084  
9d8d44f7dcf72754e70elb7dfb447bb4ef49d1a718f6171bbce200950e0ce926  
106b151a3e871d5ce49731bd6650a9b0ca972dal5c5f136d44820ea6383c08f3b  
384cf2338e789c513f618cc5694a6f0cee104511e1ed7c5f23alebfd8a0db842  
4553240156dbf622831b0c643d1c551b6f3f7a98d29b85c2de05a65fa615eee1  
6495bd90737672115b53e91c5d90028cf3f1a93953a153de53b44084e9ccff6b  
736693926daefeb2d77aa5ad689b92f31686669df16d1715cc58f7a2cfb72dd  
1a51e92f825993a74022be7e9eb6054654457094d14928f20215e7b222ac56b5  
1adbec8d8bdb6983979a7e3a21b44b5d1518ca97d0b5195f51ed6a24350c8974  
7eledea51b448e3e9147054ce927873c90db394d86888e07dff177593d6f79e1  
52302204aeb03be2386af3e24078bd028b1689f5e147c9f452c8ceb02ec59cc9  
db63a03576f6ceafe98239023897da0236630a53c0de7f435a19869792fab36e7  
b9e635760f9069e6432e700035ac2a02879ffff0alelbec522047193d94eb5df  
1efd53eeal144ca78940852f5ec9727904b366ede4f5e2d331fad5fc282ea2c4  
7e923142771c3dd75a87357487def99e5f18e9d9ed623c175d02888c51f82c07  
a80d54716b3c3c2bdb2e9f0a9bbaeebeb4d52936876406f5c00e8e4bbd0a5ec  
05797e6207c5ab6c88f1a688421bd05a114f4d7de2ac241fa0e8bedff47f762d  
dcbeaa91004f8d31e85095c81054994ad3826e344ba96040810fc0b2ad1de48c  
fade002c62e5a49a0731ab38344bc1636df16bf607d56855e56d684003c718e4  
bad9e5a099979fcddeeb1c4a7776cd37a3417cb0e184e29ef9bc0e87475ba663  
be09e00ab562eb7c0f7165f969a9b42414198ccf1bfff2a2c8d689a414ece7662  
927665689e94db961ebaec5615cbc1a7895c6851ac961432ff1118d4607d32ef  
9dc732d51333be4b4d0e30dde784eca8be47e741be9c19631dc470a52ef4dc1  
3a4f3633fd434d787c170977b417df598e1d0dde506bb71d6f0bc17ec703b03  
cdc1965cb36993f633b0472e50d0923ac6c66fdf1d3e6459cc121f0f5f94d09e  
9dbcf5d690e23233838a0bacb7c638d1b2650a4308cd171b6855126d1da672a6  
ed85a8d78c286fb56f4ab3d21497528045c63262c8a42af2f9802c53b7bb8be2  
8e78fe0b5ce45fbb7a1af1a3b28a8d94b7890e3c882e39bc98e9f0ad76025bf0  
dd2f00298e7141a226b3d7cee414f604d1e0ba54d11d5fe58bccea6ad77ad2e8  
clcaacf32459014b7b91001b1efa8ad172a523fb8e365b577121bf9fd88a2c60  
c21e821d7b6acb47a5a995e40caced5c223b8fe6de5e18e9d2e5893aefebb7aa  
e7ff1a146260e2f110e939528213a0025a38ec79aabc861b25ebc509a4674c13  
2aaacb7e0146f14efd11cfcaf4caa4f775a716ce325e0a435a4d349d720bcf13  
7450afc45046fclalf83a9d329777a7084e4aadae7122ce97005930528eb3c7f  
7f1129b372887a371155a3ba201a25cbf1dcb64e7cdee092c3141fb5550fe3d0  
dd82e870e78b2b46500818113b8f6569773c677385b69a42b77dcba7acffd95  
fd4452e23aaald37eld2151ea658d40a3596b27ac9f8129dc6cf0643772624b  
59f4f461230df471ca26087c3942d5c6687df6082835935a3f87cb762b0c3b1d  
0dda4a6533965bef1b7b8292e254c014d090fed857c44c1839c694c0a64e3fad  
90a11f534722b6ee1574f2e149d55d744de4887024e08511431c062750e16c74  
ab9f3242f2db3ffb12a8d6107faa229d6f6373b07f36d3932b3bdb04c19dd64e  
add7f93c3c564c358a1c81dcflc9c31e5b06568f97544c17dc15698c5cb38983

```
a9afc42783faa773a52c9d8260690be9e3156aa5bc1509dea3f69587695cd6ff
172ba83e6a6d8a7d6bbebbbcda3672731983f89bc5831dc37c3f3c5c56facc69
7f3cb20bd5dbadb702e54844ac2f626901fe159db93dfd4773d8fe73562b846
c1fc856d1802762840ebc72d7988bde75cbca70d319d32ce0cc0253bb2ad4557
23ee0c7f4736ce6e6665c5aca32a481c53839bc259167b013d0423395eeb9aaa
ee3206149a7d550d67fc5fdfe4a8a5c35d2510b664379ab8f72855a2af47abce
2a632048eaf89e5cb4a88debc53a595103acce4f1cff18acff07afeleb5716aa
1e40b63134c3a3ae9579fa87f515be093c2d29db6d6b65c93661e00636b59270
4d093cc6716c2342eb1853d48c85c63ac8a2854462c7b77e7e3bd1eac5bca28f
faa00b5d349f8a547ad875b96a8c2b2910c9301309a3f9138a5693111f55b3c0
09ca947c39dfc82d98eb1caa4a9cbe885f786fa86e55be062222f8ba90a97407
3326b31212aece0a34a60' }
}
```

### C.3. Example Certificates

NOTE: The example certificates in this section have key usage bits set to digitalSignature, keyCertSign, and cRLSign to lessen the number of examples, i.e., brevity. Certificate Policies (CPs) [RFC3647] for production CAs should consider whether this combination is appropriate.

The following is a self-signed certificate for the ML-DSA-44 public key in the previous section. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the certificates are the same.

```
-----BEGIN CERTIFICATE-----
MIIP1DCCBgqgAwIBAgIUfZ/+byL9XMqSuk32/V4o0N44804wCwYJYIZIAWUDBAMR
MCIXDTALBgNVBAoTBELFVEYxETAPBgNVBAMTCExBTvBTIFdHMB4XDTIwMDIwMzA0
MzIxMFoXDTQwMDEyOTA0MzIxMFowIjENMAsGA1UEChMESUVURjERMA8GA1UEAxMI
TEFNUFUMgV0cwggUyMASGCWCGSAFlAwQDEQOCBSEA17K0clSq4NtF55MNSpjSyX2P
E5fReJ2voXaksxbpvs1PyZrTqVgbeadB07qjPnFJy0LtURVpOsBB+suYit61/g4d
hJEYSZWlksOX0ilOLhT5CqQUUjgmiZrEP0zMrLwm6agyuVEY1ctDPL75ZgsAE44I
F/YediyidMNq1VTrIqrBFi5KsBrLoeOMTv2PgLZbMz0PcuVd/nHOnB67mInnxWEG
wPlzgDoq7P6v3teqPLLO2lTRK9jNNqeM+XWU00er0l6ICsRS5XQu0ejRqCr6huWQ
x1jBWuTShA2SvKGLCQ9ASWWX/KfYuVE/GhvabpUKqpjeRnUH1KTlpPBZkhZYLDVY
9i7aiQWrNYFnDEoCd3oz4Mpylf2PT/bRoKOnaD1l9fX3/GDaAj6CbF+SFEwC99G6
EHWYdVPqk2f8122ZC3+pnNRa/biDbUPkWFUYffBYR5cJoB6mg1kl+nBGCZDNPcG6
QBupS6sd3kGsZ6szGdysoGBI1MTu8n7hOpwX0FOPQw8tZC3CQVZg3niHfY2KvHJS
OXjAQuQoX0MZhGxEEmJCl2hEwQ5Va6IVtacZ5Z0MayqW05hZBx/cws3nUkp77a5U
6FsxjoVOj+Ky8+36yXGRKCCr9HlBEW6T9r9n/MfkHhLjo5FlhRKDa9YZRHT2ZYr
nqla8Ze05fxg8rHtFd46W+9fib3HnZEFHZsoFudPpUUX79wcvnTUSIV/R2vNWPIc
C2U7O3ak4HamVZowJxhVXMY/dIwaq6uSXwI4YcqM0Pe62yhx9n1VMm10URNa1F9K
G6aRGPuyyKMO7JOS7z+XcGbJrdXHEMxkexUU0hfZWMcBfD6Q/SDATmdLkEhuk3Cj
GgAdMvRz155JBnSefkd/oLdFCPil8jeDErg8Jb04jKcW//dHi69CtxZn7arJfEax
KWQ+WG5bBVomIRlG1PNuZ1vtWGD6BCoxXZgmFklqkjfdWl+/SVSQpb1N8ki5XEQu
d4S2BWcxZqxCRB0sIKgnpmj5i8geMW3Z4NEbe/XNq06NwLumwiYRJAKYYMz17xE
GbMNpegs4fBkRR0xNqBU+Mql3rLbw6nXbZbs55Z5wHnaVfe9vLURVnDGncSK1IE
47XCGfFoixTtC8C4AbPm6C3NQ+nA6fQXRM2Yfb0byIINi7Ej8E+s0bG2hd1aKxuN
u/PtkzZw8JWhgLTxktCLELj6u9/MKyRRjjLuoKXgyQTKhEeACD87DNLQuLavZ7w1
W5SUA13HsKePqA46Lb/rUTKIUDYHgZjpSTZRRnh+wCUfkiujDp9R32KmlyeEzz3S
BTkxdt+jJKUSvZSXCjbdNKUUqGer8Os28BRbCatkZRTkAXOymWEaKhxIiRYnWYdo
oxFAYLPeQ0ht9RUioc6IswmFwhb45u0XjdVnswSglMr7qIKig0LxepqiauWNTjAI
PSw1j99WbD9dYqQoVnvJ6ozpXKoPNUdLC/qPM5olCrTfzyCDvo7vvBBV4Y/hU3Du
yyYFZtg/8GshGq7EPKKbVMzQD4gVokZe8LRlFcx+QfMSTwnv/3OTCatYspoUWaAL
z1A46TjJZ49y6w505f2q5m2fhXP81/xCtJWfS/i2HXhDPoawM1lukZHE2L9IezkF
wQjPlqwsM633LfPUfhNDtaHuV6uscUzwG8NlwI9kqcIJYN7Wbpst9TlawqHwgOG
KujzFbpZJejt76Z5NpoiAnZhUffqll+fgeznbMBwtVhp5NuXhm8FyDCzJCyDEqNC
MEAwDgYDVR0PAQH/BAQDAAGGMA8GA1UEEwB/wQFMAMBAF8wHQYDVR0OBBYEFdKa
B7H6u0j1KjCfEaGj4SOIyL/MASGCWCGSAFlAwQDEQOCXUAZ6iVH8MI4S9oZ2Ef
3CVL9Ly1FPf18v3rcvqOGgMAYWd7hM0nVZfYMVQZWWaxQWcMsOiBE0YN14oaejiV
wRyKGZV3XANWtd60e8h8TovxyTJ/xK/Vw3hlU+F9YpsPJxQnZUGUMrXnzNC6YeUc
rT3Y+Vk4wjXr7O6vixauM2bzAMU1jse+nrI6HqGj2lhoZwTwSD+Wim5LH4lnCgE0
s2oY1scn3JsCexJ5R5OkjHq2bt9XrBgRORTADQOrtlpL0d3Eze/dDZm/Klby9OR
Ia4HUL7FWtWoy86Y5TiuUj1h1pKZdjMPYj/JXAHRQDtJ5cuoGBL0N1DdATEJNCee
-----
```

zQfMqzTCyJcN091QkuFjDhQjzJ+sQ6G02w49lw8KpmlASuh7BLTPcuz7Z+rLpNjN  
jmW67rR6+hHMK474mSKIznuO3vVKnidntjLhSYclsoxvYPCLWWnl4m3XyjlrlnzD  
4Soec2I2AjkNZKCO9KKA81cRzIcNjJc7sbnrLv/hKXNUTESn4s3yAyRPU7N6bVIy  
N9ifBvblU07WMPi8A7/f9zVCaLYx87ym9P7GGpMjDYrPUQpOaKQdu4ycWuPrLEA  
2BoHIVzbHHm9373BT1LjcxjR5SbbhNfG+42hwG284VlVzclW/XiipaWN8jnONmxt  
kLMui9R/wf0TCehilMDDtRznfm37b2ci5o9MP/LrTDRpMVBudDuwIZmLgPQ/bj08  
n+VHD8D2WADpR/kEMpDhSwG2P44mwwE4CUKGBHS0qQLOSRwMlQVEzwxpOOrLMusw  
JmzoLE0KNsUR6o/3xAlUmjqCZMqYPYxtXgNfJEJDp3VliqyZKliES3EQ0/h8m7oZ  
3YqNkrEpTgVV7EmVpUjCvszjWgXcSKynVVSWQd3j0Zf83zXRLwmq8+anJ3XNGCSa  
IecO2sZxDbaiHhWfYRkt0BGRM2QM//IPMyeXhRa/1svmbOEHGxJG9LqTffkBs+01  
Bp7r3/9lRZ+5t3eukpinpJrCT0AgeV3l3ujbzyCiQbboFDaPS4+kKvi+iS2eHjiu  
S/WkfPlGo5jksxhkceJFNPsTmGCyXGPy2/haU9hkiMg9/wmuIKm/gxRfIBh/DoIr  
1HWZjTuWcBGWtu2NuXeAvo/MbMtpB0u6mWYktHQcVxA2LenU+N5LEPbbHp+AmPQC  
RZPqBziTyx/nuVnFD+/EAbPKzeqMKKtW6nfkKt/Md4zmilvhWxx7c+wDlo9cyAf  
vsS0p5uXKKlwzaC4mBIVdPYNlZtAjBCK8asKpH3/NyYJ8xhsBjxLLiQifKiG0pA  
LLBy/LyJWmo4R4zkAtUILD4FcsIyLMIJlsqWjaNdey7bwGI75hZQkBIF8QJxFVtT  
n4HQbtuNe2ek7e72d+bayceJvlUAFXTu6oeX9/UuS7AhuY4giNzIlpNOgNwWXRxx  
REmwvPrzJatZZ7cwfsKTezSSQlv204q70+2X2h0VtUg/pkz3GknE07S3ggDR9Qkg  
bywQS/42luPIADbbAKXhHaBaX/TaD/uZVn+BOZ5sqWmxEbbHtvzlSea02JlFk4Hq  
kWbpuzByCJ25SuDRr+Xyn84ZDnetumQ0lBkc2ro+rZKXw8YGMyt0aX8ZwJxL4qNB  
/WFFEproVsOru8G7iwXgt4QP8WRBSp2kTlQUbNTF3gxOTsslkUerTnvcRQ0GpK06  
DRQG8wbjgewpHyw7O8Sfi34EjAzic0gwtIp501/MWmKpRUGaow9LPreiaLq2TBIQ  
DXEHUb9fEhY77QKeir8cpue3sShqcz9TLA5REJGqsP/8/URk7lZjiI+YwBRLp2U2  
D//ONPEq8fxrZntacZRxsdx2id/yTWumtj5swjFA4yk0tunadltDMgEYuKgr+Jw9  
G3/yFTDnepHK41V6x8eE/4JjUAvIJWADDWxud07oF/wsY0AnUuWe9DkW09g8IWhk  
NukDTdpsl08hCLF06qH3MSHJrdUAzs2GGLMCvtrXK2L3k70PcLqMXhbPSr7d1RGW  
gW0BlRfr4l+2LJ952SMv3xzuxgT43aX3FFVBxXk7nFrhWJWIpuYXRhTqASkzoZ  
KzsIRyW0ZbsaIsy0tgzzyhQvdoOoJn+2sKjcCzpfY6tgRD9sfucOmlsGet/cm5YP  
iJYei2qKMeYcvACWiI8NGY370zhlikble04xXnfJwEOYx66NjTHZqkz1/TiCBGU  
a7h+l/fnut6VfkxSlyZ2r5Gsdx7DUfNkEeKyzIMnYRA3zw3047lHqH714rV5VbE3  
yYEQWvdtYlHMFm2z9DDta59RRATOemm7AA1fYsfodrV/QPji5qPmvpHtCvfitbdL  
Fg88Zh1zV5nV+0doUTXFVR9poJRE9fASlF5uqCJ9Jx5ISfvIkGz1fmfqXhUN9fE7  
C0Ev17IYQLguTXFznRvsXvnliwR9Ut/g85JtXUiku4F2ThCBMHBDBov6p128kP+2  
7LBgShM4IG80clxon8sWh6y0RLUz1MTamEYZKXAPZzJoWhbzdNns/QTsJNP8wlu  
vBRtdkb6w4Vrm6GO2BXY6pQUBPcoDuymAhfAF9TxRn860QeMcT/NRSU9Z/8nRnz  
3KbAuMTYsQ6qbjULtdWfF9B4b4YUDQR22z8w1zCNLzgwF1GSI12xhf3ejRlwjGZJ  
J/1lUp4pEegRS/c+Li2OUvQr9Jxi8XGidEJZY1T8oVpzdJf3C29gpARWSDAXrFn0  
lgZHnqFyebcCluDW8r/wGtYmI2EC53+FlOF5AFch+3LzObZzerqwr4UMOA+B5c  
QMU5vDvlLFcWLzVJHMXJfCHL5nVSukXCMawr+DbeKjrkseG0UX0gpUbQy0vHIH1K  
2geD2xyl3TJ8jCaKOxb/Hu+KfkvtOCsh07TA+cnTV1WHR77svUcMERzHXWOFm8+U  
omIXALO1EiDbpu38gERRLkC84eMhRBQjKcdmlcBFsmilt3cfIofypuhMRiIFjIke  
00y2GEDQVsZGA/LX1HILQd4dEFDDQI2LPvCG5qe28HTfWspzsqK94IRESzm+Vmdp  
IjNzkTyrPI06yMvxaHGajwUtLWCREJOG/uXhswbX7EviVYyqCR4vzDLVXAulxo/  
OsHaQhMX8xYOLXontx7SNcBlU/EEBww5QklKuldg5igr7bDxsvZ6vHy/wcNlZY3  
RUdidnuDkpSmlhIoLz4/SW2Tm6C2u9La5evu7xAfiYlul8LE3/P0AAAAAAAAAAAA  
AAAAABcmOEM=

-----END CERTIFICATE-----

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER { 2 }
    }
    INTEGER { '159ffe6f22fd5cc42c524df6fd5e28d0de38f34e' }
    SEQUENCE {
      OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
    }
    SEQUENCE {
      SET {
        SEQUENCE {
          # organizationName
          OBJECT_IDENTIFIER { 2.5.4.10 }
          PrintableString { "IETF" }
        }
      }
    }
  }
}
```

```
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 { 2.16.840.1.101.3.4.3.17 }
  }
  BIT_STRING { '00' 'd7b2b47254aae0db45e7930d4a98d2c97d8f139
7d1789dafa17024b316e9bec94fc9946d42f19b79a7413bbaa33e7149cb42ed5
115693ac041facb988adeb5fe0e1d8631184995b592c397d2294e2e14f90aa41
4ba3826899ac43f4cccacbc26e9a832b95118d5cb433cbef9660b00138e0817f
61e762ca274c36ad554eb22aac1162e4ab01acba1e38c4efd8f80b65b333d0f7
2e55dfe71ce9c1ebb9889e7c56106c0fd73803a2aecfeafded7aa3cb2ceda54d
12bd8cd36a78cf975943b47abd25e880ac452e5742ed1e8d1a82afa86e590c75
8c15ae4d2840d92bca1a5090f40496597fca7d8b9513f1a1bda6e950aaa98de4
67507d4a4f5a4f0599216582c3572f62eda8905ab3581670c4a02777a33e0ca7
295fd8f4ff6d1a0a3a7683d65f5f5f7fc60da023e826c5f92144c02f7d1ba107
5987553ea9367fcd76d990b7fa99cd45afdb8836d43e459f5187df058479709a
01ea6835935fa70460990cd3dc1ba401ba94bab1dde41ac67ab3319dcaca0604
8d4c4eef27ee13a9c17d0538f430f2d642dc2415660de78877d8d8abc7252397
8c042e4285f4319846c44126242976844c10e556ba215b5a719e59d0c6b2a96d
39859071fdcc2cde7524a7bedae54e85b318e854e8fe2b2f3edfac9719128270
aafd1e5044c3a4fdaf9ff31f90784b8e8e4596144a0daf586511d3d9962b9ea
95af197b4e5fc60d2b1ed15de3a5bef5f89bdc79d91051d9b2816e74fa54531e
fdclcbe74d448857f476bcd58f21c0b653b3b76a4e076a6559a302718555cc63
f74859aabab925f023861ca8cd0f7badb2871f67d55326d7451135ad45f4a1ba
69118fbb2c8a30eec9392ef3f977066c9add5c710cc647b1514d217d958c7017
c3e90fd20c04e674b90486e9370a31a001d32f473979e4906749e7e477fa0b74
508f8a5f2378312b83c25bd388ca0b0fff7478baf42b71667edaac97c46b1296
43e586e5b055a0c211946d4f36e675bed5860fa042a315d9826164d6a9237c35
a5fbf495490a5bd4df248b95c4aae7784b605673166ac4245b5b4b082a09e932
3e62f2078c5b76783446defd736ad3a3702d49b089844900a61833397bc4419b
30d7a97a0b387c1911474c4d41b53e32a977acb6f0ea75db65bb39e59e701e76
957def6f2d44559c31a77122b5204e3b5c219f1688b14ed0bc0b801b3e6e82dc
d43e9c0e9f41744cd9815bd1bc8820d8bb123f04facd1b1b685dd5a2b1b8dbbf
3ed933670f095a180b4f192d08b10b8fabbdffcc2b24518e32eea0a5e0c904ca8
44780083f3b0cd2d0b8b6af67bc355b9494025dc7b0a78fa80e3a2dbfeb51328
851d6078198e9493651ae787ec0251f922ba30e9f51df62a6d72784cf3dd2053
93176dfa324a512bd94970a36dd34a514a86791f0eb36f0145b09ab64651b4a0
313b299611a2a1c48891627598768a3114060ba4443486df51522a1ce88b3098
5c216f8e6ed178dd567b304a0d4cafba882a28342f17a9aa26ae58db630083d2
c358fdf566c3f5d62a428567bc9ea8ce95caa0f35474b0bfa8f339a250ab4dfc
```

```

f2083be8eefbc1055e18fe15370eecb260566d83ff06b211aaec43ca29b54ccd
00f8815a2465ef0b46515cc7e41f3124f09efff739309ab58b29a1459a00bce5
038e938c9678f72eb0e4ee5fdaae66d9f8573fc97fc42b4959f4bf8b61d78433
e86b0335d6e9191c4d8bf487b3905c108cfd6ac24b0ceb7dcb7cf51f84d0ed68
7b95eaeblc533c06f0d97023d92a70825837b59ba6cb7d4e56b0a87c203862ae
8f315ba5925e8edefa679369a2202766151f16a965f9f81ece76cc070b55869e
4db9784cf05c830b3242c8312' }
}
[3] {
    SEQUENCE {
        SEQUENCE {
            # keyUsage
            OBJECT_IDENTIFIER { 2.5.29.15 }
            BOOLEAN { TRUE }
            OCTET_STRING {
                BIT_STRING { b'1000011' }
            }
        }
        SEQUENCE {
            # basicConstraints
            OBJECT_IDENTIFIER { 2.5.29.19 }
            BOOLEAN { TRUE }
            OCTET_STRING {
                SEQUENCE {
                    BOOLEAN { TRUE }
                }
            }
        }
        SEQUENCE {
            # subjectKeyIdentifier
            OBJECT_IDENTIFIER { 2.5.29.14 }
            OCTET_STRING {
                OCTET_STRING { '329a07b1fabb48f52a309f11a1898f848e23
22ff' }
            }
        }
    }
}
SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.17 }
    BIT_STRING { '00' '67a8951fc308e12f6867611fdc254bf4bcb514f7f5f
2fdeb72fa8e1a030061677b84cd275597d83154195966b141670cb0e88113460
d978a1a7a3895c11ca41995775c09d64ddeb47bc87c4e8bf1c9327fc4afd5c37
86553e17d629b0f27142765481432b5e7ccd0ba61e51cad3dd8f95938c235ebe
ceeaf8b16ae3366f300c5358ec7be9eb23a1eala3da58686704f0483f968a6e4
b1f89670a0134b36a18d6c727dc9b027b12794793a48c7ab66edf57ac1811391
4c00d0a11b65a652f47771337bf743666fca95bcbd39121ae0750bec55ad5a8c
bce98e538ae523947d6929976330fca3fc95c01d1403b49e5cba81812f43650d
d01310934279ecd07ccab34c2ca30a7d3dd5092e1630e1423cc9fac43a1b4db0
e3d970f0aa66d404ae87b04b4cf72ecfb67eacba4d8cd8e65baeeb47afal1cc2
b8ef8992288667b8edef54a9e2767b632e1498735b28c6f60f08b5969e5e26dd
7ca396b9e5cc3e12ale73623602328d64a08ef4a29af35711cc870d26373bb1b
9eb2effe12973544c44a7e2cdf203244f53b37a6d523237d89f06f6f5534ed63
113c8f00eff7fdcd509a2d8c7cef29bd3fb186a4c8c362b3d442939a29076ee3
2716b8fae5100d81a07215cdb1c79bddfbdc14f52e37318d1e526db84d160fb8
dalc06dbcel5955cdc2d6fd78a2a5a58df239ce366c6d90b32e8bd47fc1fd130
9e86294c0c3b51ce77e6dfb6f6722e68f4c3ff2eb4c346931506e743bb021998
b80f43f6e3d3c9fe54777c0f65800e947f9043290e14b01b63f8e26c30138094
2866c74b4a902ce491c0c950544cf0c6938eacb32eb30266ce82c4d0a36c511e
a8ff7c409549a3a8264ca983d8c6d5e035f244243a775758aac992b58844b711
0d3f87c9bba19dd8a8d2ab1294e0555ec4995a548dc56cce35a05dc48aca7555
b1641dde3d197fcd35d12f09aaf3e6a72775cd18249a21e70edac6710db6a21
elc0561192dd0119133640cfff20f3187978516bfd6cbe66ce1071b1246f4ba9
37df901b3ed35069eebdfbf65459fb9b777ae9298a7a49ac24f4020795de5dee

```

The following is a self-signed certificate for the ML-DSA-65 public key in the previous section. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the certificates are the same.

MIIVjTCCCCIqgAwIBAgIUfZ/+byL9XMqSuk32/V4o0N44804wCwYJYIZIAWUDBAMS  
MCiXDTALBgNVBAoTBElfVEYxETAPBgNVBAMTCExBTVBTIFdHMB4XDTIwMDIwMzA0  
MzIxMFoXDTQwMDEyOTA0MzIxMFowIjENMAsGA1UEChMESUVURjERMA8GA1UEAxMi  
TEFNUFMcgV0cwggEYMasGCWCGSFAfLAwQDEgOCB6EASG9kZkZlZm93biwrZSC0RiK  
X2JZSf2PWKvH5pa9TcfQWzjb5su3wHmZ0/YG+HqiTaIzmiqLVHFfY+LvG606J7mfS  
wDIJVNvYEsRhip/xlurwOSi9UVEfijYjYR3NsfeJzDVL45UEHEXyJEIzG3Eb9VoAc/

xMNQwr5XK6804uL7Fsz+oIAo2ZrEmuu3WTFdzHec2rYv/zzqi6IjPR5W+8XFoecm  
3mP63SrwFrEZf3+j2XGi2Sdxc/zlW2d0WvC3whlZfb65Pmoy80HEmlqL6egLCi0f  
KqRRVdbIrH2fK6wA7j994UQcZSXOfn/8JAj6vRRBNKoSkWQbulGcaRNwo0nmHul  
XfaenoVh9hqApyaZUDhl/tm37nKo4XoZxAgUT0spr+9wMcOm2FcWELQsn0ISRaiP  
GX4WgSsDEVm2W5aH5bPpNMUiWumKebpz0rOZ1zUQ7/rRnl04RQ8LqPzhAS/ZjSYK  
dKqqE/riSaAGscNPW6C4gvJjeCIvs28ig8JD8P/rXxu0FKCnDVXj1ApWtsvIiuHw  
O3sogtmN7qKOFFYd7f2OrxzvLtLKiWUPIWT0bR6g0MKkPg3aYKtv09u0XW2dCJX  
hZvyLzpBfs8fnYkxel5TnVh68WueExPgRRT/pkuos/8rgyH4gRyz+wIsj2ROcKS4  
Ci+/7mBKu3N5CR6o5sXHTfwCg2ZrQMB5OHACggShNr9dqVaOt5jTSQOL2wwR4DRF  
54R8tQacdc8orGAcD5nZWCEN28siblGv758d5HsHOHPW0/10Vr7eCFCC50opiyZU  
j0swkxVfNmyPpgHGr4WN+jLAhJGyopiH+QM1lJpdbtqmeYgqOpXWv22XCiIfS509  
jL84SvgarJXisyLOBHiayDcnpdweVZ+Wr0HYoFNRb+7uvFJ0brarKBngkQhxDYNf  
AR+mMGWHKtM0lc3/srIxBQfPL8mTrjf9qX9PMJza8PZ+2Z2QIVV2CDhJ+VOyRtf+  
2z/bZ2eYUKWtQE5kFH+3z09q7d0Fr7S4NJaNH+iAFJYNz12UIjzSbhKkeNaeX75p  
cDELMiWghFAYz8eyq0MKE6axrHuWLMY7PZEawvEQaGE/vgKb/c4Cz1zTiVDtcsG5  
RO37x1YVr4f4ZMBR88VUVsVBKGOkDABr2rVivf8FcbjTw5F7vTAIgLuL6Zgjm5X6  
kbFWQW1POYS6280wmD7TWStNnvfUI2/QD1DZiqU6I1rEFycg932WFyZymAz+j/el  
pwJ4PtWroxsiWQFaES/H9GipwvlGQDkALTdvZ4tMt5i8EWIwv3qafBi6A7elj9B1  
FdMRUEntYUvnoH50QwB1DfHSxYdTOJBZ6vw9eFzN0xwHZIvtwDpc04rUbQZNWcE9  
VzdHKfxOKVNi4qUZEgRTBCi8FSKvoo/1/hZV4wTKW8jCetDgxqOd1N8olWwUs4zJ  
NoLO/kArvV6C0pxGtKTrXTe0j8Vo3+DMbo4Wuuof5RNVkPGSL0c+g2ewIW27gVaw  
ud5Vkt8IA5xCNRxZ5Vfdla+OCJoV5iXo9t7mOThsRkl9eiYyiHdN5Ygn3pYptBtE  
JBQf14+4MxII797DxuDeObxXBj89zWxHA3PAiJHqKcvHzG1kg7iIkIOs6GqntRsc  
LP5uKtGNl842+8VupC+ul+anrBFIZeEMNm3x67HnsRqQmFBP1Zdb3x9J3HAAK2PB  
c5qdJj+6lAc/ap9sK4r0tMMyoQOgz/pd7rLQYso8IV/TYAjr58UWT0pEJO901Ige  
1m9GSHcycyCASeVR4ZHtOpxlifAhgJMyjVKQfChezjxmzd0rSCVyNpTsGniHHauLS  
AH4WcZ7UAIDTNPfaUunlpZkeOcrwg6lbgz8CrRCgjBptDyYMAHKFvUovR3A6Wu9G  
UofSU7GKwiUUMWIQ/1ZoFLEPh6KTlvGZ08OVmZDQwSaLT1DV+fzvU/I3vQwouAGC  
1mWXQfFPEL+7IbuhKrYgqiOW9WwGhrTqkBeZaiQhay/orXbEqRSO75qGo2Naaqd7  
wdz7b7pZp339qbdTDcDKhkji2XNzjgG6uPCLSQXoSqRkG9YCQqZdSamXy8jHys1  
4V6y+gTsvZTVp3q68eDhYQEKmQCH9bRuqYiyvAUS/ad6kj2t1sRcUwHQLINnMmW1  
qy4Q9LpSD2u6lWSlw9Xie9sID30g4TKWoxgZVMOCzJyUPr4X3lwfeq4Kj+EmxHdY  
W1lNZiONaitq9ejNmB5pqs1tTz/SXthvIh5Lk/ZfWSmWdTniS5IldQwwcHVQtYU2  
0QmnExxaW75KVxVWfBJTSux2YHYe67n64okcd0WJuA5WatVX3e9zZxlrcifqmHDv  
Cd3+x51lrkxmmh5tSBddr96ulrPM6+1nRf8VOaDg9a+WgjpTM2lPc3gCLspS4WCvR  
Ms3MSZwf28IeUniyGmitAlLHnwOk072ExM39xsUpAF4efNmjSacWijVWm6XeqBiW  
jVqRRmv5k4gv2JBcZivxOgcKN137UaOIoYtSv+96GvIT0dbkBXzDOKqvBGga026  
yQHsF82XKPy1TgTlIppOg+T55xGyllabco9KMPQRri9E/YlUFndmxhfeFnEcZak  
6BshBLxGCgUeAvLoRE+jQjBAMA4GA1UdDWEB/wQEAWIBhjAPBgNVHRMBAf8EBTAD  
AQH/MB0GA1UdDgQWBQBQbWBPjzTNGFJyMnrzyOwpOWpAO6jALBglghkgBZQMEAxID  
ggzuABGBaGipDGaTS9ux0ZxTpqXcMFNF9tzIZpskKERpMQ6aV8erHwK1+knGM75H  
XVSS2dfuo5FCaBmpJpql1PQ01CtN/LulqD3M010+evbv3WYJch605zkUALRH5Xg9  
NKps3fGNrf+wYuCjyJn+D/Y75gWpM25S7jXrsu4vu2TNqlzkyzYehJx6zu3B70QJ  
0vfBCLthjdBepjQ33aA5bAgJoIMDd3UUJwtdDeYP+Wof6qRq3CaYeigq/hfBb5sY  
m6MS61y8ICDjHve05b2iguECEkeZGXfxSF0w/tIgyhPoRx6PvIuyuVI14a43ttSP  
zATqALqoA6nUifcgr+RpWMeNQBMtJlC6EnMXxB+H0wq/ZfVmx7ixgTgOm8kIzcHv  
rO6yKkbyrd4hOXsYN7eabJvuZIpFTPyxfG8kwBUl/8Vrp5hl8z9F1fJU3J8bOUha  
XmTrHU+gM8oNvRnUHYufcLpJkhiufVWvuXtHsmyvZm9N6nkOCDCkJwUop91d0Pde  
2dBHOKcb2L1lWfKy4N43nt9ntldr4s0LieIb1XDFM+eJmMpv6/mb1no7W9koXf+j  
zIrbeY9nMGvQW+opV2XA8HEYyJ2iaFrAn9bcyO/CFCSyPRchJ7s06FfSFISEw6ak  
D3hTCMqSaPYk4THepKBi73/PdKcyVXEZLXFTTlWpV+PacRE4rgPlfpWe+6lOtsZW  
8AG+FqzLE1Ag87Hj5W1xmTPC0R/47lnsQ+HVWEfMGttlkCuWqfA9OkQNYK5ogLkK  
f1KBYF6Ie5Ay2vw6cKZOLHSmAynwskgqzuPOGAqEUdbomnSbulLH/Xut8Yfr0gNH  
5q2vza61r7Hw6NpCmiH3SJ3+9ST1wDS1KS9HN6gPh8q2Vps67Ezg8BnEsJ2w2Qt1  
WfFSXlNtwGZSLZVcZbk6IRsvg5E19egM7Uozmc621rdZEou56n24XyWDP3oVJrC  
y9/m7mMPesIo5+Sa0oZyG9QYf8mjgckUbs8+z1xFX4s+aJB3bk+ACbJBS2EnJUjM  
Pi2vvQ60nU+euOLxRBBizMkShiWUoAsM/1Gk7OM2WU0mdNPSrWVNih4F0LLsxhB1  
DBa/7+Kk9X9XqvMaTP+RJU2Z6r0Xhz/0QODSH1aefm2AYCgmV/fUIj8SQsMFxnrb  
ocarCvc0BbJLMPRqm71SPsVzZCqHwME+aLDM1TE6Mqj4uR8feilTgK8mclcUgQLQ  
CsJAM/xT2B3RGVUSx4W21q0FYPy4L9NCYKMFog8+3ChmCg5u6XYKncShltyoEE8  
XVDgEKgxONy5huCYp6Do087KelAGg6Br6WTmDGwnXOIzyQNMEJlaOZaCCKUqitfu  
d+DvAD3+bzk6WTwsj7OMUEeqo5NBUXMR/eWTJRBMVT97f+6SnGld+UBliVi6V/Sx  
OeTWQMO91jKd9lMar8uT/WyyvByUCevHzEAe5YiLMezPS8hw7lu4XRhe+3uD5JsX  
854zVKorraOhlt0sZHLxdNO+656htKo4d05ObGbbp1tWmvWw5VEcX233yqSnN0vj  
+/0191UfS7YOYrCQhtbds+gLlL8ZhpBhdcZd/HLWfuShBdvjwRRmNg1G51KF9G1x  
qAxLr9ZiUoOPKDG9IWD3RRDSuXCBCJCPh1FQ4JVZDgxc2vnraC9ikS7iBdnrcFbM

ASjTvoHNuo5j42aqca8dStxXW4WX9gNd1Ld+ItLA2GaBilEK+mf+f+37xC46xZ/B  
g/kWxT9HYHF5SwxZ7zszZLSKykJd0ziUIdeYMGZ4Yo6v08SU51/2ZSzAxQW4TZ6  
j88YJBsuX8ariqiCKOTF+lHavSK7RjsaN+McvJ0KR6RZw9iBe09najevLYT1HxZP  
KfvVQVWfyhmevOoyo3ZhQP07zORuoXqXOidypQWpY2RS+g7WU+HaFyeFzZAbYFEL  
M5Eibhl6apEtPOXglDKWTiLNdU6ws0T5ymHNgrAZLtq308RhQkTCFR7/yYnlbcMh  
9MApe0Z8/aNFEU3jbmTFBRZGYX7tfqJMHgYAaVW6I2u27Ix/bcsLDN+KlhwK1QmH  
IzpxaAAeSh6fOq7DDcmlahEuxMZx/mV7SA8a8LQvYMk0KTeuexHw6B+hSipLUREK  
bMIYSwYS2qMJLkI+TFP7nY4KvPGaKiIIBFDHMTKRH9jS2B+rUiVaDqCMZW7rZ8De  
EGjGYTb0dnrT0ItmVRypQyi36PyUybAr39Ry7XDDQOJwdXOhq/qrL8IMQOhXgGAV  
WD3VGVCJAaQHHgEM8nVENxtuDl62S71zn03EKo82x3F7MGnYfDaHfShb1UCRxIC2  
SPraAn8iH3lsmTl3CD+5HdEBv3xzeY+d/TKL2z1395SOMQNNEwWnJ2tyYwkueRdc  
40lEomIp9vm2gjZiV6nAnqaac87vdzOjGx2u0hLWfR+77tfl2P9q9BAd28yCTAie  
i+OcgjBG0ooisI9qxAXRFmkgnJtEsOE0Fk37az3MBPOo9jWiPlKfGKn/n8/YcAHk  
f5z30IiwK/BenYLJPPffWCdXW3OxXOEcmPzKmt++iOHjpAeNiGJU8OBvjHn8oGBx  
ONb+XmvgNuzOkS6XtcPjt5bzbQBFFXnxiqbW5F9qPfgg28I397cQDI4ysGw460+e  
hf7lSqfCFUhKENkPcUF2eSBYni3VLLmdw5WscUk3Ey4kmiouvLk5opVdfJruyR  
lbuZMTqThXRZMqdxicwEonZZaGzWBFm4MFFRm3oXJ9Nap+1QgIM6uqHVSbW27rP  
7ph5iP93E9L4lr78xUXPlbEq8sB2u/5lUVS+jIu01RjklU+hIBLML6uOmNTHX8RU  
AjyQas+bOQ3rhvik2bPaybLzWEhYuDpBaiOyn7aWtZHD5hRmZrobo3WcVBnnWv+p  
bjn3bKluMhEtnXI40tOP5TVAGUKP0k2eab5PRhHRvdzg7Zn4DZctA37w+pxwr/TC  
hXAa2eyUnxhxrXv8Hu9FrF8omCRyyW8s4Hmc+WVgl6VXQl1bE0WKK1CtRUKQaiNCB  
Ha6UYRczREGIFYwkY1RMAoQwwSuqeJG3yaPT7ezYSDqEZBAVr6j3RzgNsf0MMk/q  
VDPOA6g/D99DIB6D9ghUFSgai/1Rvo5eaVs7B9X7c0+qK8H0zusYGDFd5fr9b+7W  
9j0Zo54bGu4uAW+7vh7pq8jqOG+L3bMkth8b/7ZsLfkkYct1qP2VfOL8qWGWzOFL  
x6k9anNFGd5Ip52e5KvRENCHSKuHp7zrzK/WyVzU81ZLJYHCv4P3RHxStQHMDaQn  
qxtPEXgX9ORWF2aw8mf9XbXarHrkHOkYhwi+tF7dLxVDPmREJKmly/jqfSaJPlap  
0es4QSdF5CEBha7oixy00ejqGx5z3HoG6maIAOGUTb/aTQpPR8OmCzccP6rqERwS  
6Sl+TznKi6nbbrjRcyDO/9TnM8G1Aj3T0fiU9h2hXJQnD3vuRwI5H8TkrDK4804C  
MmZKH/pnAWl9UmOl/066Pz4g0XEX/jg8wPKHvnMyd6QbSud5Y1swOqcnperhhkVN  
+mJqTkSujjFr7EMdkUSg1SK0BeTVS9lSb6iu7bLa2rOha9l/zPIlFp7WiHqANnOW  
xgcl3QJHVkvxqiJDirShYlS2bcn8xYL6e1PNxfJCqxEfDJHmkQwYDiqRZpkumJ2Z  
5+uYPctX6+6bpIrmLBQZfXR/YgFLlF5t5rtHadL3DCjOWyvT0tOhvQfaeOoJgSa  
rYrm5GzvClE0SF1PPsn/qsFY0s8fpjpVOWuU+E3qi59V6LVZB4NEyn8x8qTsdyeZ  
+Z+d7LbnsPirvSFU+r/ZUCTP8Rzd2ejH8akGoUepeXgqUXHdqI86jvgoTds8vHUG  
7E3OGjBH4my94Vanx608HIEhtY6zq2Xl8IkRvwUhO9dLIUZqYNAGC5n/8NQRxRqi  
iY0RxJ9UObtef5YlNsNN0XmL4tXvJ9esMNTMFR5bHLlFW5dpfHd2TCzAZKxRPeGr  
uKQl4KFmXfvcmw18tV7YXNTitPtBb+5osiJIX8GBG9leipxNytxK/qoVqvffjytS  
f4Bi0XC/Ile4xQ46UwTvGQKLttrHYeg3vG+gX5raRK2Ny6IXDJj0scYE79q83TAc  
uWXH6mJ0D04EdB/ut+2n5xL5VDde/rXlznbtCYTwxa4BbJmYjwQCikVzDeknXdMj  
xsV0Euw3Okm3CIQp7biPo7l08y5keJl16HEpx7sWT37mNOoj4AFdm79wzEJQhl6p  
KOo4BpfjletTFQAcU6E3weyVD9ROi7WtSBH4EFhFOfgfgalCHD8DHbwDdsA+dhIj  
9mORCp7dEUPjt5Qi5mimlqQwYFFCHI+ap6VYsrhpzWr3gPi8EENRsbTUEWwezM/n  
+BH4UnmFmQY7SGZyeHuDVfNzdNIAAAAAAAAAAAAAAAAAAAAAAAAAAYNDxMc  
IA==

-----END CERTIFICATE-----

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER { 2 }
    }
    INTEGER { '159ffe6f22fd5cc42c524df6fd5e28d0de38f34e' }
    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 { 2.16.840.1.101.3.4.3.18 }
    }
    BIT_STRING { '00' '48683d91978e31eb3dddb8b0473482d2b88a5f6
25949fd8f58a561e696bd4c27d05b38dbb2edf01e664efd81be1ea893688ce68
aa2d51c5958f8bbbc6eb4e89ee67d2c0320954d57212cac7229ff1d6eaf03928b
d51511f8d88d847736c7de2730d5978e5410713160978867711bf5539a0bfc4c
350c2be572baf0ee2e2fb16ccfea08028d99ac49aebb75937ddce111cdab62ff
f3cea8ba2233d1e56fbc5c5a1e726de63fadd2af016b119177fa3d971a2d9277
173fce55b67745af0b7c21d597dbeb93e6a32f341c49a5a8be9e825088d1f2aa
45155d6c8ae15367e4eb003b8fdf7851071949739f9fff09023eaf45104d2a84
a45906eed4671a44dc28d27987bb55df69e9e8561f61a80a72699503865fed9b
7ee72a8e17a19c408144f4b29afef7031c3a6d8571610b42c9f421245a88f197
e16812b031159b65b9687e5b3e934c5225ae98a79ba73d2b399d73510effad19
e53b8450f0ba8fce1012fd98d260a74aaaa13fae249a006b1c34f5ba0b882f26
378222fb36f2283c243f0ffeb5f1bb414a0a70d55e3d40a56b6cbc88aelf03b7
b2882d98deea28e145c9dedfd8eaf1cef2ed94a8b050f8964f46d1ea0d0c2a43
e0dda6182adbf4f6ed175b6742257859bf22f3a417ecf1f9d89317b5e539d587
af16b9e1313e04514ffa64ba8b3fff2b8321f8811cb3fb022c8f644e70a4b80a2
fbfee604abb7379091ea8e6c5c74dfc0283666b40c0793870028204a136bf5da
9568eb726d349038bdb0c11e03445e7847cb5069c75cf28ac601c7799d958210
ddbcb22951afef9f1de47b073873d643f97456bede085082e74a298b2cd8f4
b3093155f366c8fa601c6af858dfa32c08491b2a29887f90335949a5d6edaa67
9882a3a95d6bf6d970a221f4b9d3d8cbf384af81aac95e2b3294e04789ac8372
7a5dc04559f96af41d8a053516feeeebc52746eb6ab2819e09108710d835f011
fa63065872ad334d5cdfffb2b2310507e92fc993ae317da97f4f309cdaf0f67ed
99d90215576083849f953b246d7fedb3fdb67679850a5ad404e64147fb7cf4f6
aeddd05afb4b834968d1fe88014960dce5d942236526e12a478d69e5fbe69703
10b308c06845018cfc7b2ab430a13a6b1ac7bb02cccbb3d911ac2f11068613fb
e029bfdce02cf5cd38950ed72c83944edfbc75615af87f864c051f3c55456c54
12863a40c06d1dab562bdf0571b8d3c3917bbd300880bba5e998239b95fa91b
7d6416d4f398b3adbcd30983ed3592b4d9ef7d4236fd00f50d98aa53a235ac41
72720f77d96172672980cfe8ff7a5a702783edc2ba31b2259015a112fc7f468a
9c2f9464039002d30ef678b4cb798bc116216bf7a9a7c18ba03b7b58fd07515d
3115049d3614be7a07e744300750df1d2c58753389059eafc3d785ccdd31c076
48bedc03a5c3b8ad46d064d59c13d57374729fc4e295362e2a5191204530428b
c1522afa28ff5fe1655e304ca5bc8c27ad0e0c6a39dd4df28956c14b38cc9368
2cefe402bbd5e82d29c464e44eb5d37b48fc568dfe0cc6e8e16baea05e513559
0f19294e73e8367b0216dbb815030b9de55913f08039c42351c59e5515dd5af8
e089a15e625e8f6dee639386c46497d7a263288774de581a7de9629b41b44241

```

```

41f978fb8331208efdec3c6e0de39bc57063f3dcd6c470373c08891ea29cbc7c
c6d6483b8889083ace86aa7b51b1c2cfe6e2ad18d97ce36fbc56ea42fae97e6a
7ac114864478c366df1ebb1e7b11a9098504fd5975bdf1f49dc70002b63c1739
a9d263fbad4073f6a9f6c2b8af4b4c332a103a0cffa5deeb2d062ca3c215fd36
0026be7c5164f4a4424ef74948804d66f46487732c8202c795478647b4ea71d6
27c086024cca354a41f0877b38f19b3774ad2095c8da53b069e21c76ae2d2007
e16719ed40080d334f7da52e9f5a5990439caf083a95b833f02ad10a08cla6d0
f260c007285bd4a2f47703a5aef465287d253b18ac22514316210ff566814b10
f87a293d6f199d3c3959990d0c1268b4f50d5f9fcefbbf237bd0c28b80182d66
59741f14f10fbfbb21bba12ab620aa2396f56c0686b4ea9017990224216b2fe8a
d76c4a9148eef9a86a3635a6aa77bc1dcfb6fba59a77dfa9b7530dc0ca8648c
8d973738e01bab8f08b4905e84aa4641bd602410cd97520265f2f231f2b35e15
eb2fa04d2bd94d5a77abaf1e0e161010a990087f5b46ea988b2bc0512fda0fa9
23dadd6c45c5301d09483673265b5ab2e10f4ba520f6bbad564a5c3d5e27bdb0
80f7d20e13296a3181954c39c649c943ebe17df5c1f7aae0a8fe126c477585a5
d4d648a0d008b6af5e8cd31be69a9296d4f3fd25ed86f221e4b93f65f5929967
533624b9235750c30707550b58536d109a7131c5a5bbe4a5715567c12534aec7
660761eebb9fae2891c774589b80e566ad557ddef7367196b7227ea9870ef09d
dfec79d6b9319a6879b5205d76bf7aba5acf33afb59d17fc54e68383d6be5a08
e9b66da53dcde008bb294b8582bd132cdcc49959fdbbc21e52721880c8ad0352c
79f03a43bbd84c4cdfdc6c529005e1e7cd9a349a7168a35569ba5dea818968d5
a91466bd6e64e20bf62417198afc4e81c28dd77ed4028232398b52fbde86bc84
f475b9016710ce2aabc11a06b4dbac901ec16cf365ca3f2d53813948a693a0f9
3e79c46ca5d5a6dca3d28ca50ad18bd13fca55059dd9b185f79f9c47196a4e81
b2104bc460a051e02f2e8444f' }
}
[3] {
    SEQUENCE {
        SEQUENCE {
            # keyUsage
            OBJECT_IDENTIFIER { 2.5.29.15 }
            BOOLEAN { TRUE }
            OCTET_STRING {
                BIT_STRING { b'1000011' }
            }
        }
        SEQUENCE {
            # basicConstraints
            OBJECT_IDENTIFIER { 2.5.29.19 }
            BOOLEAN { TRUE }
            OCTET_STRING {
                SEQUENCE {
                    BOOLEAN { TRUE }
                }
            }
        }
        SEQUENCE {
            # subjectKeyIdentifier
            OBJECT_IDENTIFIER { 2.5.29.14 }
            OCTET_STRING {
                OCTET_STRING { '1b0563e3cd3346149c8c9ebcf23b0a4e5a90
0eea' }
            }
        }
    }
}
}
SEQUENCE {
    OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.18 }
}
BIT_STRING { '00' '11816868a90c66934bdbb1d19c53a6a5dc30535ff6d
cc8669b24284ae9310e9a57c7918702b5fa49c633be475d5492d9d7eea391426
819a9269ab594f434942b4dfcbba5a83dccc353be7af6efdd6609721e8ee7391
400b447e5783d34aa6cddf18dadfffb0cae0a3c899fe0ff63be605a9336e52ee3
5ebb2ee2fbb64cdaa5ce4cb361e849c7aceedc1ef4409d2f7c108bb618dd05ea
63437dda0396c0809a08303777514270b4375e60ff9639feaa46adc269812282

```

afe17c16f9b189ba312ea563c2020e31ef7b4e5bda282e1021247991977f1485  
d30fed220ca13e8471e8fbc8bb2b95235e1ae37b6d48fcc04ea00baa803a9d48  
9f720afe46958c78d40131326573a127317c41f87d30abf65f566c7b8b181380  
e9bc908cdclefaceeb24246f2ac3e21397b1837b79a6c9bee648a454cfcb17c6  
f24c01525fffc56ba79865f33f45d5f254dc9f1b39485a5e64eb1d4fa033ca0d5  
6b9d41d8b9f70ba499218ae7d55afb97b47b26caf666f4dea790e0830a427052  
8a7dd5dd0f75ed9d04738a71bd8bd6559f2b2e0de379edf67b6576be2cd0b89e  
21bd570c533e78998ca6febf99bd67a3b5bd9285dfffa3cc8adb798f67306bd05  
bea295765c0f07118c89da2685ac09fd6dcc8efc2142b323d172127bb0ee857d  
2148484c3a6a40f785308ca9268f624e131dea4a062ef7fcf74a7325571192d7  
1534f5c0fbfe3da711138ae03e57e959efba94eb6c656f001be16accb135020f  
3b1e3e56d719933c2d11ff8ee59ec43e1d55847cc1adb75902b96a9f03d3a440  
dc8ae6880b90a7f5281605e887b9032dafc3a70a64e9474a60329f0b2482acee  
3ce180a8451d6e89a749bba52c7fd7badf187d1d20347e6adafcc0ea5afb1f0e  
8da423221f7489dfef524f5c034b5292f4737a80f87cab6569b3aec4ce0f019c  
4b09db0d90b7559f1525e536dc066522cb6557196e4e8846cbe0e44d7d7a033b  
528ce673adb5add644394e7a9f6e17c960cfde8549ac2cbdf6ee630f7ac228e  
7e49ad286721bd4187fc9a3a9c9146d2f3ecf5c455f8b3e6890776e4f8009b24  
14b61272548cc3e2dafbd0eb49d4f9eb8e2f1441062ccc912862594a00b0cff5  
1a4ece336594d2674d3ecad654d8a1e05d0b2ecc610650c16bfefe2a4f57f57a  
af31a4cff91254d99eabd17873fff440e0d21f569e7e6d80602826bfff7d4223f1  
242c305c67adba1c6ab09573405b24b30fad09bbd523ec573642a87c0c13e68b  
0cc95313a32a8f8b91f1f7a295380af2672571480b40b0ac8c033fc53d81dd11  
95512c785b6d6ad0560fcb82fd342c8a31f14e83cfb70a1982839bba5d82a771  
21e5b72a0413c5d50e010a83138dcb986e0983e90e8d3ceca7b500683a06be96  
4e60c6c275ce233c9034c10995a39968208a52a8ad7ee77e0ef003dfe6f393a5  
93c2c8fb38c5047aaa39341531311fde593251066553f7b7fee929c695df9406  
58958ba57f4b139e4d640c3bd96329df6531aafcb93fd6cb2bc1c9409ebc7cc4  
01ee5888b31eccf4bc870ee5bb85d185efb7b83e49b17f39e3354a3abada3a1d  
6dd2c64797174d3beeb9ealb4aa3874ee4e6c66eaa75b569af5b0e5511c5f6df  
7caa4a7374be3fbfd25f6551f4bb60e62b0901ed6ddb3e80b94bf1986906175c  
65dfc72f07ee4a105dbe3c11466360946e65285f46d71a80c4bafd648ba8a0f2  
831bd2160f74510d2b9770108970f875150e095590e0c5cdaf9eb682f62912ee  
205d9eb7056cc0128d3be81cdba8e63e366aa71af1d4adc575b8597f6035dd4b  
77e22d2c0d866818b510afa67fe7fedfbc42e3ac59fc183f916c53f476071794  
b0c59ef3b336592d22b2909774ce250875e60c819e18a3abf4f12539d7fd994b  
3031416e1367a8fcb18241b2e5fcb6ab8aa88228e4c5fa51dabd22bb463b1a37e  
31cbc9d0a47a459c3d88178ef676a37af9584f51f164f29fbd541559fca199eb  
cea32a3766140fd3bcce46ea17a973a2772a505a9636452fa0ed653e1da17278  
5cd901b60510b3391226e1d7a6a912d3ce5e09432964e22cd754eb0b344f9ca6  
1cd82b0192edab7d3c4614244c2151effc989e56dc321f4c0297b467cfda3451  
14de36e64c5051646617eed7ea24c1e06006955ba236bb6ec8c7f6dcb0b0cdf8  
ad61c0ad50987233a7168001e4a1e9f3aaec30dc9b56a112ec4c657fe657b480  
f1af0b42f60c9342937ae7b11f0e81fa14a2a4b51178a6cc2184b0612daa3092  
e423e4c53fb9d8e0abcf19a2a22086c50c731344a1fd8d2d81fab52255a0ea08  
c656eeb67c0de1068c66136f4767ad3d08b66551ca94328b7e8fc94c9b02bdfd  
472ed70dd40e2705753a1abfaab2fc20c40e857806015583dd519570901a4071  
e010cf27544371b6e05a1eb64bbd739f4dc42a8f36c7717b3069d87c36871a5285  
bd54091c480b648fac0027f221f7d6c993977083fb91dd101bf7c73798f9dfd3  
28bdb3d77f7948e31034d1305a7276b7263092e79175ce0ed44a26229f6f9b68  
2366257a9c09ea69a73ceef7733a31b1daed212d67d1fbbbeed7cbd8ff6af4101  
ddbccc824c089e8be39c823046d28a22b08f6ac405d114c920349b44b287b4164  
dfb6b3dcc04f3a8f635a23e529f18a9ff9fcfd87001e47f9cf7d088b02bf05e9  
d82c93c57d609d5d6dcec573840a63f32a6b7efa23878e901e36218953c381be  
38479fca0607138d6fe5e6be036ecce912e97b5c3e3b796f36d00451579f18aa  
6d6e45f6a3df820dbc237f7b7100c8e32b06c38eb4f9e85fee54aa7c215484a1  
0d924a4f7141767920729e2dd52cb99dc395ac714937132e249a2a2ebcb939a2  
955d7c9aeec9195bb99313a9385745932a477189cc04a27659686cd60459b8305  
1519b7a1727d35aa7ed5080833abaa1d5481c11dbbacfee987988ff7713d2fab8  
6befcc545cf95b12af2c076bbfe65baf4be8c8bb4d518e4d54fa12012cc2fab8  
e98d4c75fc454023c906acf9b390deb86f8a4d9b3dac9b2f3584858b83a416a2  
3b29fb696b591dde6146666ba1ba3759c5419e75affa96e39f76ca96e32112d9  
d72383ad38fe5354019428fd24d9e69be4f4611d1bddce0ed99f80d972d037ef  
0fa9c70aff4c285701ad9ec949f186bc6ff07bbd16b17ca26091cb25bcb381e6  
73e595835e955d09756c4d1628ad42b5150a41a88d0811dae946117334441881  
58c2463544c028430c12baa7891b7c9a3d3edecd8483a84641015afa8f747380

The following is a self-signed certificate for the ML-DSA-87 public key in the previous section. The textual encoding [RFC7468] is followed by the so-called "pretty print"; the certificates are the same.

-----BEGIN CERTIFICATE-----  
MIIdMzCCCwqgAwIBAgIUFPZ/+byL9XMqSuk32/V4o0N44804wCwYJYIZIAWUDBAMT  
MCIxDTALBgNVBAoTBElFVEYxETAPBgNVBAMTCExBTVBTIFdHMB4XDTIwMDIwMzA0  
MzIxMFoXDTQwMDEyOTA0MzIxMFowIjENMAsGA1UEChMESUVURjERMA8GA1UEAxMI  
TEFNUFMgV0cwggoyMAsGCWCGSAGFlAwQDEwOCCEAL5K87C8kMGHqgvzPPC9f9mX  
cderQbkCWMw+n6QJMcSSNozI7m6Iatkl2fEM/WlIe/+GPHuqGILSxExZ+Bitynn/E  
ORXN5I2hiW1f4RmxDC3e9iyzB5VadLQjNuUoNt5h2pQfJtFqKaYBBVq+GQCGea9/  
CFNxIPcHk7jgnMdm57e0yaXHqhxg8kRRuh6TPbGj7hbbHlVnyGz0bgwWFCqQq+7E/  
H01bn0gl+dh9/OsWLQ70p/3Ey6F0PNHIE7SWfaFsYHZLZWnfjuW9y//ppOBXSOb9  
8iWvnk7rd3O2Lo+F+bVrVILFVRHe+9iYBqSsNpvtLSVhAPaIppqleCnCYJtxESeke  
I8VQbmQjYe9aMTcS95vEsxhoYcqFpLqxfn+UPRuKMzqjrznzha0QNYBj54E2vVyXH  
8ak/rRpaJ7Z4lb0kmqgKWhd4grzLit+Jox/lod9DIIUAETWk8KjxuCZPpuvlo0nYrs  
rRoWKZzPL9nHuFus4s7TqhJ2umHueO1+XKW2fN1FipNUAw5qu7q/VqCiMW/snbqD  
tRlC/Tfn8eD5CFXVxmUJshAmXcHlTsRLQ7p8+a7xGLRNgJES5lFmpmUeEWzr5JIp  
pwYsCZMfcavSKT929+/DIVupeAADf1jkcL27tDwbBDnq95xu2TtEqsnp6fvhUYDm  
+ypky+4ozEwP53deXYcPHALlsnPFaEYXZYtJt3nLdTonfQ5x/UJetrswPwzhKdtr  
9wdA8x5jl2tQxzEul5fXjFsaawkpfo0fMkW4Kq/XDtnXNMLgeP6ELk0ROBzllcczp  
iyjaUduQVrxyjFsLEYHi+9OhtMeasaX+/s43Fnr3ct2tF0tMOYLaWlnQ6esXPsYx  
UJEXACEjq172qhKcuFhXJ7k1liihQHXE6cvPx2zFxQob5tkCAE68GBF11WS/At91H  
xz7Zx1sR6dfGn3yt/DKAQqYsUnPEO+HDT4deIGTOp7XJfw0y9ZvV8lOEZTulxPqk  
W+qLiUAoQ+ZFtrkmmivZin2ssDMYj/sGBFD33wgAU+aWmyUeh17OwyZ8WSHa1pq2  
mnXgazelU12VJmsIL08JyTFiszsNn3MHPoqqUhBEN/7Wb47j6rvUXWeyWoEz9JZG  
ilK6/9v62T7vGpgYteQuxyJ4ij2NNSn8d30rpXCAHfrgHsiDAoN8H7ngNVcnZF7h  
BGw/kV9dG6C2tT7awNipUGUY/8g0FVw7T+ba+mzIpcz1PHOghJ2NRPfc9ydU5w4bfff  
tEe7TvSdGnPYXG7ziAJUODokmEGsVGj6HHVzklzG9ZlCpsMqXLAHF8TbUSCDqY4  
PAjzs4TPIzjnicUT9hjmVPsM8m7hBFEeHtf8joev9ig24QkVTLJAFW2/YigxsMZD  
0cVRTvp3qY0puFwt4Fpl+mFe7hZJW9kHN2chFbU+kcXZACjPPxqTlToVPeU7RaHo

nM/2tzZpOSba7+uy13qlrWibkvMWhmad8W0XFcxY96LPty3RpR6S+CWZOnQCK+fp  
62BUZURXCU0Uko8gIV57IirFalGtvsjYvbaYOXmn46IbRLXRUYypfQtRlfUelqJD  
UMiXR+Ht6lG0SOPpFHBUpJ4c8kNs5TYaIjgff8XdZPW954VIwIgSusDviOGrz4k  
B4vQKLFon14UfJ9FLIzrAuxZzJ22OgNXb06v6YI5AjiX2gI2YwpTwN5/Q1oZhpeS  
+rNue55jV2DwkGnmQy5wADWsKgKHn/8KHhvsUiBHGT2U613x79U+6hFEyniUCFL1  
7JcnkEs2bt5PXi0zH61fwoLqLEfpIxQnccPddahzV0h975nl8Y6dntYjwXXQKIjF  
H4LAeoDVRxazw8K9vi6fCpu6rr601Sk2h2QG9cAOjku9Cl7AV5fmIHxatsiPGmiE  
Ib0FoRT0194qwkH6Dovt/0f3Yt3L6qkQBPjThOujXIEFSZStOCbjRLqWBAgQ/Asq  
0d5Iz63gAsYuWkmgcxqzg0S8FjbfFr9gfVaFXlBWhAA8cY5LrZ5aCZl5/N3uscSn  
d2zTejQXyW4YTinvM8DodHW6ZjvgnGCrVi63wPcWX5aam0JBQZjM8b/yosjWiaQU  
7OdmKSdmVonpTb1h667FYVy8GniVxoUayWFDL/ERjUYH0y753HMTUTM75LTQ4w3e  
p4TsQLH5H0G+nBljHcRwpS703BOK82M/1DTXh8Fw13tBffWY4dDd5Qa7cdBwvBfs  
cOOWPNwZzcs2mT9jOwRy5Q0JI6xsZv3x0+ZFnmEH8PX5TQnp289daQ4jIzg4oLrL  
fGONGyZQpDCM0XG2hVem0dpnKm7YWO14wob7VvSrPSFJdSgEXGMmLIpCry+YasU7  
e7i+KOEPA4LXORfu3oa8aOyio2Ut4kOPIguObYy6fCtdgJb8N0vACmOcUGiJrPXzu  
QU9gTR4LpU0R1f5YvM6mrXetLowcqs8yRZAUT7kQAbHvqK0XKLI/uoNltXcSG/n9  
iKLGDCHoIde2rLR6WpleQMrO1ciJuP5t5eGOnS5Yk67+u3quf/GhRiYOLxE0k5Uo  
IToAJaO0x5qryGGyXrxQmkZ0wTKqrLfgFG8U79Ec/K9Mqk93WnFs4yXgpDWk00nX  
ILzxN0UK/EUEb8Gh+DqdMpd3pwhOSq2ucSLolwBZMFKO8f38RKbNyihO3EVWjui  
AaJcvx3LZOfn7gksMUH7VVD+PQ3YLocOV4srRlAIGBE7j2Vpdzxcnc4W2mkK3fcun  
rP/ZX9RFLiOqodN+HaIVHqZY1Ao1lrJ6yfgSncbPBkN3JiSlN09GEjDfRxyiYIfD  
lClcZoffYIKDWTWj+Hy3YrDDsdDdpKZTOWW+8be4KS4lTAFNCQ/thXxEwYOcaUwK  
ZOP62QoR9TRyK27hV08uFJ1V10TeSiCTghRFDHAYnUOfsdKufMkLy2z/7EqjWEH  
+qIplvY3OwfzbTkys72wTBndZOrd5PDxWTDWKHIHc8cnDHlSGVo+XVEwX3BVpjF  
yziYOpr8Qng/qnc6UsnYJgaQvp4xVqpbwVCD6j9pWHaVzW/xcrqD5qbYp9a767vN  
o2cnMZg/ibxYMDw3w/PFXW+sxpfzyyC9XbrblwLlSESSl2JpAf4Vnbk9/Udz2P5z  
ViuEBB/IVtGAJ2KEDrxy15iL3nXLynDTGdMs4MwCU7sq1FVYPuDH9HNS5uZmXFrK  
MqSBxTg5vCWRZ7AT0Eizle65qq7jIGFJp9VQ1n/F/f5Kilw10lELZkN5q49yhVoq  
9Hq84qYyBI6vieXLSojevFol1RA6zOTxz/GKz/B6/h61cWqh5Atje0w6OulXn6h/  
UVvgk8LSnbbWtlyTZh4AY2tZJwTQk8xnFsI0LrGFPUjIXGosiihURix7d+fjvR6s  
W8oo/6oAtdNJ+KVHrYdb1qjCspEMkwEwmj+ROKVpMRH1WzwAnKlHw538gtmOscqk  
qcvoheG+oblW+BiIi+LqQqXQHMyazEhKuzgo0pgo0IwQDAOBgNVHQ8BAf8EBAMC  
AYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUiYhnULV8JNs/wBLmHt5ZdTM3  
N08wCwYJYIZIAWUDBAMTA4ISFAAIEdlWXvx7l0QPi9mBi0Zr5TjbzO2xNkr9J6d4  
3J98fPMtFHVbMPEwhJjZizroPmedfxNYjxX4PYY9TruXu4HDYatYvtuR87PSAHvt  
kxXs9T6wDRbEJDsBw5lsxDAO6W+F6dv2kxmx2hs4ik0JF93wSeygXg0uUgSF8SA  
w677he/ZvPuteNt674Mc2zqOyOAYWM6dWjDJMtKmfDLk2vAlph0BubRHI9MHGzil  
qUj7Ska31jdMX2a/ARE5b/fbWiFtjiJk/AGEqnJqZLR23DBqDolg0vS751YUGBpR  
/33bwU5HCHr3hIO7LwVhJOzxxi+2hBOApsR61lh/81UPnGFNIopvVtNa7n8Za6ri  
vIHEVcf48CsSJSN4mdVPkRx3CbtvPC2BXUhu83TE2iBwmdwfz/P1WefFLlrGCKQw  
E0GYKgp+YoCQipTISdFrNvCYUKgWbTh6aTldpFi2j93iPhIr857jdrXrBQ3R/K+i  
KisjM3U9YKiZKrtiAiCSruWj+bb4HArinzITmfqWnpX4TzgpwoF5B3nxfRzVonee  
bQVNpxZk/JLWQWwybcfZHsTRb6awtP7xvWtGu0auCG0f0DBIW6WPzvQ9TyO3ur4  
IyvLvz0j/L8CjIRvaeq8M+s5R0IGES6yYHikv3YR5gBAT63y4+rmL+/b4M4KMELU  
4sFtIcwhQ8nVxDX9UjZaBr5mqX4AC4AP423FAO14RQVUDWS6qvHUMrVi/9afQtak  
Qp7Z4j86AkDWPObDiSSAa9rJjLlc5kBXmiJtHLHvMK8WGz2tl8S9pYhbqUjs7mMN  
yJBUq1NERt6pDEgWffh8FDUxmZ6Sw2sJst9giOaPfAPOTI7qgKATCyQ9Dj31/VbT  
5vTasPnJLeaf0iK591k/ARkc/YRv+w25A5gR6MpC2N8gMmnDFNf0x7nXwC4o0pqr  
jDNUjLTGnVLzz9kOEhZs9VNrBn+flpQS6fLm4YH1SH3He+NIFhs/H9wdIAwtE6iR  
xDrb5J5FH5IaR6sWUv2ifKUsjFJI4ziifezeYJQJlgcNBnMjUHVH0soWRGZerAq  
ZWwfnzt8n7BD+BGIP+88BftaFwPOVndu5vKbY9R+efPMwoN9VFKSxCtCAk/Y4eiM  
7QwNIQMMCbwo794DMwYWGxat9Jql8JzSMFYH5rusNdtqs63fkm5m8SczmKq3xuW  
D+Gd7ilJA69xJUte2EMhiEty2Z1XBVE944cXeZWwPrwMuuokaa7YOZw/DqObVfcU  
hntKj5cS3pARFNnJU9Nr7lJrtThgT6tETGaQEACyM+QWK0z0B3sJisyfXwz76q9Z  
aX+Z/a6i8AUGBA6GTy8K1aCfawNu5Xdn8iV/qVHhgNP5XX6G3f61RDr8zUY9+Xa3  
OCDrsUnw3zhunja9H5UiFQRQa2tzz7T7WW2B1lR+mQrI3ZsDrNFCh9axwCe2ge4H  
iQx9D6uf6ldqmEHZYmM3ZdUYRZ2TsBBjYhzU2y70M0lCAkMXIPxJUaIbE0lrt0d  
qwmfRr2r4ZuDW+1B0ptXweDrHXQdJf7SHri+n9xK1PH1keemtotpv7ctBzFB6tWe  
MOJIN7tiVaX3V4YZEvfr19L1vSRkFKoVEYDu0BOagJYAdX6rS+hr1WgoI92/yZ4X  
dd8lRTAGiC4nc/A+THYT2BCRYSCVIKjrtDQd1zizj/qj93Hs8GWWyx70vx65cfpU  
6BsXiakzrQ8PZpDVBq/d4Nd6rslm3oLr17S8PlsQIN/flrKNJGhP+08sc4Bfs8Pa  
ZiqnICuEZsxGrfgbvcJwO8jTTblfUORj0U7VQyvDr9bejy4TpfoB3g+JG8s4d8GQ  
DFBSuxqt42E3CYMqPdpzmUyF485u1UzPMYPB++hhYn4zR14Azf+8RWqaOYQu8L3+  
auZWn9SzlaWd19WZGPVnjkd/2pHF5G6Pfu0RU3x2Bw+NbCFzEzw6mDn9WZiag8mA  
90gU236/Vv6PKRqXqegczB/KBJwc3Ebs/gUJfv4yKULcxcquKgYxfIFiYgCgqzVo  
NYp79pKINC3l6Gf4ARGnjsjxKHApKe7RqGafZlPQjevLY3q0KT82x/173Ypw88RV

-----END CERTIFICATE-----

```

SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER { 2 }
    }
    INTEGER { '159ffe6f22fd5cc42c524df6fd5e28d0de38f34e' }
    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 { 2.16.840.1.101.3.4.3.19 }
      }
      BIT_STRING { '00' '9792bcec2f2430686a82fccf3c2f5ff665e771d
7ab41b90258cfa7e90ec97124a73b323b9ba21ab64d767c433f5a521effe18f8
6e46a188952c4467e048b729e7fc4d115e7e48da1896d5fe119b10dcddef62cb
307954074b42336e52836de61da941f8d37ea68ac8106fabe19070679af60085
37120f70793b8ea9cc0e6e7b7b4c9a5c7421c60f24451bale933db1a2eel6c79
559f21b3d1b8305850aa42afbb13f1f4d5b9f4835f9d87dfceb162d0ef4a7fdc
4cba1743cd1c87bb4967da16cc8764b6569df8ee5bdcbbffe9a4e05748e6fdf22
5af9e4eeb7773b62e8f85f9b56b548945551844fbd89806a4ac369bed2d25610
0f688a6ad5e0a709826dc4449e91e23c5506e642361ef5a313712f79bc4b3186
861ca85a4bab17e7f943d1b8a333aa3ae7ce16b440d6018f9e04daf5725c7f1a
93fad1a5a27b67895bd249aa91685de20af32c8b7e268c7f96877d0c85001135
a4f0a8f1b8264fa6ebe5a349d8aead1a16299ccf2fd9c7b85bace2ced3aa127
6ba61ee78ed7e5ca5b67cdd458a9354030e6abbbabf56a0a2316fec9dba83b51
d42fd3167f1e0f90855d5c66509b210265dc1e54ec44b43ba7cf9aef118b44d8
0912ce75166a6651e116cebe49229a7062c09931f71abd2293f76f7efc3215ba
97800037e58e470bdbbb43c1b0439eaf79c54d93b44aac9efe9fbel151874cfb2
a64cbee28cc4c0fe7775e5d870f1c02e5b2e3c5004c995f24c9b779cb753a277

```

d0e71fd425eb6bc2ca56ce129db51f70740f31e63976b50c7312e9797d78c5b1  
ac24a5fa347cc916e0a83f5c3b675cd30b81e3fa10b93444e07397571cce98b2  
8da51db9056bc728c5b0b1181e2fbd387b4c79ab1a5fefece37167af772ddad1  
4eb4c3982da5a59d0e9eb173ec6315091170027a3ab5ef6aa129cb8585727b93  
58a28501d713a72f3f1db31714286f9b6408013af06045d75592fc0b7dd47c73  
ed9c75b11e9d7c69f7cadfc3280a9062c5273c43be1c34f87448864cea7b5c97  
d6d32f59bd5f25384653bb5c4faa45bea8b89402843e645b6b9269e2bd988dda  
cb033328fffb060450f7df080053e6969b251e875ecec32cfc592840d69ab69a7  
5e06b379c535d95266b082f4f09c93162b33b0d9f7307a4eaaa52104437fed66  
f8ee3eabbd45d67b25a8133f496468b52baffdbfad93eef1a9818b5e42ec7227  
88a3d8d3529fc777d2ba570801dfae01ec88302837c1fb9e0355727645ee1046  
c3f915f6ae82dad4fb6b0356a46518fffc834155c3b4fe6dafa6cc8a5ccf53c73  
a0849d8d44f7dcf72754e70elb7dfb447bb4ef49d1a718f6171bbce200950e0c  
e926106b151a3e871d5ce49731bd6650a9b0ca972da1c5f136d44820ea6383c0  
8f3b384cf2338e789c513f618cc5694a6f0cee104511e1ed7c5f23a1ebfd8a0d  
b8424553240156dbf622831b0c643d1c551b6f3f7a98d29b85c2de05a65fa615  
eee16495bd90737672115b53e91c5d90028cf3f1a93953a153de53b44084e9cc  
ff6b736693926daefebbd2d77aa5ad689b92f31686669df16d1715cc58f7a2cfb  
72dd1a51e92f825993a74022be7e9eb6054654457094d14928f20215e7b222ac  
56b51adbec8d8bdb6983979a7e3a21b44b5d1518ca97d0b5195f51ed6a24350c  
89747e1edea51b448e3e9147054ce927873c90db394d86888e07dff177593d6f  
79e152302204aeb03be2386af3e24078bd028b1689f5e147c9f452c8ceb02ec5  
9cc9db63a03576ceeafe98239023897da0236630a53c0de7f435a19869792fab  
36e7b9e635760f09069e6432e700035ac2a02879fff0a1e1bec522047193d94e  
b5df1ef5d3eeal144ca78940852f5ec9727904b366ede4f5e2d331fad5fc282e  
a2c47e923142771c3dd75a87357487def99e5f18e9d9ed623c175d02888c51f8  
2c07a80d54716b3c3c2bdbbe2e9f0a9bbaaebebd4d52936876406f5c00e8e4bbd0  
a5ec05797e6207c5ab6c88f1a688421bd05a114f4d7de2ac241fa0e8bedff47f  
762ddcbeaa91004f8d31e85095c81054994ad3826e344ba96040810fc0b2ad1d  
e48cfade002c62e5a49a0731ab38344bc1636df16bf607d56855e56d684003c7  
18e4bad9e5a099979fcddeeb1c4a7776cd37a3417cb0e184e29ef9bc0e87475b  
a663be09e00ab562eb7c0f7165f969a9b42414198ccf1bfff2a2c8d689a414ece  
7662927665689e94db961ebaec5615cbc1a7895c6851ac961432ff1118d4607d  
32ef9dc732d51333be4b4d0e30dde784eca8be47e741be9c19631dc470a52ef  
4dc13a4f3633fd434d787c170977b417df598e1d0dde506bb71d6f0bc17ec70e  
3d03cdc1965cb36993f633b0472e50d0923ac6c66fdf1d3e6459cc121f0f5f94  
d09e9dbcf5d690e23233838a0bacb7c638d1b2650a4308cd171b6855126d1da6  
72a6ed85a8d78c286fb56f4ab3d21497528045c63262c8a42af2f9802c53b7bb  
8be28e78fe0b5ce45fbb7a1af1a3b28a8d94b7890e3c882e39bc98e9f0ad7602  
5bf0dd2f00298e7141a226b3d7cee414f604d1e0ba54d11d5fe58bcc6a6ad77a  
d2e8c1caacf32459014b7b91001b1efa8ad172a523fb8e365b577121bf9fd88a  
2c60c21e821d7b6acb47a5a995e40caced5c223b8fe6de5e18e9d2e5893aefeb  
b7aae7ff1a146260e2f110e939528213a0025a38ec79aabc861b25ebc509a467  
4c132aaacb7e0146f14efd11cfcaf4caa4f775a716ce325e0a435a4d349d720b  
cf137450afc45046fclal1f83a9d329777a7084e4aadae7122ce97005930528eb  
3c7f7f1129b372887a371155a3ba201a25cbf1dcb64e7cdee092c3141fb5550f  
e3d0dd82e870e578b2b46500818113b8f6569773c677385b69a42b77dcb47acf  
fd95fd4452e23aaald37eld2151ea658d40a3596b27ac9f8129dc6cf0643772  
624b59f4f461230df471ca26087c3942d5c6687df6082835935a3f87cb762b0c  
3b1d0dda4a6533965bef1b7b8292e254c014d090fed857c44c1839c694c0a64e  
3fad90a11f534722b6ee1574f2e149d55d744de4887024e08511431c062750e1  
6c74ab9f3242f2db3fffb12a8d6107faa229d6f6373b07f36d3932b3bdb04c19d  
d64eadd7f93c3c564c358a1c81dcf1c9c31e5b06568f97544c17dc15698c5cb3  
8983a9afc42783faa773a52c9d8260690be9e3156aa5bc1509dea3f69587695c  
d6ff172ba83e6a6d8a7d6bbbebbbcbda3672731983f89bc5831dc37c3f3c5c56fa  
cc697f3cb20bd5dbadbd702e54844ac2f626901fe159db93dfd4773d8fe73562  
b846c1fc856d1802762840ebc72d7988bde75cbca70d319d32ce0cc0253bb2ad  
455723ee0c7f4736ce6e6665c5aca32a481c53839bc259167b013d0423395eeb  
9aaee3206149a7d550b67fc5fdfe4a8a5c35d2510b664379ab8f72855a2af47  
abce2a632048eaf89e5cb4a88debc53a595103acce4f1cff18acff07afe1eb57  
16aa1e40b63134c3a3ae9579fa87f515be093c2d29db6d6b65c93661e00636b5  
92704d093cc6716c2342eb1853d48c85c63ac8a2854462c7b77e7e3bd1eac5bc  
a28ffaa00b5d349f8a547ad875b96a8c2b2910c9301309a3f9138a5693111f55  
b3c009ca947c39dfc82d98eb1caa4a9cbe885f786fa86e55be062222f8ba90a9  
74073326b31212aece0a34a60` }

```

[3] {
  SEQUENCE {
    SEQUENCE {
      # keyUsage
      OBJECT_IDENTIFIER { 2.5.29.15 }
      BOOLEAN { TRUE }
      OCTET_STRING {
        BIT_STRING { b'1000011' }
      }
    }
    SEQUENCE {
      # basicConstraints
      OBJECT_IDENTIFIER { 2.5.29.19 }
      BOOLEAN { TRUE }
      OCTET_STRING {
        SEQUENCE {
          BOOLEAN { TRUE }
        }
      }
    }
    SEQUENCE {
      # subjectKeyIdentifier
      OBJECT_IDENTIFIER { 2.5.29.14 }
      OCTET_STRING {
        OCTET_STRING { '89886750b57c24db3fc012e61ede59753337
374f' }
      }
    }
  }
}

SEQUENCE {
  OBJECT_IDENTIFIER { 2.16.840.1.101.3.4.3.19 }
}

BIT_STRING { '00' '08783d565efc7b97440f8bd9818b466be538dbccedb
136447d27a778dc9f7c7cf32d14755b30f1308498d98b3ace3e679d7f13588f1
5f83d863d4ebb97bb81c3c9ab58bedb91f3b3d200756d9315ecf53eb00d181e0
490ec070e65b310c0a3a5be17a76fda4c66c7686ce22934245f77c127b281783
4b9481217c480c3a07b844fd9bcf52d78db7aef831cdb3a8ec8e01858ce9d5a3
0c932d2a67dd2e4daf035a61d01b9b44723d3071b38a5a948fb4a4037d6374c5
f66bf0117b96ff7db5a216d8c88e4fc0184aa726a64b476dc306a0e8960d2f4b
be65614181a51ff7ddbc14e47087af78483bb2f056124ecf1922fb6841380a6c
47ad6587fff3550f9c614d228a6f56d35aee7f196baae2bc81c455c7f8f02b122
5237899d54f911c7709bb6f3c2d815d486ef374c4da207099dc1fcff3f559e7c
52f5ac60a44301341982a0a7e6280908a94c849d16b36f09850a8166d387a693
d5da458b68fdde23e122bf39ee376b5eb050dd1fcafa22a2b2333753d60a8992
abb62022092aee589f9b0781c0ae29f321399fab03695f84f3829c281790779f
17d1cd5a2779e6d054da71664fc92d6190c30c9b71f647b1345be9ac2d3fbc6f
5ad1aed1ab821b47f40c1216e963f3bd0f53c8edeeaf8232bcbbf3d23fcbf028
c846f684abc33eb3944e20612ceb26078a4bf7611e60040b7adf2e3eae62fefd
be0ce0a3042d4e2c16d21cc2143c9d5c435fd52365a06be66a97e000b800fe36
dc500ed784505547564baaaf1d4311bc8fffd69f42d6a4429ed9e23f3a0240d63
ce6c3892b006bdac98cb95ce640579a28ed1cblef30af161b3dad97c4bda5885
ba948d2ee630dc89054ab5344ad3ea90c481615f87c143531999e92c36b234ad
f6088e68f7c03ce4c8eea80a0130b243d0e3df5fd56d3e6f4dab123c92de69fd
222b9f7593f01191cfd846fffb0db9039811e8ca42d8df203269c314d7f4c7b9d
7c02e28d29a918c336e2654c69d52f3cfd90e12166cf5536b067f9fd69412e9f
2e6e181f5487dc77be348161b3f1fcd1d200c2d13a891c43adbe49e451f921a4
7ab1652fda27ca52c8c5248e338a27decde60940996070d067323507d6f1f4b2
85911997ab02a656c1f9f3b7c9fb043f811883fef3c05fb5a1703ce56776ee6f
29b63d47e79f3ccc2837d545292c42b42024fd8e1e88ced0c0d21030c09bc1fa
3bf780cccc18586c5ab7d26a97c27348c1581f9aeeb0d76daaceb77e49b99bc49
cce62aadf1b960fe19dee294903af71254b5ed84321884b72d99d5705513de38
7177995b03ebc0cbaea2469aed8399c3f0ea39b55f7148674ca8f9712de90111
4d9c953d36bee526bb538604fab444c66901000989be4162b4cf4077b098acc9
f5f0cfbeaaf59697f99fdaea2f00506040e864f2f0ad5a09f6b036ee57767f22

```

57fa951e180d3f95d7e86ddfeb5443afccd463df976b73820d1b149f0df386e9  
e36bd1f95221504506b6b73cfb4fb596d8197547e990ac8dd9b03acd14287d6b  
1c027b681ee07890c7d0fab9fea576a9841d960c9b765d5186116764ec0418d8  
873536cbbd0c3b508090c5c83f12546886c4d25aedd1dab099f46bdabe19b835  
be941d29b57c1e0eb1d741d25fed21eb8be9fdc4ad4f1f591e7a6b68b69bfb72  
d073141ead59e30e24837bb6255a5f757861912f7d1d7d2f5bd246414aa15118  
0eed0139a809600757eab4be86b95682823ddbfc99e1775df25453006882e277  
3f03e4c7613d8171161209520a263aed750775ce28eafe3f771ecf06596cb1ef  
4bf1eb971fa54e81b1789a933ad0f0f6690d506afdde0d77aaec966de82ebd7b  
4bc3e5b1020dfdfd6b28d24684ffbf4f2c73805fb3c3da662aa7202b8466cc46a  
df81bbdc2703bc8d34db95f50e463d14ed5432bc3afd6de8f2e13a5fa01de0f8  
91bcb3877c1900c5052bb1aade3613709832a3dda73994c85e3ce6ed54ccf318  
3c1fbe861627e33475e00cdfbfc456a9a39842ef0bdf6ae6569fd4b395a59dd  
7d59918f5678e40ffda91c5e46e8f7eed11537c76070f8d6c2173133c3a9839f  
d59989a83c980f74814db7ebf56fe8f291a97a9e81ccclfca049c1cdc46ecfe0  
5097efe3229495cc5caae2a06317c81626200a0ab3568358a7bf69288342de5e  
867f80111a78ec8f128702929eed1a8669f6653d08debc637ab4293f36c7f97  
bdd8a70f3c4558e24dfa2afc3ab6c7ec97637d0b6176351f45fb06ca37dade13  
eeb2715ec8f945c6bfd97762586c3b1acba792af955e59348b71b2b594a608c6  
7b9f89228f2c46accb8d0cedfe090b908776f22edc10dfd36647b01776c9a508  
9f5003fadbed280eadc4cb6dca5813fff1153b0c8703b15880d8a7b38f058cc1  
fc5bf5c450e7de8b721c7ad632adbebb02c5864bba9f3a685842c206879bbcb8  
4d00dcb7fe9bbf2069792d38d12ff7180c013406d381d7c51fd06c9be308c50b  
472bc49059d116a92be0690ef14ab43d1c20c76dedf76ffe79e3a346d89b8f38  
43a87d8787c09d59c59f4cddf45c7ab1942fc738c0fe9ced0fc5b5597e328157  
288d305ee13a054558e91184cc688226e3aba1d47459211fc6ddea1a2823d11f  
e21cf97003eb261f115f27fd863d7c19b81a6f120b8460bee9af2176c5eeca7  
75b8558e6e03a96d4d59c54b79abefe72234bf20c28aa16c554533bdf04d8913  
8cc2db43f34e1eff36528e3d30facb2823f3be23e71a08357fc7b01dd1aa35abd  
7e5333557e33d03329c3ac7012e0c699db25505c3ca198a4b270d1b9e61c77  
82d4aefad06bfbdd30bc03163bec99b439840289b2e26ec106dab49fc8054af  
74b8e1160ba4a2f5b992de20ac9153d65b0fd6df5b8c5dfa5e62c5dc174a97dc  
94ebeae4f27f101c2515f1b10021feec182d54502198e6c6c026549883de8531  
4e01f2c6719724fd87dba13cb6820c54645b2b8ad8ce2d14ecf38385380fd77e  
d1cf987af0ab39b0ab4806d55890cc99d9e1528351a33edd1a438113d2af1c6a  
4ae0c19a87d2cd38136cf32df268b4e2e71da897fe2felc3bcdbe87b4d4d2cf9  
122aec6dea01b6c6ece4a45e5d63fa0e55beb9612d3289ed1d5515eff83f51216  
62a4e1ea69c577a58f9a2d4d86f4bd5aca6db61c4b29f2f5278e0db04b4110f2  
662b5368f21aa957c822f0a0303ec9f56fe9030f302d16b2c4bf621ed91ab393  
645b8f9c7907c40ece541c8a0ff34cefc8b13bf187b270af0fe4346694be4b1a  
46bf806df744faa488d9d7112e9c541e27316b9bbe7ef0d15afe06fe821e4b5f  
140124ee215da5ce9a11d865bf83017cdfab6b4014e31f9da293078ddf7c5125  
4e2da95f19a508d01dc8f846b1652d4de57a7251e6393240ed14303e395fb188  
079345e0fb853f876cc1edb4290e2684cc35311e8602c71a57bd3a6c9a804591  
727be34f6fab723f48a196febc6f0f9b34f344fd9706790a3e63d1a989cbcdf  
30f8eb71fcb024635adec568fe9d39a194c8cd2fbbf6a131390dc311e9c5381b  
5542466b3c60a8eeb621e6e653b8b52fd5dd3f8d0f3fe3f0ea948b0c7862de25  
e064c2947359fa25bdc8a35e5ce33677646d0874150b72522ec6241d19d06db0  
380cd0ea8be776e7cf7ca0d1bd59c5584fece0db84d1a767a162029d682e4063  
7d7c378c847ae185e2d6dffe4e15d55bafd0d35fc8d7ff56fe5fa7cbc2ee1833  
7184dc62f5e50dec5cda90629d6c81a9fedab2579019cd49dd76bf997f543bc2  
35941a70107925ff095153ec610772c5fd524c80c228d80e781e864e295d20c6  
896f502887b18ed2307e8eeaea56e2649639349652f509528e4b80ea477d7a6a  
453807b26361b1eca6fcec4e06c504166742c12f8a44a359fef2727d34f47201  
f75a7055629b28397e575e4cc9de39adc08f42410b5232f8f2e7b86fdf3e1ebb  
e734b7acba49d308a6151c1352de2e20b1fed060d5e6fb58d6f23b2847dc53b6  
7519b92dba604e448f3990570f09bd65f685545a02462cd24c72f2f7989cbe87  
b0c52da52eea1770aaecf7d568d0b1bf1aed3ca8f58f332299e391b4413b6c6f  
eba11d43262177a2a446ce5afc59c48288781cf9167fe5a1bf42629c6d094c65  
37abdea5f4b4a3a7f1e8a3e8cff1026ddefc29bae39e75249364a953ec52231  
bb5813a80b3af25efca43800a74c4664632f6dc189cc2cd95478b594fc578ea3  
a15840e92822b7166c8611d464af2e8d1baa5bcaf1c1649589a7eb16b889b54e  
0b7ced0ba25a51e34f4d0f152fbe69e1f43682d81a5de05f89628b1b5ef10032  
7e4b4fb3a02385762b4able721da7ff61733c41d7071e819ec44c03311474330  
e97a6c0248d1dd99419feb83980f2422a9e7c9065469c4103d76bdb7b8524c4e  
21914095fe25eea171d88dce27d96f7649a717d9415ba05138b6a26a685fb768

1. The first ML-DSA-PrivateKey example includes the both CHOICE , i.e., both seed and expandedKey are included. The seed and expandedKey values can be checked for inconsistencies.
2. The second ML-DSA-PrivateKey example includes only expandedKey. The public key fails to match the tr hash value in the private

key.

3. The third ML-DSA-PrivateKey example also includes only expandedKey. The private s\_1 and s\_2 vectors imply a t vector whose private low bits do not match the t\_0 vector portion of the private key (its high bits t\_1 are the primary content of the public key).

The second and third examples would not be detected by implementations that do not regenerate the public key from the private key or, when they do, they neglect to check consistency of tr and t\_0.

The following is the first example:

```
-----BEGIN PRIVATE KEY-----
MIIKPgIBADALBgIghkgBZQMEAxEEggoqMIIKJgQgAAECAwQFBgcICQoLDA0ODxAR
EhmUFYRXGBkaGxwdHh8EggoAUQyb/R3XN090iucd1YKBEGqTQS7Y+jV/dLu0Zh7L
GSHTp1/JO4jvDmqbhrVs7BmZm+gQaMhZ1t8RXGCMFQEXDrbAVcIvYlWSSXbYlaX1
TSw4WWxAPM72+XPiKl+MfCuoNjNEcJCniyK7Qc/e2vvLLt7PkhDM5hLkKrCh8T65
3DwUkDGJwoHgsDHALISCEgi jtDDSKEoEByDDRELgQC5EoHEBqSwDjMqSQSQYMiQA
Ii5KlmaLGZAI MyBShkUbCEyTGIQZAG1TgAwQpChQBgogBgwjETLSxEDSEgIENIYj
lQygtkxbSJGMEoQgGQKRGI EKJRACoGlgkCgDxjCTBJARuJAERTLBIEzawpDZiCwY
RiTksAUjsWyKEIwEgXDLpDDYRmLBxhDIyEXBlgweEgrkKGYcJXCcsohigGxiOEWE
gEyjoA0jBw7IRiAklskRgVICHATI UxghCGQsg3QNoAZgE0blmEUEIUaJkCcwIij
GBADAiGSMlGYCDIIoYpAE m4MjKEYGU4iAmTCMBFCFhJjFwiwRo4TigCXSRmKakGAR
uA2LhgBRlnHIRiQIiUEDFUChIm4kNwMAJC7CiIUEMYxawIlCRIlYxgCZMpIbISDL
Am4YGDYxiRBNNIZKGVYOG4IIAwCFCpjFoUBtCVQwmGJGVAisk3DGCokGCKbRmgQ
NUIgNmLbNAWLSmxIEIoByI0hMA6MFCZCJAQLN4xDBilCSIbYGIXIpAQUt jHRNgwi
gykAoklCuAlkiEXIAEGUOExiomjUBi7ZAg3MthFhOGTIMpJRyElSgAHGwDEAIgrB
RGaAtIRQCDASxiikCGBKsGhKxkESyGhSsHGbaAAwIR2ZhGGxRFImBRoYJOUSDAjEK
kWhnlFZRkGiBjLaBnCZMCzIji3akpDBACDasGWCJDKDRIVcxGwAQyKJxhCjBABh
hCSjQBJRIA0YMoBBNirIsCkgRwgaEkTDtpEiKYzYMmbDlhBiJnIbRWXDpmXZwGAU
EAjQxG1JMoXQBg0RJEzjtAABqUUAAM4BCMGBKgEmCNCBDGAGSBiasRILKMAHhNo5b
IiIkBwZUEiLlLoEGYRgpmFEoKNiQgI07AFgUDRIyAtkEUKzHLJgArmG0KEg7YEGKQ
NgwUAXGJBirIjMzSBFhkBkdckiHIEHFkGC7kuABSkiLqChLJEKRJoGZiJFUNg0K
mIG8aY5dr9/gBkPfhWzrn4DSmTPR/Vn0IjddemyttdtkeLCZ4DW7+GKb7Z8S4f
HY7JlsvtetEEMyRAS8/INLbZtBrGWIRQqWxf3YcrxGG51ND0lvdrYH7wnyS0ku6m
N12BMMwLEfKkmoSU747o81liHE+wiM2bPH+rG7eP6rIrB7NRY67odfeBGboLHeSdf
79U3GOWczZiFB5wtZGzNoVpiExABNAYdQC4OJIPvpxR0ULrErVz9y33/zj9KIZJy
+saqdCSssuX3kbavVhZQz7eytus2Aji7uSWgPb4M7FqBoFcPobHX/ jVvHD8oaBt2
TOjtuObFujQUndCztr62etukrM+IwyyLR4WCpFev9qGM+ZP9TCsLbEDu/rVMVS81
dnKlkkYhy/pUgsGU2jglbTD83Wib8laAlKZgXSqLBSyP2hpmU66+mX/2gQR9rCzh
gJSFdfiIGPolnU2yelQMj8YOniHNV8I5ZRKylmRFpDZo+QPVoXMnwTg0eF/c3UCO
PTc59SF1UpXMSpttjYLHENPlqJnHLb/PZMWlqfd+FE+i4GfHfKDH6RF3NUjPY0Jx
I1EJ5l/HxG+zK4clabdl6LU4fMGnnKrNKLNSF5yoq8b68GIspz/Mnni3Z8++arXx/
hzmVaytoZ6vtL0ZtyByyV26jjrxOEmpf0ZLzjkWB+Q9a+Z6QxEcTtpVlsOhnxB9w
cWFzlhZd0z1ZaMw89k3iYgaJdmNIHeUQdz8wwc1621onspo5YlZuruFSorrzz/Ru
yyg3iHNFmRv2SCNuWcziAFTSd8HbtInzNWmeqBeF7HWlhsCpRoR02ZV4im+REFrj
qPVHh3zqURGGSduly29uK6M2vjUp0w8NfyuvzbHIy2hJz3Py9kiZotff4kOgU25D
11b+/IcaVavqBxCUAz9N4c29aBGZO8reC+X9kPWuNE8NY7e3j4YmPcWppZGfXnY9
PNV0pLyhLeifev2WklahcLVYLE6l/cFE6qxmThkD8uTrZ7h75JmUqDmKNVjtJW5N
YS5XSZQz4bFhsdXvpED5F5jwr2NUPpZZDkjuEKXu811114F4wx98g776d6LI/zTY
a06arDBhDhmedQZfHmtlu575XeFZGdP11IVo4UPSCQKzc/AMxlrjNrQw2wNZJ+t
6JDEJq75MS7q5C7gvPpBd3qdmBNQwLFvyCj8ohXcpqc1Lgw12BFNTm5L2JXXle/7
QmhVrMEkSwJznkd+bOqky9uPbIlNr1fw0+NJBeqCJtxVvjngV3rE97E1RqzHFxaH
QQvju+iK/j03mKXQes6be6UWIrYz8+RhZ4jwlK2nPDklHM0+0p2sNlha3BY1+Fob
uXxZug5ze+Lor7aiIiy18xn64MxZ4QBP3pFpKew3YJKoLcJSexuJlKJ8Ky5WjnJ+
skZeuWRgmW/OYRcKyyylrgnWv0A2oyBqe8ujjv5MD20i10q/mxtA+a8IAQ0oqOL
F00uc91QcXXoUdXnQ+ZCCeNIUg1shMyx+2v6smyMLuSFEQ3R17Br1Sgw6lu2gd0S
XMYOX6h8w0Ww9ml1Huth5xm21mYiPLiejt3vPoyWrJNQ7pg4l/0VGBTG+1zaN5fo
paZzqkjiJn+EH7d+G8RVLGHu0gkbplrNqDAIHAIcN076b3CuBam2ngtjQzBPULSU
AqXPTG17rJg2B+fzgPKAgh8vuZLEaXP7/XeNMwNe6QsNuU9gfln7Tt+pqYpwm1gH
Wkqor1xYXy+1md2Ct3tLbznupLFIfQ3NVBkeDW+NVvpPvC+CF/NefkSuzOaBP1Ta
itxMHENeGFxR5cf0Sp43j59iGkdWbtJBCV8uWf4qRgRG8fdbfQ+11qAJEx4v8r4H
2Hsm6eS/CeZlEpe9fnobwS1BBNocZKSL+noqpxcmgAjbcEtZtsBXSJVBsj4OCdt3
```

```
fA/6IfpWRsNBIVR1aD2p/a0U/RH3FCZKDhwF2ZhBLEHEWWQOCr1v0W68/r1lFuIW
YcyqOoJDEup7oFhc0k4aUwDv50HJAWk3ehaPvbP+zLz84DmyVMQjXYJl9gZShi+9
tFV4KJ8aZz/kCdufmWwtLJKHIBuVx/hqbY08Xg4XyWv2pZpZIGeW779l8wQE1MI
2Yt6grThI3sytb+dM3JvqUW79clvJ288BqRZMJSN02vUIo4vPqyM/Wcuy465qS0V
ns+zr0zC2uo3z3LqK57arYABNRm8CV2VxaOqH6lGvYyUrA==
-----END PRIVATE KEY-----
```

The following is the second example:

```
-----BEGIN PRIVATE KEY-----
MIIKGAIBADALBgIghkgBZQMEAxEEggoEBIIKANeytHJUquDbReeTDUqY0sl9jxOX
0Xidr6FwJLMW6b7Joc4Pf3f421ZE3No2a/5HNL2V9DX/mmeE6pUqkHCxpTAQzmgeX
+rtI9SownxGhiY+EjiMi/+Yj7IENS77jNoWFSogmnaMglRIL/P6JoY4w9xFNg6pA
SmRrbJlziYYNElIu4ABuI4SBkYZhmyYNEYZk1KYoiHhEgkAomBRhSKZhTEJioZiI
wjgpUSRICKElwgGxCMRxIBQJFINSgKEAhBBuycBwIrVCLBhDacEmBJEUyhpWQBG
IpMgQQYuQrZMARZJFChMQahRgEYKURZRWgggAiJE3JhJ0TJR4TB108CFkqhREqFk
ADkiCUZiHMcM2Qht0AYmUkCFgEQwkQYsUMgJMMWEGpZtSpqsmQZtpEQyIKdkWjJu
EbVwIJJhJBOOBiUsCkhyYKBR0wgqmSCAWCQgJAdOWRSIEKRkYMBt4LKNGxkJIDQi
wCRBCUNxCiEgYaIBuiJSG4CAmJQAE5NN0zIpIhcKmJJPghRRICchnMAgYqKBSBhp
GoVNg0RpWyBBaxJCyxhGAakNDAlxg7AhWiJKyJIF2ZBpBDBqSwZK0rIBHEBAGUIy
UjJyVKZAWhgQDDISksKAUhJiXIIoC7RsA0KNUxAMFAEO4TZSiIQkkQIKY0YmIAYp
EcIo0CBIARnsojYJWoZiY7Rhi0ZixECCGokJEAJNJLJFIBILJmKfiCiMycBNWUgi
CidwTRkTJBgW0RQgoZJQ4gEQ7KMYDCAoogthKrtjKYp0MaEQgZGiYhRAKmaUmnN
5DgNpAan05RxQrJsGoRhG6MoQrQoCKBxGsUx4KBMATdlJChiFCiQCRBh2UAiGzNg
CQKS0CSBIAQISRHeoyItXiHEfJgIpeZHAZVkcZkKDJRQykBq0rIgwDgBgjCOE7fKI
kYCEFIgpbIREjUNoCQi4gQG2cKFBCgSHMmJGAJy0kApwggS2AYqmZRxm7hoI4Qp
GiKJFEUR3IJEUJZFDESEwLIEmqYFQ4YsRDJuiEQhIKhMmjBw47gtYyAIAyVJA0OM
SKgJyhRyUzROEkMIG6cEWTAi2ZSA4jQigUISnDAqLDQmYQRFJCYoE0YJSjJtESgJ
GLglYigRE0ENQbIRKIRMixISosaIycAwIgYG0hiOhIYwKERSEogx2SBxE8UoQwYO
AzBgZKaEWCZSTIGBhVclYshf+kOs+kkhfysXLXu8FGIOBzGKcaq73wxF6aIG7LFC
P+4V3swXYBMAFJ2SI8lubG4fqQQfx8ZJOKtokF/T3NpQ2HCC59DXHRvJsrrhMhVI8
qP5srSlK340+FbEI/3IdDMh7w906dZAYSw6EVmOpH8nhw8U6YdhnQgsE8JI1V108
ZaBjaPlBKV/QmSQTlG+R9nlkwUJnSnJcNDkUxM7PWMB0vK9FWm1795EeB6ptCTjy
7iuzwajfLdY16ENC/eoB3CSyEa0vwoHPd+WREMerxUvwyG1IC5vidkcdydYDzumM
/as+n8+3A3klYfSepEUPp7M/uRacRLTSX7nEV/SXkc09oD6slglYE8EFEyzNpOY+
SSKM0j2KHzeFbxQtk7kNsJ+Cr4kljGOqUAR6gMA2yTV+ogRvjcy1TwXSlfNCu0F9
P6w6sf0ZyIwp4Uy72S4TY8ZevUUEt1EjKblndJLhssZ6VOfxpV+Ln56gToypjpwXm
KjxeY3N0r7eutt3qYSzeKPAaIC16PONHITJ90/m4mJTQGf1dTXEZ7+Ny07oQTLi7
CYHgdN46/iANqq6tgmxEXyRNv0Ma+rNO+994JHTS/VcRj2RiFJNO2Zy6OWa+jWej
g29vGfxBkQzlfj7jrprnrhNUU63YeY2hOpW+XkdLdSquxYWi5SMgX9loiKssOjNwD
zEr+j2cVfho203+u/58XK5iRNnfFod0IXp7kwiBSwa9YGTEWZz3NO/xfNLhV3MbH
eIVknp5x9D1K6g9Lcsp+2gV4uhPTGmWNLQYKmmB/ae0b5516L7HScj04+b+r4Y+O
ezzakG5Om16ULI6uspYHDr/TZJR6lAzJeL7Wazd0nmldzXvoxJREDiueZs/vuYwL
7fs8QeMlnSzXGX++cgxIqmXrZGXB7mPjVpwq3HREkTcLf3gm/gt3odGdZBAdAyur
gQa0LS73N0flYB/kulDyPt5SHwMagX0VKUpDci6DeHhLbbDPG6norpeDkgG5zpzD
AZxvXCfLmNomFetkIlp8kysw92HniilZodi4PsY0Si9t1H52VwbQC/SnmqSbDup
HYEsjyx5erF5Zwnl0WhWd4KTUp8ChtAVw7U51hlkKjM+nlk9bj9TU51CCOnmozKF
fX9lJSKpKLkX4n4tbtUITff4uv6b7HGeybAJUuOaf9+vb4xWmjgotp2noqfQtPmAa
fHEzCSaywAetgrU5P0e2HLM0ZciAdKwJ/NUWslTDNeLwddA/sy8b8KgrGxuMOrF
HlppCYqilEfyCFtOTkuSZmJpIdLeR4UYzQkM4meuotJ62lf9iLSXbYn7hDzc0mn
bKJnnmgBv6f7AxIW+1BilwS5kjk2ul3ThTERICrfsRmV5ZtzA0z2ftA6uBOGdkjQ
JYKAh+lJqa/Ra5XXLZmx7coleqWTL/t6BwmulanA/wX7Dyu/KECe7XtfWAG+lKzt
AZ4ct4UdOFHxApBnThn/sAizAcSs9kGiuxQhbhlpyr9Ste8idJaw8weZqFXRF/rT
dEpvozUD6nmLUt3X7lQmYJ2/zT8ME7FklSBR9+1KEZcZpxLjinMoQCCB/xNUTVTS
wjev7TsVHEuo6fS964SZowZuJrvGnorwid7HFzHR3FKeqxfvc3RzTA/kdULMg4Nr
3TSgO5vImRRxYGG/uY7G5hw+1EO03K8lJDxkcIa56nAYSnmooLAM7LAKveJJjWnC
M2EBp3LL5PVxUj9RvQWILN8li4ScwUCqH68iQjoShRzg4z/UiXWklZ+lx5BjJQO
gZGrbnQbd7/gLLlpjueVxGbWFWGeZEE4LG6sAYNO6atzzqgLvInceNqRvXm2+C+J
l4XWhwDTk+Z1wiJNa3oa0hMgSVZ5ra7XAWelCGZxOlMQnbe299gTBOzf2Dsxxm7y
SDBRa0p593Mhj2sVgSLXWnqF1AR92FMAKHqhjzeGHKokyh4uax+GsW9pJl7cgZP
DNDrtTIFOA3hGsuQE89+qSa05+qs4HdHuiGI760uQx4SI9Rd0FxnHAPC5FzuZBPs
vnUn6HPkVcTmEKYYOarMC9VtJIPnjymLZqR46y9VjLr8qGvoR7rrAsWyFsJNiP6k
3ySbCeZwogcDq6wksKkavEpWRmAUQroQvs/TCZOIAFHQflagWpN556jmvv7j8i+q
EGOY93BgBuQum+HvidJcJy8RqVCVxYfXE3MihN6dvTxyF7BonihY6w/2lmg=
-----END PRIVATE KEY-----
```

The following is the third example:

```
-----BEGIN PRIVATE KEY-----
MIIKGAIBADALBgIghkgBZQMEAxEEggoEBIIKANeytHJUquDbReeTDUqY0sl9jxOX
0Xidr6FwJLMW6b7Joc4Pf3f421ZE3No2a/5HNL2V9DX/mmE6pUqkHCxpTAQymgex
+rtI9SownxGhiY+EjiMi/+Yj7IENs77jNoWFSogmnaMglRIL/P6JoY4w9xFNg6pA
SmRrbJlziYYNELIu4ABuI4SBkYZhmyYNEYZk1KYoiHhEgkAomBRhSKZhTEJIoZII
wjgpUSRICKElwgxCMRxiBQJFINsGKEAhBBuycBwIrVCLBhDacEmBJEUyhpWQBG
IpMgQQYuQrZMARZJFChMQahRgEYKURZRWgggAiJE3JhJ0TJR4TB108CFkqhREqFk
ADkiCUZiHMcM2Qht0AYmUkCFgEQwkQYsUMgJMWEGpZtSpqsmQZtpEQyIKdkWjJu
EbVwIJJhJBOOBiUsCkhyYKBR0wggmSCAWCQgJAdOWRSIEKRkYMBt4LKNgXkJIDQi
wCRBCUNxCiEgYaIBuiJSG4CAmjQAE5NN0zIpIhcKmJJPghRRICchnMAGYqKBSBhp
GovNg0RpWYBBAXJCyxhGAakNDAIxg7AhWiJKyJIF2ZBpBDBqSwZK0rIBHEBAgiUy
UjJyVKZAWHgQDDISksKAUhJiXIIoC7RsA0KNUxAMFAEO4TZSiIQkQIKY0YmIAYp
EcIo0CBIARnsOjYJWoZiY7Rhi0ZixECCGokJEAJNJLJFIBILJmKFiCiMycBNWUgi
CiduwTRkTJBgW0RQgoZJQ4gEQ7KMYDCAoogthKRtjKYp0MaEQgZGiYhRAKmNAUmN
5DgNpAan05RxQrJsGoRhG6MoQrQoCKBxGsUx4KBMATdlJChiFCiQCRBh2UAiGzNg
CQKS0CSBIAQISRheoyItXIhEFJgIpeZHAZVkcZkKDJRQykBq0rIgwDgBgjCOE7kI
kYCEFIgpbBiRejUNoCQi4gQG2cKFBCgSHMmJGAJy0kApwggS2AYqmZRxm7hoI4Qp
GiKJFEUR3IJEUJZFDESEwLIEmqYFQ4YsRDJuiEQhIKhMmjBw47gtYyaIAYVJA0OM
SKgJyhRyUzROEkMIG6cEWTAi2ZSA4jQigUISnDaqLDQmYQRFJCYoE0YJSjJtESgJ
GLglYigRE0ENQbIRKIRMixISosaIycAwIgyG0hiOhIYwKERSEogx2SBxE8UoQwYO
AzBgZkaEWCZSTIGBH/clYshf+kOs+kkhfysXLXu8FGIObZgKcaq73wxF6aIG7LFC
P+4V3swXYBMAFJ2SI8lubG4fqOQfx8ZJOKtokF/T3NpQ2HCC59DXHRVjsrhMhVI8
qp5srSlK340+FbEI/3IdDMh7w906dZAYS6EVmOpH8nhw8U6YdhnQgsE8Ji1V108
ZaBjaPlBKV/QmSQTlG+R9nlkwUJnSnJcNDkUxM7PWMB0vK9FWML795EeB6ptCTjy
7iuzwajfLdY16ENC/eoB3CSyEa0vwoHPd+WREMerxUvwyG1IC5vidkcdydYDzumM
/as+n8+3A3klYFSePEUPp7M/uRacRLTSX7nEV/SXkc09oD6slglYE8EFEyzNpOY+
SSKM0j2KHzeFbxQt7kNsJ+Cr4kljGOquAR6gMA2yTV+ogRvjY1TwXslfNCu0F9
PP6wsf0zYiwp4Uy72S4TY8ZevUUEt1EjKblnDjLhssZ6VOfxpV+Ln56gToyjpwXm
KjxeY3N0r7eutt3qYSzeKPAaIC16pONHITJ90/m4mJTQGf1dTXEZ7+Ny07oQTLi7
CYHgdn46/iANqq6tgmxEXyRNv0Ma+rNO+994JHTS/VcRj2RiFJNO2Zy6OWA+jWej
g29vGfxBkQzlFj7jrpnrhNUU63YeY2hOpW+XkdLdSquxYWi5SMgx91oiKss0jNwD
zEr+j2cVfho203+u/58XK5iRNnfFod0IXp7kwiBSwa9YGTEWZz3NO/xfNLhV3MbH
eIVknp5x9D1K6g9Lcsp+2gV4uhPTGmWNLQYKmbb/ae0b5516L7HScj04+b+r4Y+O
ezzakG50ml6ULI6uspyYHDr/TZJR6lAzJeL7Wazd0nmlDzXvoxJREDiueZs/vuYwL
7fs8QeMlnSzXGX+cgxIqmxrZGXB7mPjVpWq3HREkTcLf3gm/gt3odGdZBADAyUR
gQa0LS73N0flYB/kulDyPt5SHwMagX0VKUpDci6DeHhLbbDPG6norpeDkgG5zpzD
AZxvXCfLmNomFetkIlp8kysw92HniilZodi4PsY0Si9t1H52VwbQC/SnmqSbDup
HYEsjyx5erF5Zwnl0WhWd4KTUp8ChtAVw7U51hlkKjM+nlk9bj9TU51CCOnmozKF
HX91JSKpKLKX4n4tbUITff4uv6b7HGeybAJUuoAF9+vb4xWmjgotp2noqfQtPmAA
fHEzCSayWAetg+rU5P0e2HLM0ZciAdKwJ/NUWsLTDNeLwddA/sy8b8KgRGxuMOrF
HlppCYqilEfyCfOTkuSZMjPIdLeR4UYzQkM4meuotJ62lf9iLSXbYn7hDzc0mn
bKJnnmgBv6f7AxIW+1BilwS5kjk2ul3ThTERicrfsRmV5ZtzA0z2ftA6uBOGdkjQ
JYKAh+1Jqa/Ra5XXLZmx7coleqWTL/t6BwmulanA/wX7Dyu/KECe7XtfWAG+lkzt
AZ4ct4UdOFHxApBnThn/sAizAcSs9kGiuxQhbhlpyr9Ste8idJaw8weZqFXRF/rT
dEpvozUD6nMLut3X71QmYJ2/zT8ME7Fk1sBR9+1KEZcZpxLjinMoQCCB/xNUTVTS
wjev7TSVHEuo6fS964SjZowZuJrvGnorwid7HFzHR3FKeqxfvc3RzTA/kdU1Mg4Nr
3TSgO5vImRRxYGG/uY7G5hw+1EO03K81JDxkcIa56nAYsNmooLAM7LAKveJJjWnC
M2EBp3LL5PVxUj9RvQWILN81i4ScwUCqH68iQjoShRzg4z/UiXWklZ+1xf5BjJOQ
gZGrbnQbd7/gLLlpjueVxGbWFWGeZEE4LG6sAYNO6atzzqgLviNceNqRvXm2+C+J
14XWhwDTk+ZlwiJNa3oa0hMgSVZ5ra7XAWelCGZxOlmQnbe299gTBOzf2Dsxxm7y
SDBrRa0p593Mhj2sVgSLXWnqF1AR92FMAKqhjzeGHKokyh4uax+GsW9pJl7cgZP
DNdfTIFOA03hGsuQE89+qSa05+qs4HDHuiGI760uQx4SI9Rd0FxNhAPC5FzuZBPs
vnUn6HPkVcTmEKYYOarMC9VtJIPnjymLZqR46y9VjLr8qGvoR7rrAsWyFsJNiP6k
3ySbCeZwogcDq6wksKkavEpWRmAUQroQvs/TCZOIAFHQflagWpN556jmvv7j8i+q
EGOY93BgBuQum+HvidJcJy8RqVCVxYfXE3MihN6dvTxyF7BonihY6w/2lmg=
-----END PRIVATE KEY-----
```

#### Appendix D. Pre-Hashing (External $\mu$ -ML-DSA)

Some applications require pre-hashing that ease operational requirements around large or inconsistently-sized payloads. When signing with pre-hashing, the signature-generation process can be separated into a pre-hash step requiring only the message and other public information, and a core signature step that uses the public

key.

In the context of ML-DSA, pre-hashing can be performed with the HashML-DSA algorithm defined in Section 5.4 of [FIPS204]. ML-DSA itself supports an External  $\mu$  pre-hashing mode, which externalizes the message pre-hashing originally performed inside the signing operation. This mode is also laid out in [FIPS204-ExternalMuFAQ]. This document specifies only the use of ML-DSA's External  $\mu$  mode, and not HashML-DSA, in PKIX for reasons laid out in Section 8.3.

Implementations of ML-DSA using the External  $\mu$  pre-hashing mode requires the following algorithms, which are modified versions of the algorithms presented in [FIPS204]. The nomenclature used here has been modified from the NIST FAQ [FIPS204-ExternalMuFAQ] for clarity.

Pre-hash operation:

Compute $\mu$  (pk, M, ctx):

```
# Referred to as 'ExternalMu-ML-DSA.Prehash(pk, M, ctx)'
# in the FIPS 204 FAQ.
# M is the message, a bit-string
#  $\mu$  and ctx are byte-strings.
# ctx is the context string, which defaults to the empty string.

 $\mu$  = H(BytesToBits(H(pk, 64) || IntegerToBytes(0, 1) ||
                    IntegerToBytes(|ctx|, 1) || ctx) || M, 64)
# The functions 'BytesToBits' and 'IntegerToBytes' are defined
# in FIPS 204.
return  $\mu$ 
```

Figure 1: Compute $\mu$  Pre-Hash Operation

Sign operations:

Sign $\mu$  (sk,  $\mu$ ):

```
# Referred to as 'ExternalMu-ML-DSA.Sign(sk, mu)'
# in the FIPS 204 FAQ.

if | $\mu$ | != 64 then
    return error # return an error indication if the input  $\mu$  is not
                # 64 bytes.
end if

rnd = rand(32) # for the optional deterministic variant,
               # set rnd to all zeroes
if rnd = NULL then
    return error # return an error indication if random bit
                # generation failed
end if

sigma = Sign $\mu$ _internal(sk,  $\mu$ , rnd, isExternal $\mu$ =true)
return sigma
```

ML-DSA.Sign $\mu$ \_internal(sk, M', rnd, isExternal $\mu$ =false):

```
#  $\mu$  is passed to the function via the argument M'.
# Defaulting External $\mu$  to false means that
# this modified version of Sign_internal can be used
# in place of the original without interfering with
# functioning of pure ML-DSA mode.
```

```
# ... identical to FIPS 204 Algorithm 7, but with Line 6
# replaced with
6: if (isExternal $\mu$ ):
     $\mu$  = M'
```

```
else:
     $\mu$  = H(BytesToBits(tr) || M', 64)
```

Figure 2: The Operations for Signing  $\mu$

There is no need to specify an External  $\mu$  Verify() routine because this is identical to the original ML-DSA.Verify(). This makes External  $\mu$  mode simply an internal optimization of the signer, and allows an ML-DSA key to sometimes be used with the "one-shot" Sign() API and to sometimes be used with the External  $\mu$  API without any interoperability concerns.

The External  $\mu$  mode requires the Compute $\mu$  routine to have access to the hash of the signer's public key, which may not be available in some architectures, or require fetching it. That may allow for mismatches between tr and sk. At worst, this will produce a signature that will fail to verify under the intended public key since a compliant Verify() routine will independently compute tr from the public key. This is not believed to be a security concern since  $\mu$  is never used as-is within ML-DSA.Sign\_internal() (Algorithm 7 in [FIPS204]). Rather, it is hashed with values unknown to an attacker on lines 7 and 15. Thus, a signing oracle exposing Sign $\mu$ () does not leak any bits of the secret key. The External  $\mu$  mode also requires SHAKE256 to be available to the Compute $\mu$  routine.

#### Acknowledgments

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

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, Loganaden Velvindron, Carl Wallace, and Wei-Jun Wang.

#### Authors' Addresses

Jake Massimo  
AWS  
United States of America  
Email: jakemas@amazon.com

Panos Kampanakis  
AWS  
United States of America  
Email: kpanos@amazon.com

Sean Turner  
sn3rd  
Email: sean@sn3rd.com

Bas Westerbaan  
Cloudflare  
Email: bas@cloudflare.com