Stream: Internet Engineering Task Force (IETF)
RFC: 9802
Category: Standards Track
Published: June 2025
ISSN: 2070-1721

Authors:

D. Van Geest	K. Bashiri	S. Fluhrer	S. Gazdag	S. Kousidis
CryptoNext Security	*BSI*	*Cisco Systems*	*genua GmbH*	*BSI*

RFC 9802
Use of the HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure

Abstract

This document specifies algorithm identifiers and ASN.1 encoding formats for the following stateful Hash-Based Signature (HBS) schemes: Hierarchical Signature System (HSS), eXtended Merkle Signature Scheme (XMSS), and XMSS^{MT} (a multi-tree variant of XMSS). This specification applies to the Internet X.509 Public Key Infrastructure (PKI) when digital signatures are used to sign certificates and certificate revocation lists (CRLs).

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/rfc9802.

Copyright Notice

Table of Contents

1. Introduction

Stateful Hash-Based Signature (HBS) schemes such as the Hierarchical Signature System (HSS), eXtended Merkle Signature Scheme (XMSS), and XMSS^{MT} combine Merkle trees with One-Time Signatures (OTS). This is done in order to provide digital signature schemes that remain secure even when quantum computers become available. Their theoretic security is well understood and depends only on the security of the underlying hash function. As such, they can serve as an important building block for quantum computer resistant information and communication technology.

A stateful HBS private key consists of a finite collection of OTS keys, along with state information that tracks the usage of these keys to ensure the security of the scheme. Only a limited number of messages can be signed, and the private key's state must be updated and persisted after signing to prevent reuse of OTS keys. While the right selection of algorithm parameters would allow a private key to sign a virtually unbounded number of messages (e.g., 2^{60}), this is at the cost of a larger signature size and longer signing time. Because the private key in stateful HBS schemes is stateful and the number of signatures that can be generated is limited, these schemes may be unsuitable for use in interactive protocols. However, in some use cases, the deployment of stateful HBS schemes may be appropriate. Such use cases are described and discussed in Section 3.

2. Conventions and Definitions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Use Cases of Stateful HBS Schemes in X.509

As described in the Security Considerations in Section 10, it is imperative that stateful HBS implementations do not reuse OTS signatures. This makes stateful HBS algorithms inappropriate for general use cases. The exact conditions under which stateful HBS certificates may be used is left to certificate policies [RFC3647]. However, the intended use of stateful HBS schemes as described by [SP800208] can be used as a guideline:

> stateful HBS schemes are primarily intended for applications with the following characteristics: 1) it is necessary to implement a digital signature scheme in the near future; 2) the implementation will have a long lifetime; and 3) it would not be practical to transition to a different digital signature scheme once the implementation has been deployed.

In addition, since a stateful HBS private key can only generate a finite number of signatures, use cases for stateful HBS public keys in certificates should have a predictable range of the number of signatures that will be generated, falling safely below the maximum number of signatures that a private key can generate.

Use cases where stateful HBS public keys in certificates may be appropriate due to the relatively small number of signatures generated and the signer's ability to enforce security restrictions on the signing environment include:

- Firmware signing (see Section 1.1 of [SP800208], [CNSA2.0], and Section 6.7 of [BSI])
- Software signing ([CNSA2.0] and [ANSSI])
- Certification Authority (CA) certificates

In each of these cases, the operator tightly controls their secured signing environment and can mitigate OTS key reuse by employing state management strategies such as those in Section 10. Also, for secure private key backup and restoration, adequate mechanisms have to be implemented (see Section 11).

Generally speaking, stateful HBS public keys are not appropriate for use in end-entity certificates, however, in the firmware and software signing cases, signature generation will often be more tightly controlled. Some manufactures use common and well-established key formats like X.509 for their code signing and update mechanisms. Also, there are multi-party Internet of Things (IoT) ecosystems where publicly trusted code signing certificates are useful.

In general, root CAs [RFC4949] generate signatures in a more secure environment and issue fewer certificates than subordinate CAs [RFC4949]. This makes the use of stateful HBS public keys more appropriate in root CA certificates than in subordinate CA certificates. However, if a subordinate CA can match the security and signature count restrictions of a root CA, for example, if the subordinate CA only issues code-signing certificates, then using a stateful HBS public key in the subordinate CA certificate may be practical.

4. Algorithm Identifiers and Parameters

In this document, we define new Object Identifiers (OIDs) for identifying the different stateful hash-based signature algorithms. An additional OID is defined in [RFC9708] and repeated here for convenience.

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: this identifies the cryptographic algorithm with an OID.

parameters: these are optional and are the associated parameters for the algorithm identifier in the algorithm field.

The parameters field of the AlgorithmIdentifier for HSS, XMSS, and XMSS^{MT} public keys **MUST** be absent.

4.1. HSS Algorithm Identifier

The OID and public key algorithm identifier for HSS is defined in [RFC9708]. The definitions are repeated here for reference.

The AlgorithmIdentifier for an HSS public key **MUST** use the id-alg-hss-lms-hashsig OID.

```
    id-alg-hss-lms-hashsig  OBJECT IDENTIFIER ::= {
       iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
       smime(16) alg(3) 17 }
```

Note that the id-alg-hss-lms-hashsig algorithm identifier is also referred to as id-alg-mts-hashsig. This synonym is based on the terminology used in an early draft of the document that became [RFC8554].

The public key and signature values identify the hash function and the height used in the HSS tree. [RFC8554] and [SP800208] define these values, and additional identifiers can be registered in the "Leighton-Micali Signatures (LMS)" registry [IANA-LMS].

4.2. XMSS Algorithm Identifier

The AlgorithmIdentifier for an XMSS public key **MUST** use the id-alg-xmss-hashsig OID.

```
    id-alg-xmss-hashsig  OBJECT IDENTIFIER ::= {
       iso(1) identified-organization(3) dod(6) internet(1)
       security(5) mechanisms(5) pkix(7) algorithms(6) 34 }
```

The public key and signature values identify the hash function and the height used in the XMSS tree. [RFC8391] and [SP800208] define these values, and additional identifiers can be registered in the "Leighton-Micali Signatures (LMS)" registry [IANA-XMSS].

4.3. XMSS^{MT} Algorithm Identifier

The AlgorithmIdentifier for an XMSS^{MT} public key **MUST** use the id-alg-xmssmt-hashsig OID.

```
   id-alg-xmssmt-hashsig  OBJECT IDENTIFIER ::= {
      iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) algorithms(6) 35 }
```

The public key and signature values identify the hash function and the height used in the XMSS^{MT} tree. [RFC8391] and [SP800208] define these values, and additional identifiers can be registered in the "Leighton-Micali Signatures (LMS)" registry [IANA-XMSS].

5. Public Key Identifiers

Certificates conforming to [RFC5280] can convey a public key for any public key algorithm. The certificate indicates the algorithm through an algorithm identifier. An algorithm identifier consists of an OID and optional parameters.

[RFC8554] defines the encoding of HSS public keys, and [RFC8391] defines the encodings of XMSS and XMSS^{MT} public keys. When used in a SubjectPublicKeyInfo type, the subjectPublicKey BIT STRING contains these encodings of the public key.

This document defines ASN.1 [X680] OCTET STRING types for encoding the public keys when not used in a SubjectPublicKeyInfo. The OCTET STRING is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

5.1. HSS Public Keys

The HSS public key identifier is as follows:

```
   pk-HSS-LMS-HashSig PUBLIC-KEY ::= {
      IDENTIFIER id-alg-hss-lms-hashsig
      -- KEY no ASN.1 wrapping --
      PARAMS ARE absent
      CERT-KEY-USAGE
         { digitalSignature, nonRepudiation, keyCertSign, cRLSign } }
```

The HSS public key is defined as follows:

```
HSS-LMS-HashSig-PublicKey ::= OCTET STRING
```

[RFC8554] defines the encoding of an HSS public key using the `hss_public_key` structure. See [SP800208] and [RFC8554] for more information on the contents and format of an HSS public key. Note that the Leighton-Micali Signature (LMS) single-tree signature scheme is instantiated as HSS with the number of levels being equal to 1.

5.2. XMSS Public Keys

The XMSS public key identifier is as follows:

```
pk-XMSS-HashSig PUBLIC-KEY ::= {
   IDENTIFIER id-alg-xmss-hashsig
   -- KEY no ASN.1 wrapping --
   PARAMS ARE absent
   CERT-KEY-USAGE
      { digitalSignature, nonRepudiation, keyCertSign, cRLSign } }
```

The XMSS public key is defined as follows:

```
XMSS-HashSig-PublicKey ::= OCTET STRING
```

[RFC8391] defines the encoding of an XMSS public key using the `xmss_public_key` structure. See [SP800208] and [RFC8391] for more information on the contents and format of an XMSS public key.

5.3. XMSS^{MT} Public Keys

The XMSS^{MT} public key identifier is as follows:

```
pk-XMSSMT-HashSig PUBLIC-KEY ::= {
   IDENTIFIER id-alg-xmssmt-hashsig
   -- KEY no ASN.1 wrapping --
   PARAMS ARE absent
   CERT-KEY-USAGE
      { digitalSignature, nonRepudiation, keyCertSign, cRLSign } }
```

The XMSS^{MT} public key is defined as follows:

```
XMSSMT-HashSig-PublicKey ::= OCTET STRING
```

[RFC8391] defines the encoding of an XMSS^{MT} public key using the `xmssmt_public_key` structure. See [SP800208] and [RFC8391] for more information on the contents and format of an XMSS^{MT} public key.

6. Key Usage Bits

The intended application for the key is indicated in the keyUsage certificate extension [RFC5280]. When id-alg-hss-lms-hashsig, id-alg-xmss-hashsig, or id-alg-xmssmt-hashsig appears in the SubjectPublicKeyInfo field of a CA X.509 certificate [RFC5280], the certificate key usage extension **MUST** contain at least one of the following values: digitalSignature, nonRepudiation, keyCertSign, or cRLSign. However, it **MUST NOT** contain other values.

When id-alg-hss-lms-hashsig, id-alg-xmss-hashsig, or id-alg-xmssmt-hashsig appears in the SubjectPublicKeyInfo field of an end entity X.509 certificate [RFC5280], the certificate key usage extension **MUST** contain at least one of the following values: digitalSignature, nonRepudiation or cRLSign. However, it **MUST NOT** contain other values.

7. Signature Algorithms

The same OIDs used to identify HSS, XMSS, and XMSS^{MT} public keys are also used to identify their respective signatures. When these algorithm identifiers appear in the algorithm field of an AlgorithmIdentifier, the encoding **MUST** omit the parameters field. That is, the AlgorithmIdentifier **SHALL** be a SEQUENCE of one component, one of the OIDs defined in the following subsections.

When the signature algorithm identifiers described in this document are used to create a signature on a message, no digest algorithm is applied to the message before signing. That is, the full data to be signed is signed rather than a digest of the data.

The format of an HSS signature is described in Section 6.2 of [RFC8554]. The format of an XMSS signature is described in Appendix B.2 of [RFC8391], and the format of an XMSS^{MT} signature is described in Appendix C.2 of [RFC8391]. The octet string representing the signature is encoded directly in a BIT STRING without adding any additional ASN.1 wrapping. For the Certificate and CertificateList structures, the octet string is encoded in the "signatureValue" BIT STRING field.

7.1. HSS Signature Algorithm

The id-alg-hss-lms-hashsig OID is used to specify that an HSS signature was generated on the full message, i.e., the message was not hashed before being processed by the HSS signature algorithm.

See [SP800208] and [RFC8554] for more information on the contents and format of an HSS signature.

7.2. XMSS Signature Algorithm

The id-alg-xmss-hashsig OID is used to specify that an XMSS signature was generated on the full message, i.e., the message was not hashed before being processed by the XMSS signature algorithm.

See [SP800208] and [RFC8391] for more information on the contents and format of an XMSS signature.

The signature generation **MUST** be performed according to Section 7.2 of [SP800208].

7.3. XMSS^{MT} Signature Algorithm

The id-alg-xmssmt-hashsig OID is used to specify that an XMSS^{MT} signature was generated on the full message, i.e., the message was not hashed before being processed by the XMSS^{MT} signature algorithm.

See [SP800208] and [RFC8391] for more information on the contents and format of an XMSS^{MT} signature.

The signature generation **MUST** be performed according to Section 7.2 of [SP800208].

8. Key Generation

The key generation for XMSS and XMSS^{MT} **MUST** be performed according to Section 7.2 of [SP800208].

9. ASN.1 Module

For reference purposes, the ASN.1 syntax is presented as an ASN.1 module here [X680]. Note that as per [RFC5280], certificates use the Distinguished Encoding Rules; see [X690]. This ASN.1 module builds upon the conventions established in [RFC5912]. This module imports objects from [RFC5912] and [RFC9708].

```
X509-SHBS-2024
  { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-shbs-2024(114) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS
  PUBLIC-KEY, SIGNATURE-ALGORITHM
    FROM AlgorithmInformation-2009  -- [RFC5912]
      { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0)
        id-mod-algorithmInformation-02(58) }

  sa-HSS-LMS-HashSig, pk-HSS-LMS-HashSig
    FROM MTS-HashSig-2013 -- [RFC9708]
      { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
        id-smime(16) id-mod(0) id-mod-mts-hashsig-2013(64) };

--
-- Object Identifiers
--
```

```
-- id-alg-hss-lms-hashsig is defined in [RFC9708]

id-alg-xmss-hashsig  OBJECT IDENTIFIER ::= {
   iso(1) identified-organization(3) dod(6) internet(1) security(5)
   mechanisms(5) pkix(7) algorithms(6) 34 }

id-alg-xmssmt-hashsig  OBJECT IDENTIFIER ::= {
   iso(1) identified-organization(3) dod(6) internet(1) security(5)
   mechanisms(5) pkix(7) algorithms(6) 35 }

--
-- Signature Algorithms and Public Keys
--

-- sa-HSS-LMS-HashSig is defined in [RFC9708]

sa-XMSS-HashSig SIGNATURE-ALGORITHM ::= {
   IDENTIFIER id-alg-xmss-hashsig
   PARAMS ARE absent
   PUBLIC-KEYS { pk-XMSS-HashSig }
   SMIME-CAPS { IDENTIFIED BY id-alg-xmss-hashsig } }

sa-XMSSMT-HashSig SIGNATURE-ALGORITHM ::= {
   IDENTIFIER id-alg-xmssmt-hashsig
   PARAMS ARE absent
   PUBLIC-KEYS { pk-XMSSMT-HashSig }
   SMIME-CAPS { IDENTIFIED BY id-alg-xmssmt-hashsig } }

-- pk-HSS-LMS-HashSig is defined in [RFC9708]

pk-XMSS-HashSig PUBLIC-KEY ::= {
   IDENTIFIER id-alg-xmss-hashsig
   -- KEY no ASN.1 wrapping --
   PARAMS ARE absent
   CERT-KEY-USAGE
      { digitalSignature, nonRepudiation, keyCertSign, cRLSign } }

XMSS-HashSig-PublicKey ::= OCTET STRING

pk-XMSSMT-HashSig PUBLIC-KEY ::= {
   IDENTIFIER id-alg-xmssmt-hashsig
   -- KEY no ASN.1 wrapping --
   PARAMS ARE absent
   CERT-KEY-USAGE
      { digitalSignature, nonRepudiation, keyCertSign, cRLSign } }

XMSSMT-HashSig-PublicKey ::= OCTET STRING

--
-- Public Key (pk-) Algorithms
--
PublicKeys PUBLIC-KEY ::= {
   -- This expands PublicKeys from RFC 5912
   pk-HSS-LMS-HashSig |
   pk-XMSS-HashSig |
   pk-XMSSMT-HashSig,
   ...
}

--
-- Signature Algorithms (sa-)
--
SignatureAlgs SIGNATURE-ALGORITHM ::= {
   -- This expands SignatureAlgorithms from RFC 5912
   sa-HSS-LMS-HashSig |
   sa-XMSS-HashSig |
   sa-XMSSMT-HashSig,
   ...
}

END
```

10. Security Considerations

The security requirements of [SP800208] **MUST** be taken into account.

As stateful HBS private keys can only generate a limited number of signatures, a user needs to be aware of the total number of signatures they intend to generate in their use case; otherwise, they risk exhausting the number of OTS keys in their private key.

For stateful HBS schemes, it is crucial to stress the importance of correct state management. If an attacker were able to obtain signatures for two different messages created using the same OTS key, then it would become computationally feasible for that attacker to create forgeries [BH16]. As noted in [MCGREW] and [ETSI-TR-103-692], extreme care needs to be taken in order to avoid the risk that an OTS key will be reused accidentally. This is a new requirement that most developers will not be familiar with and requires careful handling.

Various strategies for a correct state management can be applied:

- Implement a record of all signatures generated by a key pair associated with a stateful HBS instance, for example, by logging the OTS key indexes as signatures are generated. This record may be stored outside the device that is used to generate the signature. Check the record to prevent OTS key reuse before a new signature is released. If OTS key reuse is detected, freeze all new signature generation by the private key, re-audit previously released signatures (possibly revoking the private key if previously released signatures showed OTS key reuse), and perform a post-failure audit.
- Use a stateful HBS instance only for a moderate number of signatures such that it is always practical to keep a consistent record and be able to unambiguously trace back all generated signatures.
- Apply the state reservation strategy described in Section 5 of [MCGREW], where upcoming states are reserved in advance by the signer. In this way, the number of state synchronizations between nonvolatile and volatile memory is reduced.

11. Backup and Restore Management

Certificate authorities have high demands in order to ensure the availability of signature generation throughout the validity period of signing key pairs.

Some usual backup and restore strategies when using a stateless signature scheme (e.g., SLH-DSA) are to:

- duplicate private keying material and operate redundant signing devices.
- store and safeguard a copy of the private keying material such that it can be used to set up a new signing device in case of technical difficulties.

For stateful HBS schemes, such straightforward backup and restore strategies will lead to OTS reuse with high probability as a correct state management is not guaranteed. Strategies for maintaining availability and keeping a correct state are described in Section 7 of [SP800208] and [S-HBS].

12. IANA Considerations

IANA has registered the following OID for the ASN.1 module (see Section 9) in the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry:

Decimal	Description	References
114	id-mod-pkix1-shbs-2024	RFC 9802

Table 1

IANA has registered the following entries in the "SMI Security for PKIX Algorithms" (1.3.6.1.5.5.7.6) registry [SMI-PKIX]:

Decimal	Description	References
34	id-alg-xmss-hashsig	RFC 9802
35	id-alg-xmssmt-hashsig	RFC 9802

Table 2

13. References

13.1. Normative References

[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>.

[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>.

[RFC8391] Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme", RFC 8391, DOI 10.17487/RFC8391, May 2018, <https://www.rfc-editor.org/info/rfc8391>.

[RFC8554] McGrew, D., Curcio, M., and S. Fluhrer, "Leighton-Micali Hash-Based Signatures", RFC 8554, DOI 10.17487/RFC8554, April 2019, <https://www.rfc-editor.org/info/rfc8554>.

[RFC9708] Housley, R., "Use of the HSS/LMS Hash-Based Signature Algorithm in the Cryptographic Message Syntax (CMS)", RFC 9708, DOI 10.17487/RFC9708, January 2025, <https://www.rfc-editor.org/info/rfc9708>.

[SP800208] Cooper, D., Apon, D., Dang, Q., Davidson, M., Dworkin, M., and C. Miller, "Recommendation for Stateful Hash-Based Signature Schemes", NIST SP 800-208, DOI 10.6028/nist.sp.800-208, 29 October 2020, <https://doi.org/10.6028/NIST.SP.800-208>.

[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>.

13.2. Informative References

[ANSSI] Agence nationale de la sécurité des systèmes d'information (ANSSI), "ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)", 21 December 2023, <https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf>.

[BH16] Bruinderink, L. and S. Hülsing, "Oops, I did it again - Security of One-Time Signatures under Two-Message Attacks.", Cryptology ePrint Archive, Paper 2016/1042, 2016, <https://eprint.iacr.org/2016/1042>.

[BSI] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Quantum-safe cryptography - fundamentals, current developments and recommendations", 18 May 2022, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf>.

[CNSA2.0] National Security Agency (NSA), "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ", 7 September 2022, <https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF>.

[ETSI-TR-103-692] European Telecommunications Standards Institute (ETSI), "CYBER; State management for stateful authentication mechanisms", ETSI TR 103 692 v1.1.1, November 2021, <https://www.etsi.org/deliver/etsi_tr/103600_103699/103692/01.01.01_60/tr_103692v010101p.pdf>.

[IANA-LMS] IANA, "Leighton-Micali Signatures (LMS)", <https://www.iana.org/assignments/leighton-micali-signatures/>.

[IANA-XMSS] IANA, "XMSS: Extended Hash-Based Signatures", <https://iana.org/assignments/xmss-extended-hash-based-signatures/>.

[MCGREW] McGrew, D., Kampanakis, P., Fluhrer, S., Gazdag, S., Butin, D., and J. Buchmann, "State Management for Hash-Based Signatures", Cryptology ePrint Archive, Paper 2016/357, 2 November 2016, <https://eprint.iacr.org/2016/357>.

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, DOI 10.17487/RFC3279, April 2002, <https://www.rfc-editor.org/info/rfc3279>.

[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>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC8410] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure", RFC 8410, DOI 10.17487/RFC8410, August 2018, <https://www.rfc-editor.org/info/rfc8410>.

[RFC8411] Schaad, J. and R. Andrews, "IANA Registration for the Cryptographic Algorithm Object Identifier Range", RFC 8411, DOI 10.17487/RFC8411, August 2018, <https://www.rfc-editor.org/info/rfc8411>.

[S-HBS] Wiggers, T., Bashiri, K., Kölbl, S., Goodman, J., and S. Kousidis, "Hash-based Signatures: State and Backup Management", Work in Progress, Internet-Draft, draft-wiggers-hbs-state-02, 1 April 2025, <https://datatracker.ietf.org/doc/html/draft-wiggers-hbs-state-02>.

[SMI-PKIX] IANA, "SMI Security for PKIX Algorithms", <https://www.iana.org/assignments/smi-numbers>.

Appendix A. HSS X.509 v3 Certificate Example

This section shows a self-signed X.509 v3 certificate using HSS.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e8:91:d6:06:91:4f:ce:f3
        Signature Algorithm: hss
        Issuer: C = US, ST = VA, L = Herndon, O = Bogus CA
        Validity
            Not Before: May 14 08:58:11 2024 GMT
            Not After : May 14 08:58:11 2034 GMT
        Subject: C = US, ST = VA, L = Herndon, O = Bogus CA
        Subject Public Key Info:
            Public Key Algorithm: hss
                hss public key:
                PQ key material:
                    00:00:00:01:00:00:00:05:00:00:00:04:c0:96:12:
                    8b:ea:38:30:78:eb:f6:fb:43:d7:7f:9f:9e:81:39:
                    e2:7c:b9:34:4e:6e:53:19:f0:ee:68:75:85:83:d3:
                    2b:e9:7b:14:46:9e:4e:c5:e3:5a:18:0b:30:e5:13
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                58:15:AB:F4:CF:03:69:02:60:7A:57:4D:C5:D5:B3:72:
                8A:19:21:68
            X509v3 Authority Key Identifier:
                58:15:AB:F4:CF:03:69:02:60:7A:57:4D:C5:D5:B3:72:
                8A:19:21:68
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: hss
    Signature Value:
        00:00:00:00:00:00:00:00:00:00:00:04:9c:37:52:ff:b9:d7:
        df:f5:5b:01:ba:50:c2:50:cc:6f:f3:b1:73:df:0c:2a:ea:b3:
        ed:96:1e:ce:e7:58:05:da:8d:a7:77:21:42:32:d9:f9:4a:4d:
        f7:2b:18:2a:1c:5c:69:03:f3:1c:9c:95:6d:31:9a:c9:ca:84:
        4d:ae:b3:8b:c3:71:ac:3f:87:51:be:38:b4:bf:d9:dc:90:1f:
        1e:54:bd:f9:1a:65:70:d4:46:b6:ad:4d:6d:16:b9:fb:29:f4:
        e3:86:42:4a:3f:a4:8f:01:84:9b:44:0b:23:22:9c:97:6d:d5:
        b9:26:39:11:ab:46:82:bd:10:6c:b4:7a:64:ed:c7:40:b0:33:
        f0:b5:81:1c:b4:41:54:9c:30:d9:d2:93:ba:48:8c:4f:d0:25:
        41:60:7b:90:5e:12:20:b7:30:16:16:1e:b7:ee:d8:4b:ee:ed:
        3c:70:fc:ff:36:18:aa:24:23:87:91:65:a8:95:2d:b6:1c:d1:
        02:7b:70:81:8a:18:17:c0:45:62:fe:47:a1:3e:69:54:31:67:
        58:9a:e1:e3:c9:8d:ee:1e:2a:d1:46:75:e9:e4:90:67:01:57:
        92:54:db:b4:ea:de:8b:e7:eb:fc:27:80:9b:d5:da:e0:8e:b0:
        b3:08:ca:6f:a1:1c:f4:40:65:b0:f6:f8:c9:a7:97:04:c8:7c:
        9e:56:ec:2f:4b:cd:45:8b:d7:e6:a7:50:c7:e6:21:2c:17:31:
        23:11:7a:ae:9a:b5:84:5f:e6:5c:82:99:a8:3a:a9:91:87:9a:
        24:5c:83:01:91:7c:fc:cd:be:2e:92:50:fb:12:11:96:08:0d:
        c9:24:0d:bb:6f:fb:59:05:af:7f:96:bc:a3:f4:58:e2:fa:0a:
        4a:f2:4c:f7:b3:1b:81:dd:4a:41:a0:b1:dd:52:4c:bb:6d:c0:
        a8:d9:bb:29:c8:fc:e3:7e:f8:6a:e5:5e:c4:e4:e8:7c:0b:00:
        87:15:75:a2:06:50:97:c6:1f:14:52:79:04:a8:9c:ec:b1:c7:
        6a:46:33:98:b8:63:f7:a7:2c:d4:62:78:94:1c:5d:9d:4f:a6:
        0a:ae:39:50:85:b2:09:8d:62:c9:4c:11:9f:0c:91:a5:ac:2d:
        11:bd:71:b6:0c:ea:34:98:53:fc:2e:cc:7b:a4:9c:2e:7a:a4:
        8d:e2:e8:8c:01:a9:9c:3e:b5:34:77:33:82:01:d4:ef:72:04:
        d6:5b:e5:f6:2c:1b:ae:86:c4:73:02:44:85:d6:f7:ac:a3:e8:
        f6:a9:b5:5c:6d:46:88:da:55:b8:2b:7a:4c:0c:9a:e7:cd:5d:
        62:8a:ca:c8:96:ce:8d:71:7b:d2:c1:0d:9a:35:55:2b:84:3e:
        0e:a5:fa:d6:a0:76:8e:23:b3:df:c9:3b:4f:68:56:1e:e9:3c:
        79:5b:d3:25:54:11:ad:a6:ac:58:11:49:8f:4d:c4:c1:39:99:
        76:3a:a6:d1:2f:57:ad:bf:7c:9d:57:cc:37:0d:29:84:29:7b:
        cb:46:85:c3:81:c5:33:9a:65:c3:2f:01:48:ca:44:6c:f1:84:
        3d:d0:49:c2:c1:05:db:77:4c:b9:72:3d:6f:ce:69:f2:91:c6:
        15:25:8f:da:38:7e:ef:5b:3e:5f:35:ab:a6:78:16:28:42:c1:
        2c:2f:9e:11:53:2c:bd:c4:24:7b:e9:c4:ce:3d:d6:41:c7:5d:
        92:91:c3:37:cb:72:44:d7:0d:70:85:13:0b:ac:b3:0f:b0:e5:
        e3:2e:48:b9:9c:b8:d7:3e:7c:50:69:03:7a:5f:ae:f8:6c:09:
        61:97:6b:ce:cd:e5:f0:55:fe:05:f8:97:1d:9e:81:65:f5:ff:
        9a:7a:8c:96:d8:f8:cf:d8:dc:55:ce:67:7a:00:6b:fd:bb:3f:
        1b:3d:65:94:c1:5a:b6:a0:8e:be:a4:be:26:90:5f:1f:06:d4:
        ea:3f:a6:97:40:8e:bf:18:5c:92:0f:15:e3:05:4a:14:51:1e:
        23:81:ef:cf:f7:a8:88:75:f8:2d:28:37:26:87:27:63:5c:01:
        53:0e:5e:53:d2:a7:18:eb:2f:c0:82:49:05:b0:4d:33:6f:94:
        10:91:77:f8:90:9e:ca:fe:bb:3d:c4:42:d6:89:84:98:42:f4:
        24:b3:b4:db:5e:2b:66:a9:ff:6c:18:d4:79:f8:72:73:53:9b:
        02:ed:04:73:77:a4:68:cf:4b:be:4b:16:50:62:87:f9:49:99:
        e3:a1:0c:42:92:bc:a9:e3:2d:22:82:35:7f:71:15:88:70:6a:
        01:ab:44:64:ad:e5:52:d4:97:ee:bb:44:7b:6e:08:7f:dd:94:
        fd:c9:1c:6b:59:d1:92:51:29:03:ce:ec:bf:41:a5:14:69:54:
        3a:b4:39:d9:44:5d:f1:b2:f4:5c:6b:9f:c9:5f:bb:fc:c8:c7:
        a3:8b:e1:ec:e2:d0:69:5a:40:1c:9c:9d:8a:3d:77:3b:c1:5d:
        c0:72:61:4b:37:c5:96:8c:6d:8b:f8:56:da:ac:3e:3c:72:09:
        ce:f6:c3:fe:5d:cf:37:d9:68:cd:a7:dd:f7:96:63:da:8c:1d:
        df:b8:32:cf:eb:97:11:83:fe:6b:aa:b9:e2:4b:b2:ea:62:73:
        c3:1c:e9:40:90:56:4f:12:c3:ba:f4:2b:d9:1c:50:cc:e0:51:
        d8:eb:bf:67:28:0c:2d:13:8d:b3:6f:13:6a:1d:a7:54:20:ba:
        82:5b:b8:e5:1f:89:f1:67:26:c1:dc:1b:60:57:ed:a6:2c:f2:
        17:01:7f:a5:e7:5c:64:c9:3c:08:f2:cf:48:ec:88:84:ef:03:
        c2:f5:eb:05:31:7d:fe:7f:3c:71:41:28:17:64:5f:b9:ec:54:
        79:d0:b3:98:fb:84:9c:36:8b:43:0b:d4:c9:ec:09:4a:70:13:
        62:f2:36:c8:b4:75:cc:2a:77:08:a0:9d:ef:19:d6:88:dc:e2:
        b2:4e:40:61:71:cb:c7:c3:de:16:6f:49:7f:5e:d5:17:00:00:
        00:05:79:47:12:9f:ce:eb:1d:a8:fd:0d:b0:18:44:6a:ef:54:
        28:46:e4:19:f6:2d:3e:74:bb:9d:36:0a:ae:67:4a:28:7a:1b:
        80:39:a0:08:2a:28:a0:ec:55:ee:55:aa:a1:cc:94:d4:36:1a:
        b3:57:25:30:ad:2c:5e:63:ba:22:fc:aa:7a:59:64:f6:d8:03:
        20:28:71:f9:dc:09:fa:4c:81:b9:64:1b:ad:ea:cb:db:18:17:
        5d:d8:98:bd:d2:8d:c5:04:7c:5b:92:9a:89:f6:bc:d6:55:c7:
        08:5d:3c:58:8e:18:ac:6f:88:a8:d7:9e:d4:ee:5d:f5:21:4e:
        a5:8b:19:5f:e3:f4:66:f9:25:4d:f9:c6:60:62:31:72:5c:34:
        34:67:1a:a7:6a:7d:54:a3:d8:9b:1f:5b:f8:08:41:79:5b:43
```

```
-----BEGIN CERTIFICATE-----
MIIGnjCCAXagAwIBAgIJAOiR1gaRT87zMA0GCyqGSIb3DQEJEAMRMD8xCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJWQTEQMA4GA1UEBwwHSGVybmRvbjERMA8GA1UECgwI
Qm9ndXMgQ0EwHhcNMjQwNTE0MDg1ODExWhcNMzQwNTE0MDg1ODExWjA/MQswCQYD
VQQGEwJVUzELMAkGA1UECAwCVkExEDAOBgNVBAcMB0hlcm5kb24xETAPBgNVBAoM
CEJvZ3VzIENBME4wDQYLKoZIhvcNAQkQAxEDPQAAAAABAAAABQAAAATAlhKL6jgw
eOv2+0PXf5+egTnifLk0Tm5TGfDuaHWFg9Mr6XsURp5OxeNaGAsw5ROjYzBhMB0G
A1UdDgQWBBRYFav0zwNpAmB6V03F1bNyihkhaDAfBgNVHSMEGDAWgBRYFav0zwNp
AmB6V03F1bNyihkhaDAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAN
BgsqhkiG9w0BCRADEQOCBREAAAAAAAAAAAAAAAAEnDdS/7nX3/VbAbpQwlDMb/Ox
c98MKuqz7ZYezudYBdqNp3chQjLZ+UpN9ysYKhxcaQPzHJyVbTGaycqETa6zi8Nx
rD+HUb44tL/Z3JAfHlS9+RplcNRGtq1NbRa5+yn044ZCSj+kjwGEm0QLIyKcl23V
uSY5EatGgr0QbLR6ZO3HQLAz8LWBHLRBVJww2dKTukiMT9AlQWB7kF4SILcwFhYe
t+7YS+7tPHD8/zYYqiQjh5FlqJUtthzRAntwgYoYF8BFYv5HoT5pVDFnWJrh48mN
7h4q0UZ16eSQZwFXklTbtOrei+fr/CeAm9Xa4I6wswjKb6Ec9EBlsPb4yaeXBMh8
nlbsL0vNRYvX5qdQx+YhLBcxIxF6rpq1hF/mXIKZqDqpkYeaJFyDAZF8/M2+LpJQ
+xIRlggNySQNu2/7WQWvf5a8o/RY4voKSvJM97Mbgd1KQaCx3VJMu23AqNm7Kcj8
4374auVexOTofAsAhxV1ogZQl8YfFFJ5BKic7LHHakYzmLhj96cs1GJ4lBxdnU+m
Cq45UIWyCY1iyUwRnwyRpawtEb1xtgzqNJhT/C7Me6ScLnqkjeLojAGpnD61NHcz
ggHU73IE1lvl9iwbrobEcwJEhdb3rKPo9qm1XG1GiNpVuCt6TAya581dYorKyJbO
jXF70sENmjVVK4Q+DqX61qB2jiOz38k7T2hWHuk8eVvTJVQRraasWBFJj03EwTmZ
djqm0S9Xrb98nVfMNw0phCl7y0aFw4HFM5plwy8BSMpEbPGEPdBJwsEF23dMuXI9
b85p8pHGFSWP2jh+71s+XzWrpngWKELBLC+eEVMsvcQke+nEzj3WQcddkpHDN8ty
RNcNcIUTC6yzD7Dl4y5IuZy41z58UGkDel+u+GwJYZdrzs3l8FX+BfiXHZ6BZfX/
mnqMltj4z9jcVc5negBr/bs/Gz1llMFatqCOvqS+JpBfHwbU6j+ml0COvxhckg8V
4wVKFFEeI4Hvz/eoiHX4LSg3JocnY1wBUw5eU9KnGOsvwIJJBbBNM2+UEJF3+JCe
yv67PcRC1omEmEL0JLO0214rZqn/bBjUefhyc1ObAu0Ec3ekaM9LvksWUGKH+UmZ
46EMQpK8qeMtIoI1f3EViHBqAatEZK3lUtSX7rtEe24If92U/ckca1nRklEpA87s
v0GlFGlUOrQ52URd8bL0XGufyV+7/MjHo4vh7OLQaVpAHJydij13O8FdwHJhSzfF
loxti/hW2qw+PHIJzvbD/l3PN9lozafd95Zj2owd37gyz+uXEYP+a6q54kuy6mJz
wxzpQJBWTxLDuvQr2RxQzOBR2Ou/ZygMLRONs28Tah2nVCC6glu45R+J8Wcmwdwb
YFftpizyFwF/pedcZMk8CPLPSOyIhO8DwvXrBTF9/n88cUEoF2RfuexUedCzmPuE
nDaLQwvUyewJSnATYvI2yLR1zCp3CKCd7xnWiNzisk5AYXHLx8PeFm9Jf17VFwAA
AAV5RxKfzusdqP0NsBhEau9UKEbkGfYtPnS7nTYKrmdKKHobgDmgCCoooOxV7lWq
ocyU1DYas1clMK0sXmO6Ivyqellk9tgDIChx+dwJ+kyBuWQbrerL2xgXXdiYvdKN
xQR8W5Kaifa81lXHCF08WI4YrG+IqNee1O5d9SFOpYsZX+P0ZvklTfnGYGIxclw0
NGcap2p9VKPYmx9b+AhBeVtD
-----END CERTIFICATE-----
```

Appendix B. XMSS X.509 v3 Certificate Example

This section shows a self-signed X.509 v3 certificate using XMSS.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            54:7e:64:70:29:9e:03:c5:7a:a5:5c:78:d1:27:87:8c:
            54:35:17:5d
        Signature Algorithm: xmss
        Issuer: C = FR, L = Paris, O = Bogus XMSS CA
        Validity
            Not Before: Jul 10 08:27:24 2024 GMT
            Not After : Jul  8 08:27:24 2034 GMT
        Subject: C = FR, L = Paris, O = Bogus XMSS CA
        Subject Public Key Info:
            Public Key Algorithm: xmss
                xmss public key:
                PQ key material:
                    00:00:00:01:2b:eb:bf:66:14:de:6f:96:5b:4d:2a:
                    50:00:7b:ad:5c:22:b0:13:79:72:02:14:a9:5f:fc:
                    96:e0:9b:78:8e:d6:be:8c:1c:70:3c:d8:dd:78:b2:
                    1a:14:47:be:1f:0d:74:72:3f:36:76:c2:cb:19:ad:
                    29:90:0b:82:de:9b:7f:df
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                62:CE:35:A5:47:77:FF:21:87:2E:BC:2D:27:E7:8E:F4:
                35:6B:CF:D8
            X509v3 Authority Key Identifier:
                62:CE:35:A5:47:77:FF:21:87:2E:BC:2D:27:E7:8E:F4:
                35:6B:CF:D8
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: xmss
    Signature Value:
        00:00:00:00:e5:88:a8:b8:73:ad:4d:92:f8:5c:81:c5:8a:63:
        57:6a:a7:3b:54:aa:b6:06:8a:d9:f1:c2:0b:c8:27:1e:4b:a2:
        cf:e2:da:44:ea:e8:f2:40:a8:b9:54:9c:49:36:12:24:df:74:
        ad:e5:29:ef:4f:da:88:0d:21:5d:3b:64:63:27:d0:84:b5:95:
        7a:30:18:37:cd:34:17:dd:ac:9d:9e:48:db:74:07:79:84:21:
        5a:f0:26:cd:21:64:7b:77:33:48:58:67:9b:2c:b2:85:6d:cc:
        ec:31:4b:2f:51:55:3a:85:e1:ca:04:15:ce:6e:47:39:f5:e9:
        31:45:41:ed:71:c6:4f:96:f5:ae:64:6a:bd:72:d0:8c:17:02:
        99:10:1d:14:34:ca:e5:47:e3:f7:66:96:96:11:d5:97:76:76:
        83:f1:84:a5:b6:00:5e:3e:67:97:7a:32:dc:c8:eb:4c:29:46:
        77:99:d6:da:45:e6:7b:8c:45:6d:b5:29:6b:fd:98:a2:89:8d:
        0c:30:42:f5:0b:7c:97:c5:b1:1d:e2:da:67:a9:48:a4:9e:29:
        f4:60:3f:4d:1d:48:83:82:38:ef:fa:cb:1d:86:11:a1:15:94:
        fb:d5:ee:68:f9:44:b9:3d:54:70:f3:be:17:8d:d7:2e:85:2d:
        5c:d0:a0:c5:99:52:cc:79:e7:1c:18:d9:6e:3d:0f:6c:05:51:
        33:28:35:e2:02:59:5f:1f:ed:78:0a:c6:62:f0:7d:fe:73:96:
        03:4c:b4:42:e3:00:c2:d7:cb:eb:51:10:c4:0c:64:b8:37:fe:
        85:d0:8e:11:6d:a6:16:77:b1:1e:01:d9:1e:f3:10:9c:dd:01:
        bc:38:75:5e:8f:58:9e:5b:6c:7b:0a:41:08:59:35:a9:3a:83:
        19:e0:7d:a1:f5:cf:a3:1c:4e:07:e1:ad:03:95:f2:d3:8b:79:
        33:f8:52:22:53:1b:1e:32:9a:61:3f:c4:7c:9a:e8:d5:b5:28:
        f1:84:65:d5:c1:fc:4d:16:93:88:93:69:ca:fa:94:a0:95:4e:
        23:ae:1e:60:e0:e8:b4:bf:ff:16:95:71:0f:31:74:bb:be:b8:
        5a:eb:24:95:8b:95:28:13:cd:e3:a9:65:f7:f5:6e:9b:a9:a9:
        7a:05:ce:ab:f0:54:62:d9:12:f8:a1:1a:68:df:af:15:8f:8a:
        df:67:27:c9:ed:bd:e1:81:a6:8d:9a:84:f3:91:36:d9:89:74:
        8e:ef:84:dc:5c:03:1a:08:e4:d7:f0:72:fc:6d:8a:01:34:94:
        e5:ff:08:51:1b:80:5f:e7:07:d8:9f:25:e4:1d:c3:f8:e5:d0:
        9c:50:cf:66:71:f9:cc:f7:c0:a7:d0:66:01:b7:17:a0:5f:66:
        97:a4:ff:62:ac:1c:a0:63:0d:30:28:e9:90:d5:59:a4:48:d8:
        07:87:02:4b:3f:68:23:a5:04:dc:b3:d7:45:f6:dc:b0:ec:c6:
        90:a6:1c:a1:f8:7e:84:ba:63:7e:5a:64:14:78:58:f5:75:c0:
        f5:e1:1d:bd:49:57:c0:40:08:07:99:7f:43:2e:e2:25:d8:ed:
        a3:1a:e3:78:f1:78:af:02:49:54:36:59:8e:d3:72:a5:0b:52:
        32:bd:17:a2:cf:e1:47:21:28:3d:ba:b6:24:d9:18:f9:44:73:
```

```
        35:ed:29:a4:18:bc:ed:68:cd:4a:9a:34:cb:1a:2f:b3:5f:ba:
        73:9b:18:ee:7a:a8:92:25:65:25:81:04:63:1c:22:2b:b8:ba:
        81:21:bc:f9:9d:a8:78:98:75:bc:ed:4a:c6:b7:6f:c0:91:24:
        eb:1d:f9:5d:e0:e3:78:4e:05:f6:34:0f:7b:41:54:49:20:a2:
        30:66:94:f1:da:c1:6c:3f:5e:10:92:92:a3:0c:7e:e8:8b:26:
        11:1c:d7:68:c9:31:79:b3:a4:d5:63:00:68:c3:e3:86:2d:09:
        92:4b:2d:63:7d:b8:03:a4:4c:60:b4:2c:12:d5:0b:9f:16:28:
        ea:88:2f:bb:1c:19:0b:0f:40:3d:67:e8:0b:fa:c6:e3:39:44:
        b2:bd:8a:3f:21:dd:aa:ec:a3:8c:48:dd:4c:99:43:86:d7:48:
        81:6b:e5:b9:bb:59:9f:1c:0f:3f:11:f7:7c:4b:67:a8:95:c2:
        7c:cb:3b:66:b0:79:a6:55:6f:6d:b0:29:8a:5e:7b:ee:30:68:
        f3:dd:41:29:91:f6:79:71:ae:8d:21:70:78:1d:5d:d2:f7:cf:
        e7:42:38:d1:8c:52:a6:a6:f6:b1:38:b1:2b:23:81:e1:1f:21:
        6d:99:3f:10:eb:b1:a9:73:b8:3e:31:99:cc:dd:2b:df:58:27:
        db:0b:5a:29:99:8f:b1:9f:e9:31:42:d0:26:db:53:b7:7e:30:
        41:95:c3:f0:07:83:bb:b0:63:b5:16:48:f2:a6:60:2f:32:5d:
        22:a1:da:76:4e:37:26:53:0d:95:7b:2d:b9:05:2f:93:2b:d4:
        df:c1:02:5b:f7:a5:a2:4f:11:5c:80:f4:f0:bd:c7:ea:3c:db:
        6f:e2:eb:6c:7f:c3:58:d9:31:77:4b:4d:f7:ce:bb:d6:c8:64:
        a3:01:d5:f9:a4:8d:e8:f0:ee:09:06:2c:0b:3c:ac:0a:57:d8:
        e4:81:79:ea:4a:bd:51:03:88:4c:d0:4c:0b:c4:0c:7e:2d:e7:
        df:1b:67:62:c0:d1:9c:ad:bb:d3:f0:75:dd:83:aa:70:99:2c:
        19:78:3d:26:2b:47:6f:24:c1:60:02:1e:4b:75:04:91:1f:08:
        1c:b3:79:a0:9b:db:fb:5d:3f:c7:e3:09:1f:41:3e:64:bb:ad:
        19:3d:35:e1:a6:f4:69:0b:a2:04:37:42:95:c6:c7:e5:f4:56:
        0e:67:5b:78:34:bb:07:f1:8f:e7:73:5b:87:d7:df:c9:2d:8d:
        8c:42:76:87:15:85:4b:23:03:20:34:e1:1b:f6:0c:1e:84:53:
        d9:1b:4e:d9:31:43:38:3b:88:12:84:d8:2a:38:b1:ce:0f:c7:
        07:d4:63:2d:97:89:1c:b3:44:99:eb:d4:df:32:74:be:0d:63:
        11:22:fd:fa:8e:e2:0b:56:12:56:0c:46:16:ad:44:10:26:98:
        dc:cf:c9:95:67:3e:11:c1:76:fa:b8:12:ea:96:f6:d9:91:ac:
        bf:49:b9:1c:8e:15:05:53:ac:9e:04:d2:5b:b8:87:bf:81:50:
        f7:02:a4:c0:9c:18:0f:45:ac:7a:82:cf:46:15:42:40:09:32:
        89:a5:ea:90:a5:99:68:f9:93:0c:7b:d6:7a:a8:e9:51:e2:90:
        9e:b9:ed:21:db:d9:7e:de:dc:62:6b:44:6b:9f:81:c5:77:39:
        8e:1d:78:30:de:dc:53:80:e0:c3:fa:fa:94:68:28:91:98:86:
        ff:86:04:a9:bd:58:7c:31:37:1f:db:9a:29:f3:c1:48:10:20:
        71:5f:fc:35:13:eb:7b:12:e2:7d:1c:cc:97:fe:8f:5c:a2:dd:
        f6:d2:a3:b2:ea:51:b3:ef:b1:1e:79:0b:00:53:f4:f2:52:75:
        5a:d7:17:c5:31:a0:54:4e:2b:28:2c:4f:6b:7a:27:3a:2c:04:
        da:b3:1d:04:4e:a4:4e:94:5c:a8:91:70:ab:c0:4b:75:9f:b3:
        6a:a9:4e:8a:22:e9:7f:fd:ec:53:e7:6a:6d:32:0b:8b:ab:4c:
        e7:7d:72:ec:04:62:1c:1a:45:1e:33:8e:37:ae:6a:2f:c8:fb:
        f3:69:ed:11:01:f3:f4:57:e9:29:d5:3b:0c:9c:0c:c4:cb:c3:
        38:5c:01:e7:d6:31:c3:d8:ce:24:d7:be:71:9b:c8:96:13:ca:
        5c:5d:e4:92:40:af:86:a0:4b:ff:a7:55:39:70:fd:ac:0a:e1:
        87:c7:01:4b:c3:41:36:c6:c6:33:8f:4f:25:4a:8d:70:92:ac:
        7c:95:cc:49:a9:dc:d6:6a:67:52:a5:5b:7f:2f:bb:91:e3:be:
        d6:28:fc:22:d0:72:66:e8:09:73:a7:23:c6:a6:89:38:0b:e5:
        d0:b3:f1:40:38:9c:4d:17:96:11:17:44:ef:e3:94:51:91:4c:
        5d:fe:d9:ed:c3:76:a0:2d:3b:dc:8d:b9:31:15:f6:75:58:74:
        2f:57:b4:29:21:29:6d:5f:eb:06:71:0a:f4:db:ff:c6:2f:16:
        73:a7:76:6b:d0:5b:a7:21:5c:fd:f0:11:e8:6f:9b:d0:c9:c9:
        fe:35:76:4a:4a:63:9b:ba:48:ac:af:4f:91:67:9c:5c:47:d8:
        e3:2d:03:12:5e:f1:cb:56:34:75:69:95:ad:68:96:6c:e7:4a:
        91:72:fb:9b:ba:e8:92:56:fb:9a:5b:5d:3b:9d:d3:c5:c4:52:
        42:1b:f9:4a:47:42:dd:77:49:da:2b:bd:d7:94:5f:7b:b8:64:
        b9:06:32:7c:ea:d1:36:f6:95:b8:57:41:1b:6e:66:31:2c:ee:
```

```
                 87:7a:5c:19:2f:d8:95:4a:16:93:48:f3:97:25:3d:24:61:1e:
                 d0:63:37:ee:3a:c9:a3:46:c5:94:a0:7e:24:cc:7f:72:8d:14:
                 9e:3c:33:ec:cd:9a:dd:b5:08:90:98:19:95:85:38:ff:ff:d2:
                 1e:bf:a6:c4:97:13:2b:3d:47:e9:57:59:d3:7d:99:01:6e:53:
                 4d:c0:82:97:fb:89:d6:7c:b7:23:0e:7d:6e:23:88:53:06:8f:
                 16:ff:40:0a:1b:cd:d5:1e:91:01:3e:77:3a:5f:c1:57:3a:7b:
                 c6:d5:51:d7:e2:ec:89:12:6b:9d:03:e4:9d:bb:7d:4e:02:bf:
                 67:8d:03:ca:90:56:f0:9a:97:4b:02:2d:4c:31:89:82:76:97:
                 fe:2f:d5:0a:3d:ea:0d:38:6c:30:75:5f:ae:91:53:d7:45:64:
                 df:ba:0b:22:80:44:85:6d:0e:5c:29:7f:82:9e:54:a3:7a:95:
                 be:96:79:66:9d:5b:a2:d6:2e:47:c6:99:7d:2b:32:dc:f2:b6:
                 02:91:6d:63:d4:93:45:60:c4:42:71:10:9e:fb:90:2f:e6:75:
                 71:ce:78:70:c1:da:ff:e1:47:fe:79:2b:8e:9a:81:bf:dd:02:
                 e3:78:39:71:17:b3:23:14:11:9d:29:8e:21:a1:98:b0:ac:03:
                 5a:6c:9e:62:64:ef:4f:03:ca:37:a6:ed:e4:78:d5:0d:99:29:
                 f5:5c:61:e6:48:cb:97:0e:5e:f9:2c:f6:b6:c7:7c:0c:a4:f7:
                 1a:f7:67:b5:5c:03:bf:bf:7a:e2:4d:a2:9b:5d:5d:5f:51:d0:
                 d6:52:8f:2a:20:68:08:bb:f0:9c:05:0e:ef:b3:49:0c:2a:1d:
                 8f:f9:03:b7:61:09:71:88:7d:e2:8c:e4:b8:ac:98:1b:c3:80:
                 55:a1:6b:dd:13:a2:29:4f:93:93:d3:d5:01:31:3f:7b:39:0e:
                 3a:57:6c:eb:5c:6a:5f:1b:ad:97:bd:97:23:18:91:05:0e:2b:
                 b4:b1:11:ee:f8:58:c7:08:d0:de:a2:3e:ba:54:8d:3d:63:da:
                 91:50:3a:24:8d:19:18:23:2e:cf:30:8d:5d:e3:e7:02:93:fa:
                 c8:f8:ea:05:e6:eb:06:80:90:4d:15:58:3d:26:98:13:4b:b0:
                 ac:dd:90:2e:d0:e1:eb:71:32:83:5d:2a:a9:b9:b5:24:fc:e9:
                 ec:18:ca:c9:a1:05:59:3e:fa:af:ed:4e:86:b1:fe:40:47:9b:
                 42:77:af:9c:2b:a0:e2:3e:fd:51:ab:02:77:e8:f1:39:45:aa:
                 54:b6:14:d4:14:20:fc:36:81:e6:04:98:8a:a0:c0:8a:cf:ae:
                 f6:b5:dc:b7:eb:26:86:d3:cf:1c:38:65:54:04:b1:b5:09:48:
                 f5:2d:07:ba:f8:eb:49:bd:d9:b1:54:ea:ac:c2:0d:20:10:79:
                 c1:cb:e9:dc:2d:ff:55:50:4f:f6:05:02:78:31:33:6f:15:7e:
                 24:5a:66:23:70:b3:b2:0c:17:39:ce:15:38:c5:ff:60:16:38:
                 60:74:72:c9:70:d8:59:b7:80:7f:da:f6:67:3f:d0:ba:be:1b:
                 a1:87:da:92:2d:a3:6c:99:29:57:aa:cb:d1:8d:66:f1:2d:c9:
                 56:60:24:56:4b:19:9f:f5:65:84:89:86:7d:4d:8b:f8:5b:60:
                 dd:af:2d:66:76:6c:66:d9:c6:f5:39:25:6c:e5:7b:43:97:64:
                 5c:c5:20:1e:3d:b5:dc:92:b2:9c:d8:1b:1b:e0:bc:44:7b:9c:
                 95:c5:53:48:91:b2:a5:46:16:bf:50:af:a5:44:cc:54:78:3f:
                 ed:20:d8:2e:0b:41:3d:f1:04:9d:df:3c:4a:d7:81:04:ff:8c:
                 b7:79:f8:51:8d:b7:2e:ac:2c:54:e6:fc:43:76:8e:f9:be:8c:
                 b8:5c:ad:c4:13:af:b0:6e:3b:d1:82:57:1e:f5:52:84:ca:cc:
                 d2:68:f3:2d:04:ff:27:0a:e6:a2:fa:c0:a9:97:d6:64:45:18:
                 5c:6f:9e:c1:64:22:66:db:56:02:c3:a8:57:fc:87:1b:5c:43:
                 15:8e:58:fc:f2:00:0b:4f:6a:4b:a0:5c:da:f2:e5:1b:82:4a:
                 6b:ef:db:63:d7:7d:93:1d:2f:20:78:37:17:22:82:cd:6b:c1:
                 83:61:05:81:99:0c:25:29:d6:5f:22:bc:06:67:7d:67
```

```
-----BEGIN CERTIFICATE-----
MIILSDCCAW+gAwIBAgIUVH5kcCmeA8V6pVx40SeHjFQ1F10wCgYIKwYBBQUHBiIw
NTELMAkGA1UEBhMCRlIxDjAMBgNVBAcMBVBhcmlzMRYwFAYDVQQKDA1Cb2d1cyBY
TVNTIENBMB4XDTI0MDcxMDA4MjcyNFoXDTM0MDcwODA4MjcyNFowNTELMAkGA1UE
BhMCRlIxDjAMBgNVBAcMBVBhcmlzMRYwFAYDVQQKDA1Cb2d1cyBYTVNTIENBMFMw
CgYIKwYBBQUHBiIDRQAAAAABK+u/ZhTeb5ZbTSpQAHutXCKwE3lyAhSpX/yW4Jt4
jta+jBxwPNjdeLIaFEe+Hw10cj82dsLLGa0pkAuC3pt/36NjMGEwHQYDVR0OBBYE
FGLONaVHd/8hhy68LSfnjvQ1a8/YMB8GA1UdIwQYMBaAFGLONaVHd/8hhy68LSfn
jvQ1a8/YMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMAoGCCsGAQUF
```

```
BwYiA4IJxQAAAAAA5YiouHOtTZL4XIHFimNXaqc7VKq2BorZ8cILyCceS6LP4tpE
6ujyQKi5VJxJNhIk33St5SnvT9qIDSFdO2RjJ9CEtZV6MBg3zTQX3aydnkjbdAd5
hCFa8CbNIWR7dzNIWGebLLKFbczsMUsvUVU6heHKBBXObkc59ekxRUHtccZPlvWu
ZGq9ctCMFwKZEB0UNMrlR+P3ZpaWEdWXdnaD8YSltgBePmeXejLcyOtMKUZ3mdba
ReZ7jEVttSlr/ZiiiY0MMEL1C3yXxbEd4tpnqUiknin0YD9NHUiDgjjv+ssdhhGh
FZT71e5o+US5PVRw874XjdcuhS1c0KDFmVLMeeccGNluPQ9sBVEzKDXiAllfH+14
CsZi8H3+c5YDTLRC4wDC18vrURDEDGS4N/6F0I4RbaYWd7EeAdke8xCc3QG8OHVe
j1ieW2x7CkEIWTWpOoMZ4H2h9c+jHE4H4a0DlfLTi3kz+FIiUxseMpphP8R8mujV
tSjxhGXVwfxNFpOIk2nK+pSglU4jrh5g4Oi0v/8WlXEPMXS7vrha6ySVi5UoE83j
qWX39W6bqal6Bc6r8FRi2RL4oRpo368Vj4rfZyfJ7b3hgaaNmoTzkTbZiXSO74Tc
XAMaCOTX8HL8bYoBNJTl/whRG4Bf5wfYnyXkHcP45dCcUM9mcfnM98Cn0GYBtxeg
X2aXpP9irBygYw0wKOmQ1VmkSNgHhwJLP2gjpQTcs9dF9tyw7MaQphyh+H6EumN+
WmQUeFj1dcD14R29SVfAQAgHmX9DLuIl2O2jGuN48XivAklUNlmO03KlC1IyvRei
z+FHISg9urYk2Rj5RHM17SmkGLztaM1KmjTLGi+zX7pzmxjueqiSJWUlgQRjHCIr
uLqBIbz5nah4mHW87UrGt2/AkSTrHfld4ON4TgX2NA97QVRJIKIwZpTx2sFsP14Q
kpKjDH7oiyYRHNdoyTF5s6TVYwBow+OGLQmSSy1jfbgDpExgtCwS1QufFijqiC+7
HBkLD0A9Z+gL+sbjOUSyvYo/Id2q7KOMSN1MmUOG10iBa+W5u1mfHA8/Efd8S2eo
lcJ8yztmsHmmVW9tsCmKXnvuMGjz3UEpkfZ5ca6NIXB4HV3S98/nQjjRjFKmpvax
OLErI4HhHyFtmT8Q67Gpc7g+MZnM3SvfWCfbC1opmY+xn+kxQtAm21O3fjBBlcPw
B4O7sGO1FkjypmAvMl0iodp2TjcmUw2Vey25BS+TK9TfwQJb96WiTxFcgPTwvcfq
PNtv4utsf8NY2TF3S033zrvWyGSjAdX5pI3o8O4JBiwLPKwKV9jkgXnqSr1RA4hM
0EwLxAx+LeffG2diwNGcrbvT8HXdg6pwmSwZeD0mK0dvJMFgAh5LdQSRHwgcs3mg
m9v7XT/H4wkfQT5ku60ZPTXhpvRpC6IEN0KVxsfl9FYOZ1t4NLsH8Y/nc1uH19/J
LY2MQnaHFYVLIwMgNOEb9gwehFPZG07ZMUM4O4gShNgqOLHOD8cH1GMtl4kcs0SZ
69TfMnS+DWMRIv36juILVhJWDEYWrUQQJpjcz8mVZz4RwXb6uBLqlvbZkay/Sbkc
jhUFU6yeBNJbuIe/gVD3AqTAnBgPRax6gs9GFUJACTKJpeqQpZlo+ZMMe9Z6qOlR
4pCeue0h29l+3txia0Rrn4HFdzmOHXgw3txTgODD+vqUaCiRmIb/hgSpvVh8MTcf
25op88FIECBxX/w1E+t7EuJ9HMyX/o9cot320qOy6lGz77EeeQsAU/TyUnVa1xfF
MaBUTisoLE9reic6LATasx0ETqROlFyokXCrwEt1n7NqqU6KIul//exT52ptMguL
q0znfXLsBGIcGkUeM443rmovyPvzae0RAfP0V+kp1TsMnAzEy8M4XAHn1jHD2M4k
175xm8iWE8pcXeSSQK+GoEv/p1U5cP2sCuGHxwFLw0E2xsYzj08lSo1wkqx8lcxJ
qdzWamdSpVt/L7uR477WKPwi0HJm6AlzpyPGpok4C+XQs/FAOJxNF5YRF0Tv45RR
kUxd/tntw3agLTvcjbkxFfZ1WHQvV7QpISltX+sGcQr02//GLxZzp3Zr0FunIVz9
8BHob5vQycn+NXZKSmObukisr0+RZ5xcR9jjLQMSXvHLVjR1aZWtaJZs50qRcvub
uuiSVvuaW107ndPFxFJCG/lKR0Ldd0naK73XlF97uGS5BjJ86tE29pW4V0EbbmYx
LO6HelwZL9iVShaTSPOXJT0kYR7QYzfuOsmjRsWUoH4kzH9yjRSePDPszZrdtQiQ
mBmVhTj//9Iev6bElxMrPUfpV1nTfZkBblNNwIKX+4nWfLcjDn1uI4hTBo8W/0AK
G83VHpEBPnc6X8FXOnvG1VHX4uyJEmudA+Sdu31OAr9njQPKkFbwmpdLAi1MMYmC
dpf+L9UKPeoNOGwwdV+ukVPXRWTfugsigESFbQ5cKX+CnlSjepW+lnlmnVui1i5H
xpl9KzLc8rYCkW1j1JNFYMRCcRCe+5Av5nVxznhwwdr/4Uf+eSuOmoG/3QLjeDlx
F7MjFBGdKY4hoZiwrANabJ5iZO9PA8o3pu3keNUNmSn1XGHmSMuXDl75LPa2x3wM
pPca92e1XAO/v3riTaKbXV1fUdDWUo8qIGgIu/CcBQ7vs0kMKh2P+QO3YQlxiH3i
jOS4rJgbw4BVoWvdE6IpT5OT09UBMT97OQ46V2zrXGpfG62XvZcjGJEFDiu0sRHu
+FjHCNDeoj66VI09Y9qRUDokjRkYIy7PMI1d4+cCk/rI+OoF5usGgJBNFVg9JpgT
S7Cs3ZAu0OHrcTKDXSqpubUk/OnsGMrJoQVZPvqv7U6Gsf5AR5tCd6+cK6DiPv1R
qwJ36PE5RapUthTUFCD8NoHmBJiKoMCKz672tdy36yaG088cOGVUBLG1CUj1LQe6
+OtJvdmxVOqswg0gEHnBy+ncLf9VUE/2BQJ4MTNvFX4kWmYjcLOyDBc5zhU4xf9g
FjhgdHLJcNhZt4B/2vZnP9C6vhuhh9qSLaNsmSlXqsvRjWbxLclWYCRWSxmf9WWE
iYZ9TYv4W2Ddry1mdmxm2cb1OSVs5XtDl2RcxSAePbXckrKc2Bsb4LxEe5yVxVNI
kbKlRha/UK+lRMxUeD/tINguC0E98QSd3zxK14EE/4y3efhRjbcurCxU5vxDdo75
voy4XK3EE6+wbjvRglce9VKEyszSaPMtBP8nCuai+sCpl9ZkRRhcb57BZCJm21YC
w6hX/IcbXEMVjlj88gALT2pLoFza8uUbgkpr79tj132THS8geDcXIoLNa8GDYQWB
mQwlKdZfIrwGZ31n
-----END CERTIFICATE-----
```

Appendix C. XMSS^{MT} X.509 v3 Certificate Example

This section shows a self-signed X.509 v3 certificate using XMSS^{MT}.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5c:22:ad:8a:06:51:9e:67:02:6a:2d:43:3e:8b:c7:23:
            43:77:80:c8
        Signature Algorithm: xmssmt
        Issuer: C = FR, L = Paris, O = Bogus XMSSMT CA
        Validity
            Not Before: Jul 10 08:28:04 2024 GMT
            Not After : Jul  8 08:28:04 2034 GMT
        Subject: C = FR, L = Paris, O = Bogus XMSSMT CA
        Subject Public Key Info:
            Public Key Algorithm: xmssmt
                xmssmt public key:
                PQ key material:
                    00:00:00:01:4b:a7:89:11:6f:fc:1d:fb:d3:e7:71:
                    73:b8:a2:48:ef:53:b9:9d:1f:c6:8a:7c:be:4f:8a:
                    29:fa:41:fd:bd:da:20:7f:f6:3b:b0:c5:b8:a7:c2:
                    f2:5a:f2:26:14:eb:36:f0:26:2f:87:74:fb:0e:d5:
                    7e:17:a0:d1:4d:b6:cf:51
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                7C:7D:59:B8:95:61:D5:03:6A:1E:3D:F1:24:AB:1D:ED:
                04:CD:DB:5F
            X509v3 Authority Key Identifier:
                7C:7D:59:B8:95:61:D5:03:6A:1E:3D:F1:24:AB:1D:ED:
                04:CD:DB:5F
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: xmssmt
    Signature Value:
        00:00:00:57:c4:98:89:ff:d9:0a:8e:6e:6f:16:95:8c:ec:35:
        42:21:c2:ca:56:ed:f8:81:f1:b2:4f:2b:6d:73:f4:37:55:fc:
        f4:4e:15:eb:6b:90:de:34:fe:d6:96:70:94:8d:c1:e7:4a:32:
        49:30:3a:40:a4:67:d2:fb:da:f8:d8:a1:7a:48:22:1c:e3:98:
        bc:d0:68:85:29:c9:e5:f7:5c:56:d8:9c:80:be:68:ed:11:eb:
        39:0f:ef:cb:09:b2:28:30:a6:2b:05:bc:de:11:22:be:c4:dc:
        08:9a:3d:b4:49:37:1f:54:5e:5f:2d:93:62:b0:95:c5:5d:23:
        92:f3:55:40:78:19:00:56:9e:a2:f1:0e:4b:ae:75:d6:92:09:
        b1:79:ec:c9:18:67:19:09:86:83:74:5d:0a:06:ab:da:f0:af:
        02:97:4d:d7:73:06:8b:a2:84:c7:09:af:dd:8b:15:39:e4:30:
        9f:c9:00:25:a8:33:4d:de:e8:25:b6:35:0b:51:bf:7a:34:a7:
        e8:84:e8:fa:39:5b:aa:37:6e:95:89:ac:26:4a:4e:ca:be:29:
        08:4b:3c:28:a7:85:6a:ad:5a:d2:93:eb:12:e1:9a:87:1c:40:
        3b:cf:15:6c:43:4e:88:21:54:52:7e:0d:6d:17:29:8d:15:6f:
        ef:42:5a:a9:25:d0:97:80:61:31:22:a4:9f:25:17:51:ad:0b:
        a1:cb:93:b4:f5:a6:b0:22:1b:6d:50:64:2a:48:bd:05:16:88:
        00:e3:7b:56:d0:03:b3:7a:2d:6a:0b:f3:de:a2:8c:6e:81:80:
```

```
        2c:8f:e9:d8:78:ed:5b:99:c9:13:d1:b6:eb:78:c3:40:2b:a1:
        7a:84:0a:ba:12:87:5e:1d:38:24:22:8f:c0:a3:65:1c:1c:ce:
        2d:8e:e5:2f:1f:be:93:5c:fe:1c:cd:a8:9d:7e:7e:cf:18:e2:
        9c:c5:54:dc:62:61:74:23:55:64:66:21:96:4c:a7:2e:8a:94:
        a6:35:10:a5:e8:5e:6e:91:ac:a8:cb:ed:51:2b:66:45:03:f5:
        87:ed:4d:8c:4e:6d:54:80:a1:33:8a:84:9d:23:31:90:c6:05:
        11:a7:9d:bd:51:0a:73:47:bc:08:49:11:b3:98:ff:01:14:69:
        d7:c0:a0:0c:55:e4:5e:e2:fa:84:ac:27:b3:85:2c:99:71:52:
        9c:33:f8:9d:8c:d2:13:bc:6e:18:79:15:a7:02:ee:15:eb:27:
        d8:af:24:38:02:9c:ca:30:f3:e2:30:41:2f:62:a2:2c:a5:81:
        1b:71:6d:b1:94:bd:c6:3d:9e:5e:51:45:de:5b:f4:d7:e6:35:
        e7:d8:7c:d5:98:ec:7e:0e:f8:9d:c1:a7:7b:b3:65:b1:a1:4b:
        2d:ec:d9:12:45:6b:1f:0b:1c:6b:3b:0a:66:76:39:f4:cc:9b:
        e1:b7:17:f7:53:fc:c3:a6:18:f7:2e:45:52:b1:18:99:75:d1:
        69:bb:77:c8:1a:84:5f:06:b5:8b:cb:02:b0:b2:0f:bf:17:18:
        65:3d:a7:72:5b:71:9f:92:7e:3a:df:84:cc:65:5c:c4:5b:70:
        fd:cc:38:9e:12:6e:f9:ff:1f:02:fc:ca:f5:68:86:fc:ca:71:
        f1:3d:7b:32:b4:d4:c3:a2:20:16:3f:12:07:71:95:3b:d4:b1:
        1e:fc:8c:1f:34:8c:c8:ab:8c:bb:75:93:c1:1a:d2:85:3e:9a:
        e6:04:86:88:de:27:46:ca:f3:f7:f3:8e:54:18:ea:aa:ae:14:
        02:b1:4a:6a:e0:24:77:40:28:8d:37:27:9c:87:6a:81:09:d2:
        01:4d:20:7f:de:84:a8:80:8c:8e:63:82:be:66:df:87:30:5c:
        b8:71:0a:e9:91:68:71:6e:97:97:f0:27:4e:fa:ae:6a:85:ac:
        80:cd:38:48:49:c1:2b:9d:db:54:c5:f0:bf:fa:06:e8:96:3a:
        c0:95:f0:88:bd:8e:80:78:3d:dc:ad:5d:0a:56:dd:c7:80:9f:
        fc:64:58:4d:6d:27:f6:d7:1a:8c:b2:1c:09:ea:7d:4f:74:99:
        0d:4a:0c:b8:b0:ef:74:dd:6f:6f:dc:e5:83:e1:e3:c2:e8:58:
        17:b8:44:8a:2d:ec:df:54:f6:1f:67:a2:b3:c5:19:fb:b9:c7:
        1b:3c:ea:bd:2c:e1:43:65:d1:5a:17:dc:93:9d:c5:85:0c:55:
        34:13:49:15:92:e2:52:14:d1:81:aa:62:02:1a:ba:c9:b0:53:
        85:8e:7b:d1:4e:34:76:ac:79:d7:b3:48:92:bf:55:7e:2d:5c:
        cd:32:9b:c1:41:a7:a3:cd:b7:94:5c:96:1e:3e:27:4d:eb:f0:
        61:4b:a4:e3:3c:bb:69:85:37:e9:9c:98:f4:68:7a:61:77:8c:
        bd:b9:30:d6:f1:fd:69:78:3f:96:99:7b:69:39:90:b3:7c:b6:
        88:ed:cd:19:da:42:64:e5:32:4c:a2:30:f7:c4:e8:27:93:70:
        ed:fa:5e:ca:8e:7a:d1:13:af:15:b1:59:c9:9b:91:61:0b:06:
        d5:cc:2e:80:bb:49:93:dd:be:53:88:be:af:80:64:7c:5e:be:
        7b:8b:e7:5f:39:af:ab:67:42:6b:06:aa:ef:d6:69:af:a9:00:
        1f:a0:15:10:04:3e:db:93:b2:37:db:eb:85:59:43:a2:8d:8f:
        06:8c:cb:a2:1d:a8:3c:9f:f4:a4:7c:c8:cd:ff:f0:a8:79:0f:
        e7:d8:94:67:ec:17:3f:fa:6e:04:07:4f:bf:86:04:6c:fc:46:
        87:b5:10:85:a4:07:e8:af:a9:ec:5d:28:5c:80:8c:31:cc:c7:
        b3:81:17:0b:4b:7d:1c:9e:74:02:1e:ef:de:0d:1b:c1:c0:04:
        4d:46:fd:dc:0b:a4:c6:33:e6:85:0a:60:39:4d:0b:f9:49:44:
        33:e0:15:99:19:bf:c7:8a:c6:96:04:93:37:6b:5d:e8:be:73:
        d4:80:b8:81:0f:9a:91:44:cf:72:02:d3:c9:f8:e0:7d:d2:9b:
        2b:ff:eb:42:6e:38:7e:dc:cd:a7:90:c5:2c:2b:a0:23:37:b9:
        64:10:a6:27:68:47:c5:f1:e8:8d:41:c1:49:e8:35:48:ce:c8:
        08:4c:ad:f2:ad:5d:e9:62:eb:c9:3c:61:85:18:c6:34:73:fd:
        26:a4:f0:50:83:9b:64:54:aa:55:6c:d8:a2:21:81:ff:9c:27:
        39:1f:c3:a2:0e:e5:53:b1:d7:fa:1f:ef:29:8b:c2:90:98:ea:
        2e:dd:45:bf:c3:6c:a3:93:47:99:03:18:25:e8:a5:ee:2e:77:
        eb:7f:f4:49:49:59:98:c1:fc:ab:1e:ad:20:bd:f8:24:fd:21:
        1b:da:5a:07:55:c8:50:05:31:50:93:b2:f8:6e:db:73:4d:5f:
        34:aa:f3:34:83:90:f0:41:6d:c8:43:56:d1:75:07:f5:16:20:
        b3:99:b2:c7:34:25:c4:0e:74:5a:51:0f:7b:3b:7f:6a:a9:41:
        17:b5:47:62:2d:4f:b9:61:97:60:e9:ae:ca:ad:31:6e:4b:0a:
        47:9c:53:66:a3:4e:c3:96:7c:01:a0:8e:ae:83:45:42:e6:92:
                12:8e:97:6f:e8:a0:b7:7d:a6:74:24:aa:20:b0:fa:9e:98:e8:
                7c:b4:da:30:e9:94:08:96:b7:b9:53:4f:75:5f:0c:4d:82:e3:
                cf:6e:bc:fa:23:4f:fa:33:17:7c:98:b6:1e:47:89:3e:d9:a1:
                aa:42:19:25:ae:9e:3f:53:44:ac:91:96:d8:55:c3:40:1d:fa:
                ad:86:38:62:bd:27:2f:26:34:be:ad:9a:01:44:42:c8:54:a5:
                3a:e9:0a:ff:f8:41:6d:38:1e:e2:3d:08:3a:94:4f:1e:60:d0:
                b1:c2:8e:94:34:f0:30:3e:f0:91:25:ee:98:34:b4:8d:95:4e:
                cf:ed:1d:61:89:c9:59:10:68:f2:bc:2e:5c:bd:c0:0f:1d:9c:
                2f:7c:c0:27:25:14:9b:de:a3:74:64:28:14:2c:a2:b2:90:3a:
                a4:6a:50:e9:8e:ca:78:e5:b6:74:56:e0:92:69:7d:b4:2e:e0:
                e7:66:92:16:92:a0:c3:db:4f:d3:d0:57:4d:4a:28:ee:b7:cc:
                04:ef:17:d9:fc:01:bb:1e:b2:5b:02:3d:1f:5a:85:73:a1:81:
                96:b7:33:5d:79:e5:6b:c9:29:73:34:01:69:ea:57:f0:01:be:
                4e:f3:5c:f3:0a:a7:37:08:ad:18:9c:c7:4c:59:d0:5d:bb:01:
                f1:53:76:cb:cd:d9:84:5e:bc:22:11:76:01:d9:e3:af:17:03:
                01:ef:38:4c:ad:c1:7d:a9:c6:61:2b:ba:9c:81:95:86:af:bb:
                73:90:dc:d9:2f:d1:3f:95:6a:b9:46:0f:fb:84:64:7c:7d:86:
                65:aa:10:71:56:19:5f:60:52:7f:19:fa:d5:5a:e0:90:e4:b9:
                62:55:71:2a:61:f9:37:2f:5e:07:71:43:cf:06:ca:6a:d5:52:
                c8:33:e1:ad:b2:3e:a4:61:01:00:bc:55:5d:0a:f3:e6:4f:35:
                06:c4:a8:3f:4c:8b:9b:c9:41:4b:f4:c1:57:ee:3c:c0:44:68:
                52:5a:2d:b9:a7:f2:41:da:c4:8d:7d:db:40:b6:fc:47:63:5a:
                69:a1:c7:8c:cc:3f:af:51:94:37:95:58:82:79:d2:16:4a:bf:
                12:0b:59:a5:a5:11:71:e6:1c:63:3b:ea:f0:2f:10:e0:97:9a:
                a1:04:53:d0:72:f4:3c:77:3b:78:ee:b5:aa:6b:f5:bb:5c:e9:
                35:4f:69:65:87:29:24:ec:47:7b:78:5a:a7:c1:e5:f1:73:7d:
                4d:79:ef:ef:4e:75:87:db:8f:36:fd:50:3e:74:dc:17:d4:c3:
                3f:4f:82:24:51:1b:12:16:26:61:db:93:15:19:39:55:f5:05:
                2c:6e:85:dd:b2:cc:4f:c0:09:0a:76:46:d8:e4:f2:11:92:a1:
                e0:36:a8:25:c7:45:19:6c:98:eb:9a:fa:c1:ec:80:18:ce:d1:
                f8:c4:23:9a:f9:b8:1f:05:67:8e:45:cb:e6:ee:0b:fa:db:67:
                1f:62:2c:49:78:bb:55:98:1e:33:42:63:f2:db:ee:73:f7:60:
                80:6d:5f:9a:e8:8c:89:39:5b:b2:84:e2:c3:99:77:f3:5f:19:
                ec:b8:2b:ce:60:59:2c:66:06:f9:c1:43:b9:fd:94:35:9e:28:
                9d:a0:8e:fd:0d:c6:1a:bb:20:93:b0:63:6a:83:2f:0a:db:c2:
                b3:8e:b1:dd:f5:ab:19:09:53:7a:db:72:3f:1e:25:07:eb:1a:
                7d:21:da:88:22:e6:f0:ba:b3:15:6f:95:f3:72:d2:cb:6d:48:
                b8:ba:7b:aa:40:7f:81:fe:ba:15:c2:77:9d:86:58:bc:7d:89:
                2e:7b:3a:96:04:9f:f1:3a:50:48:5a:25:4d:91:b6:ed:de:f6:
                2e:4d:e5:77:11:6d:76:f4:23:5f:91:f0:0f:79:59:7a:f3:32:
                24:11:c4:88:30:21:26:3b:f1:79:0f:04:06:ad:82:6d:ea:58:
                4e:aa:4e:0a:7f:7b:5c:a5:ab:de:76:a9:a9:c7:d9:e3:eb:d6:
                84:80:02:ab:da:4c:5b:49:90:29:c5:cb:5b:1c:06:61:e8:9a:
                cf:a4:ea:9d:31:16:6a:21:3a:d9:22:25:b8:39:9d:4c:e3:86:
                76:a8:dd:d8:b4:db:88:f9:5e:61:c3:1d:87:df:a9:31:33:7a:
                b3:50:3e:f2:cd:ad:a0:9d:98:5f:6c:e2:f0:d8:27:b9:c2:37:
                7f:8d:b4:f8:84:13:5f:22:6d:9b:81:bd:1c:e5:75:ae:b5:95:
                d1:cb:d0:c6:e3:78:ec:8c:71:6d:8c:5d:40:79:7d:58:3d:5c:
                63:77:cc:2e:a2:63:a9:71:30:2f:59:2a:ec:82:b1:e5:b9:d6:
                bf:fb:21:e6:97:fc:70:45:9a:c7:e8:d2:81:73:b1:f5:bc:76:
                ca:b4:be:9f:39:b5:2d:f2:3e:c5:32:e3:ae:3c:fd:74:a1:36:
                5a:5c:4d:f6:de:d2:d5:66:61:74:88:2e:4b:69:7c:29:2f:e0:
                2a:d6:d8:93:99:41:bc:7b:7f:fc:c3:1c:84:ed:16:c0:08:78:
                fb:57:61:9e:83:7a:d1:e9:b7:ad:9a:85:1c:c3:ba:a3:e4:18:
                b6:00:f6:35:27:e2:27:1d:10:dc:44:1d:11:05:a2:db:df:0a:
                59:98:9c:f3:ca:3a:b3:26:2d:d1:c4:3c:fc:21:f3:3c:39:62:
                7f:f4:bd:91:74:ef:02:83:da:4a:22:40:60:9f:6a:9f:8b:8f:
                f1:e4:1e:99:d5:17:55:62:1c:60:01:7d:c7:41:db:19:9e:29:
```

```
         01:ba:a0:5f:41:f3:61:ed:9d:0c:9c:ef:32:8b:b0:8a:89:b1:
         e4:06:c9:2f:4d:42:2a:01:84:29:ac:f1:41:a0:a1:c9:b4:83:
         d9:87:1a:53:1f:7f:d4:85:12:2e:79:f3:2c:88:06:73:62:ee:
         16:bc:c7:8b:e7:09:96:ba:02:b5:56:ab:6f:c0:cf:76:64:62:
         0e:1e:b5:e4:69:42:4d:ed:56:96:d9:1d:8d:07:40:7a:c5:bd:
         d3:9f:43:07:e4:9d:b6:26:2b:33:6a:79:d9:8a:ec:ee:51:73:
         f1:91:b0:e8:90:42:db:11:55:57:1b:01:10:fc:11:ff:77:b4:
         09:01:6d:f8:8c:cf:72:16:df:09:12:09:bd:49:ef:33:b9:c5:
         8d:35:60:77:80:8f:ee:98:18:be:bb:3a:61:e9:5b:6a:09:b0:
         0a:1e:38:80:e9:71:46:77:a1:19:7a:c3:04:57:a5:77:e6:5a:
         01:77:d2:92:90:f6:99:50:87:3f:30:8a:37:3d:37:1e:6b:1d:
         a4:71:3c:6b:15:07:01:f6:3d:43:96:a3:f7:30:cf:08:2c:32:
         a3:ca:67:6e:59:da:51:2e:96:bc:97:41:4b:7c:5f:97:a3:cf:
         46:20:9e:64:96:08:f7:0c:03:4b:b4:83:09:db:6c:bb:94:23:
         4e:ff:7b:fb:2f:84:66:0a:96:f9:e1:58:ff:0d:3c:84:62:9c:
         6b:60:9f:7e:39:cf:33:f3:03:2f:c7:d0:8b:6f:f3:9a:62:cc:
         33:c4:bd:b4:fc:b8:80:9d:fe:9e:c2:f0:d0:9e:07:71:a8:f9:
         1f:a7:64:4d:63:f9:6b:ce:3e:44:0a:3f:05:58:90:0d:0c:20:
         7d:4e:c7:52:d0:e5:b7:61:d3:6a:52:08:37:91:15:3c:cf:41:
         ec:ef:88:56:dc:14:2a:12:55:cb:05:01:23:89:c0:fe:ca:de:
         40:d2:d0:96:a3:1f:07:4a:58:96:fa:b2:ef:78:96:f0:73:25:
         c8:2e:20:3b:d8:02:cf:e7:ca:b0:29:1a:25:7f:15:96:2d:fd:
         52:bb:29:c3:fc:bf:b1:7c:d8:0f:76:21:05:28:2e:89:d9:82:
         0e:cb:cd:03:1f:c3:71:b4:0f:75:52:e5:b4:93:8c:ac:ed:d5:
         30:5a:b9:33:84:fd:3c:da:dc:e6:84:6d:c2:66:be:93:ad:67:
         7f:db:d0:08:95:64:5a:2c:13:7f:e2:05:b5:dc:d0:bf:4d:6e:
         93:c2:3b:8c:3b:b1:5c:3a:28:e8:c3:96:ed:59:e2:62:52:8e:
         95:8d:b5:e1:c1:f2:34:5b:bf:5a:cc:f1:ee:ec:3d:6c:61:99:
         f2:c8:e4:05:5f:ea:d5:74:3c:ff:df:1b:20:bd:35:30:c0:27:
         f8:a4:6e:73:45:81:e2:b9:15:52:c7:a0:e7:c8:fd:7b:8e:f7:
         d2:0c:c4:e9:22:69:4e:70:62:c7:8a:a2:a6:61:7c:0b:5a:74:
         8d:0f:c0:e5:66:dc:18:7b:74:3b:72:ab:1a:53:b3:49:ef:50:
         aa:76:80:e7:11:53:90:ab:24:d1:2e:fc:66:41:cf:b3:cc:ae:
         ac:f9:eb:1e:19:f7:bc:54:00:16:da:b0:d4:2b:74:c7:35:fb:
         08:ff:67:14:83:5a:eb:6b:b7:b4:63:28:e2:b6:b8:d4:0c:13:
         6a:8c:bb:30:c1:fb:6c:42:df:23:c4:f0:be:25:df:2b:39:11:
         bb:82:c3:e7:f9:04:48:77:cf:d0:5e:3d:6e:19:7f:b3:c4:2f:
         c4:ec:51:5f:9d:c7:8f:88:9f:21:79:8d:a0:17:3e:17:73:b4:
         f5:a2:71:70:e6:99:c4:fd:4c:f2:63:64:23:22:c3:72:71:52:
         43:42:a5:90:e3:59:77:50:ff:a1:09:2e:c7:f6:7e:17:f2:a2:
         d6:7e:2c:75:f2:ab:9e:36:78:ab:57:be:c5:91:71:70:2c:ba:
         03:91:80:97:f4:9e:16:bc:fa:80:f4:22:2a:b5:75:15:57:d9:
         b0:92:9e:b1:35:db:26:96:77:28:9c:89:99:db:9b:55:d4:29:
         15:5f:54:8a:0d:58:a8:95:13:95:17:6c:6b:b0:2a:a3:fa:1a:
         ec:2e:b4:0e:08:ea:8f:e1:8c:59:cf:7d:60:00:f3:bf:b7:e4:
         5f:08:a6:02:ef:ce:d7:9c:8d:6f:56:d7:c9:35:e9:e5:cf:d2:
         f5:28:ca:e6:36:ef:c4:26:52:d5:4d:04:ec:50:73:87:dc:70:
         1f:1a:db:07:bf:4c:e9:ec:57:98:7f:bc:c8:31:9e:7e:e6:3a:
         b4:c4:77:93:39:56:57:67:05:84:8d:03:02:d9:bf:04:6b:fe:
         71:8a:be:b6:8a:ae:44:b0:dd:db:1f:6a:26:e5:50:d5:ff:03:
         81:d8:1b:9f:3f:a6:bc:1b:52:b5:49:93:b0:27:fd:59:d4:7d:
         69:e9:63:35:0b:9b:de:a1:d4:70:0c:08:41:4b:76:d6:cd:c8:
         65:8c:bb:9a:6e:e4:f1:e2:30:13:9d:a3:c7:67:16:0f:7d:bd:
         ac:dc:aa:9c:17:01:a6:27:14:fa:4a:c1:27:3f:07:7b:9f:2f:
         47:56:cc:f0:96:38:e9:58:7c:1f:6c:73:10:3c:11:68:2a:3c:
         5f:74:fe:37:ae:8b:e9:eb:c6:06:30:6f:62:3c:5c:6c:2d:c7:
         5b:24:6d:cc:75:3f:d7:d4:e6:72:64:8a:ad:03:67:ad:cd:cb:
         2d:7c:82:49:a9:ef:e8:b9:be:f2:6c:98:42:4e:26:46:04:58:
```

```
        a5:2b:c9:88:9b:a4:91:7f:22:09:12:52:2a:d1:4e:36:22:d8:
        53:bc:38:93:ad:11:19:c5:e7:c9:83:00:b4:b6:b0:ac:96:32:
        ca:d0:08:69:e4:d2:29:86:74:74:49:be:4a:b2:bf:f2:2f:c2:
        52:fd:15:3c:8d:07:12:3a:98:c7:49:67:81:1d:b1:5d:e8:f4:
        42:79:a0:f7:44:b8:95:9f:e1:37:41:5b:c9:b1:89:90:7b:66:
        96:eb:8e:dc:1b:d7:73:b2:eb:c1:42:41:e8:2d:28:ba:74:ea:
        7c:77:87:76:5b:36:10:3d:87:08:52:94:e6:60:95:c1:1b:c9:
        27:c1:42:aa:32:62:ed:ca:6f:04:4e:11:3a:3d:3d:e0:d8:3a:
        c0:ff:b9:9a:94:b1:79:f3:01:14:3a:99:34:59:8e:d9:ac:f1:
        a9:77:b5:2d:59:e1:29:96:1b:13:80:8b:10:94:3e:c2:51:db:
        c1:24:06:02:47:96:9b:ae:5d:25:34:af:4b:65:f3:8a:eb:65:
        7c:a5:5e:7c:a2:d6:1d:41:20:13:0b:5e:ea:67:b2:eb:bf:6c:
        44:fb:76:31:58:5e:d2:33:6d:6f:9c:3a:41:70:34:11:6f:99:
        8c:42:9d:d6:2b:14:79:b0:ac:d4:de:3a:b0:d8:d2:97:88:9a:
        17:68:3e:79:a8:b0:4a:d7:a7:3c:63:c5:29:c1:65:76:74:7e:
        c2:de:b8:49:ce:26:5f:d2:62:2d:0f:5c:cc:6c:53:c0:a4:75:
        05:52:d1:52:38:ae:72:17:7c:02:67:6b:76:38:e7:72:aa:38:
        70:5e:af:a2:98:c0:c1:7a:a0:6d:ec:90:51:8d:d5:99:8b:39:
        05:6a:eb:0c:87:37:5b:4b:00:91:2c:7d:8a:6d:c1:23:10:44:
        26:5a:47:f7:7f:8f:86:1c:c2:a7:9f:9e:48:f6:42:cd:d1:3c:
        d9:e8:95:de:00:3c:ec:db:a1:a3:c0:7f:f7:17:3b:4a:dc:d2:
        f5:d4:9b:12:19:0f:6d:13:38:72:06:21:eb:94:88:87:8f:a1:
        de:f6:d7:a0:88:aa:e3:47:bb:69:e8:30:59:82:d2:3a:6d:c7:
        26:95:92:a4:58:07:eb:db:a5:d1:bb:51:00:28:ef:6f:c8:ce:
        9c:0f:d9:8d:e0:b3:14:db:90:dd:f9:26:af:b0:88:48:ae:22:
        71:26:af:d5:e0:4d:5c:41:e6:0b:f2:5c:9b:bb:69:82:09:5a:
        58:63:b9:0c:8a:22:37:aa:a2:71:2a:a5:d9:a7:7b:9f:d5:f4:
        17:8d:bd:4e:de:08:6a:a4:20:ce:a6:85:c7:fa:05:c7:d8:03:
        77:0c:dd:40:32:11:43:2a:8c:50:22:4b:fa:a1:d1:f1:94:42:
        3f:d5:b8:a0:dd:01:71:6e:30:34:ff:a6:76:80:e6:c1:04:8b:
        f0:c3:38:14:98:ae:eb:fd:05:98:d1:96:7e:b4:bf:51:ce:aa:
        b4:66:71:30:9f:7a:45:b6:ed:d1:6e:8f:b0:6c:a5:f5:4f:ee:
        bc:ea:65:5e:24:43:73:4b:50:8e:c8:68:0f:23:48:ed:dd:ff:
        84:97:9b:31:0d:bb:2c:db:69:6b:0c:34:73:3e:ae:69:d2:f5:
        be:a8:99:be:7b:40:82:f4:fe:35:f5:3d:a3:b1:b4:e2:6c:79:
        b7:0b:29:ad:30:3d:56:9d:bc:24:e9:e6:a5:6d:cc:83:18:7b:
        d5:98:a3:5f:dd:71:72:29:71:45:8f:41:52:ce:86:99:5c:f1:
        40:0c:1e:b1:97:da:3a:14:4a:a7:02:48:d8:4e:63:12:99:da:
        28:e9:de:0d:17:90:3a:f5:da:9a:01:7c:15:12:bf:00:48:7d:
        63:8c:89:0b:b9:77:95:01:27:b2:33:73:4b:ab:a8:f3:24:ee:
        c1:d3:0c:a3:9e:26:fe:24:23:3b:82:b4:1a:5e:72:dc:9e:91:
        3a:7b:85:64:0d:30:2e:6b:55:53:7e:a2:4f:b7:10:e4:77:a1:
        01:4a:b2:d7:7f:1c:94:a6:a7:e5:66:e2:c7:e5:37:6d:89:2c:
        72:b1:53:cf:d6:67:0f:77:f8:bf:07:20:98:99:60:ef:2e:72:
        c0:72:9e:79:2a:ca:a2:f7:bc:82:db:53:f7:68:e3:ed:4f:38:
        64:83:1b:dd:a5:78:dc:db:08:a9:34:35:f6:f1:9c:76:85:5e:
        cd:59:a3:c8:89:50:5b:bd:a0:64:06:b4:d7:db:7a:e1:75:57:
        13:90:ce:05:4b:a0:f6:22:70:0b:78:a0:84:46:87:b4:a7:0d:
        88:c6:41:c5:93:cb:77:37:d1:af:37:48:b9:47:db:99:7a:98:
        36:82:cb:27:6a:9a:de:80:24:3a:29:eb:ab:bd:b0:40:0d:a6:
        50:e5:a4:72:a3:19:cb:f3:52:8e:2f:1d:10:ef:7d:0a:15:6c:
        49:08:53:55:84:85:5c:73:53:ce:3e:18:e5:04:92:a6:99:db:
        4d:7b:c7:a9:99:ce:aa:90:48:73:7a:61:f5:92:73:da:b4:26:
        74:a1:39:74:e3:82:f9:32:e0:08:ef:bc:2f:9f:6d:e1:da:3d:
        f0:a5:46:b6:17:95:b8:6b:13:7d:f3:a1:31:8d:b7:47:a0:45:
        aa:20:53:d6:f0:3c:eb:a2:e7:7a:26:8c:c6:c7:cb:0f:21:5a:
        df:46:06:c5:b2:2d:a5:3b:b7:01:fd:0f:55:1b:5e:58:00:70:
        94:a3:7f:48:8e:4a:67:a4:14:5d:e0:ba:b6:f9:9b:e7:de:61:
```

```
        d8:67:83:ac:b7:01:eb:62:c5:22:b8:48:3a:96:55:fb:1a:4a:
        c4:63:30:f3:78:05:a6:ab:0c:e7:33:a0:88:f7:e2:e3:4a:1b:
        fd:66:3c:14:be:ee:20:d1:32:95:db:97:ff:d9:c2:bc:7a:c8:
        e4:ba:24:c5:b2:2e:16:f8:53:af:b4:57:56:25:26:f5:36:48:
        eb:0c:20:f9:3b:73:ff:dd:bd:20:81:0c:f5:55:89:7d:46:1b:
        05:b6:25:df:96:99:ea:09:79:60:72:d8:37:92:a8:f1:75:a3:
        5c:6d:54:b7:f3:32:17:35:1a:2d:96:e5:5e:fc:cd:54:30:49:
        af:6f:1a:42:d9:98:52:72:73:74:72:b7:72:95:80:1d:31:5a:
        e4:83:b7:b6:d4:14:00:0b:59:ce:7c:bc:1d:72:24:ab:74:d6:
        2c:9c:20:b1:0a:78:6f:a9:76:8d:6c:37:02:35:bd:6f:99:ee:
        d1:45:36:f1:34:60:7a:12:57:27:68:05:26:14:75:3c:9f:0d:
        3e:b7:5d:b8:2a:6c:1d:a7:b0:41:c4:f4:3d:ae:8e:51:54:37:
        65:ad:0a:c9:28:a0:3f:04:ed:54:59:c4:9f:1d:3d:70:97:5f:
        f9:44:53:ff:15:9f:03:13:7b:41:6b:c0:f7:8f:a3:27:2b:03:
        39:37:8f:bd:91:65:4d:74:a9:9f:45:6a:a4:25:dc:4c:f9:7e:
        59:fc:4e:93:7c:89:8f:71:8e:a6:99:66:5e:6a:25:a4:c0:a6:
        fa:25:f7:68:5c:8a:02:f5:7b:49:cd:89:e1:77:78:95:1b:a9:
        21:78:6e:f4:7a:e2:04:e5:0e:21:52:bf:04:cd:0c:69:5d:d7:
        f2:57:71:9f:d8:01:e0:f3:10:cc:15:2d:fd:99:78:ff:dc:1f:
        8f:a9:31:0d:0f:9f:f4:2c:a1:3d:4f:b2:51:92:68:f0:ec:d8:
        5f:c4:55:a1:4c:c8:12:e9:05:7e:05:93:5f:f9:76:99:85:18:
        29:24:60:14:5d:b3:79:f9:4b:7c:e4:22:71:8a:c2:66:45:d2:
        41:14:5d:59:4c:0a:b5:2b:ab:bd:c6:50:f8:87:37:42:e6:d4:
        96:72:cf:45:f0:d4:bf:0d:c5:17:9f:f1:b9:12:5c:a8:74:89:
        9e:56:07:cf:8f:98:9a:da:d7:db:7f:c7:d0:3a:0a:14:cd:5a:
        66:0c:eb:02:76:a0:d4:56:e6:e8:be:a1:f0:c7:23:b3:4f:86:
        90:1a:5a:16:8e:07:0d:24:d1:ee:03:98:9f
```

```
-----BEGIN CERTIFICATE-----
MIIU6zCCAXOgAwIBAgIUXCKtigZRnmcCai1DPovHI0N3gMgwCgYIKwYBBQUHBiMw
NzELMAkGA1UEBhMCRlIxDjAMBgNVBAcMBVBhcmlzMRgwFgYDVQQKDA9Cb2d1cyBY
TVNTTVQgQ0EwHhcNMjQwNzEwMDgyODA0WhcNMzQwNzA4MDgyODA0WjA3MQswCQYD
VQQGEwJGUjEOMAwGA1UEBwwFUGFyaXMxGDAWBgNVBAoMD0JvZ3VzIFhNU1NNVCBD
QTBTMAoGCCsGAQUFBwYjA0UAAAAAAUuniRFv/B370+dxc7iiSO9TuZ0fxop8vk+K
KfpB/b3aIH/2O7DFuKfC8lryJhTrNvAmL4d0+w7Vfheg0U22z1GjYzBhMB0GA1Ud
DgQWBBR8fVm4lWHVA2oePfEkqx3tBM3bXzAfBgNVHSMEGDAWgBR8fVm4lWHVA2oe
PfEkqx3tBM3bXzAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAKBggr
BgEFBQcGIwOCE2QAAAAAV8SYif/ZCo5ubxaVjOw1QiHCylbt+IHxsk8rbXP0N1X8
9E4V62uQ3jT+1pZwlI3B50oySTA6QKRn0vva+NihekgiHOOYvNBohSnJ5fdcVtic
gL5o7RHrOQ/vywmyKDCmKwW83hEivsTcCJo9tEk3H1ReXy2TYrCVxV0jkvNVQHgZ
AFaeovEOS6511pIJsXnsyRhnGQmGg3RdCgar2vCvApdN13MGi6KExwmv3YsVOeQw
n8kAJagzTd7oJbY1C1G/ejSn6ITo+jlbqjdulYmsJkpOyr4pCEs8KKeFaq1a0pPr
EuGahxxAO88VbENOiCFUUn4NbRcpjRVv70JaqSXQl4BhMSKknyUXUa0LocuTtPWm
sCIbbVBkKki9BRaIAON7VtADs3otagvz3qKMboGALI/p2HjtW5nJE9G263jDQCuh
eoQKuhKHXh04JCKPwKNlHBzOLY7lLx++k1z+HM2onX5+zxjinMVU3GJhdCNVZGYh
lkynLoqUpjUQpehebpGsqMvtUStmRQP1h+1NjE5tVIChM4qEnSMxkMYFEaedvVEK
c0e8CEkRs5j/ARRp18CgDFXkXuL6hKwns4UsmXFSnDP4nYzSE7xuGHkVpwLuFesn
2K8kOAKcyjDz4jBBL2KiLKWBG3FtsZS9xj2eXlFF3lv01+Y159h81Zjsfg74ncGn
e7NlsaFLLezZEkVrHwscazsKZnY59Myb4bcX91P8w6YY9y5FUrEYmXXRabt3yBqE
Xwa1i8sCsLIPvxcYZT2ncltxn5J+Ot+EzGVcxFtw/cw4nhJu+f8fAvzK9WiG/Mpx
8T17MrTUw6IgFj8SB3GVO9SxHvyMHzSMyKuMu3WTwRrShT6a5gSGiN4nRsrz9/OO
VBjqqq4UArFKauAkd0AojTcnnIdqgQnSAU0gf96EqICMjmOCvmbfhzBcuHEK6ZFo
cW6Xl/AnTvquaoWsgM04SEnBK53bVMXwv/oG6JY6wJXwiL2OgHg93K1dClbdx4Cf
/GRYTW0n9tcajLIcCep9T3SZDUoMuLDvdN1vb9zlg+HjwuhYF7hEii3s31T2H2ei
s8UZ+7nHGzzqvSzhQ2XRWhfck53FhQxVNBNJFZLiUhTRgapiAhq6ybBThY570U40
dqx517NIkr9Vfi1czTKbwUGno823lFyWHj4nTevwYUuk4zy7aYU36ZyY9Gh6YXeM
```

```
vbkw1vH9aXg/lpl7aTmQs3y2iO3NGdpCZOUyTKIw98ToJ5Nw7fpeyo560ROvFbFZ
yZuRYQsG1cwugLtJk92+U4i+r4BkfF6+e4vnXzmvq2dCawaq79Zpr6kAH6AVEAQ+
25OyN9vrhVlDoo2PBozLoh2oPJ/0pHzIzf/wqHkP59iUZ+wXP/puBAdPv4YEbPxG
h7UQhaQH6K+p7F0oXICMMczHs4EXC0t9HJ50Ah7v3g0bwcAETUb93AukxjPmhQpg
OU0L+UlEM+AVmRm/x4rGlgSTN2td6L5z1IC4gQ+akUTPcgLTyfjgfdKbK//rQm44
ftzNp5DFLCugIze5ZBCmJ2hHxfHojUHBSeg1SM7ICEyt8q1d6WLryTxhhRjGNHP9
JqTwUIObZFSqVWzYoiGB/5wnOR/Dog7lU7HX+h/vKYvCkJjqLt1Fv8Nso5NHmQMY
Jeil7i5363/0SUlZmMH8qx6tIL34JP0hG9paB1XIUAUxUJOy+G7bc01fNKrzNIOQ
8EFtyENW0XUH9RYgs5myxzQlxA50WlEPezt/aqlBF7VHYi1PuWGXYOmuyq0xbksK
R5xTZqNOw5Z8AaCOroNFQuaSEo6Xb+igt32mdCSqILD6npjofLTaMOmUCJa3uVNP
dV8MTYLjz268+iNP+jMXfJi2HkeJPtmhqkIZJa6eP1NErJGW2FXDQB36rYY4Yr0n
LyY0vq2aAURCyFSlOukK//hBbTge4j0IOpRPHmDQscKOlDTwMD7wkSXumDS0jZVO
z+0dYYnJWRBo8rwuXL3ADx2cL3zAJyUUm96jdGQoFCyispA6pGpQ6Y7KeOW2dFbg
kml9tC7g52aSFpKgw9tP09BXTUoo7rfMBO8X2fwBux6yWwI9H1qFc6GBlrczXXnl
a8kpczQBaepX8AG+TvNc8wqnNwitGJzHTFnQXbsB8VN2y83ZhF68IhF2AdnjrxcD
Ae84TK3BfanGYSu6nIGVhq+7c5Dc2S/RP5VquUYP+4RkfH2GZaoQcVYZX2BSfxn6
1VrgkOS5YlVxKmH5Ny9eB3FDzwbKatVSyDPhrbI+pGEBALxVXQrz5k81BsSoP0yL
m8lBS/TBV+48wERoUlotuafyQdrEjX3bQLb8R2NaaaHHjMw/r1GUN5VYgnnSFkq/
EgtZpaURceYcYzvq8C8Q4JeaoQRT0HL0PHc7eO61qmv1u1zpNU9pZYcpJOxHe3ha
p8Hl8XN9TXnv7051h9uPNv1QPnTcF9TDP0+CJFEbEhYmYduTFRk5VfUFLG6F3bLM
T8AJCnZG2OTyEZKh4DaoJcdFGWyY65r6weyAGM7R+MQjmvm4HwVnjkXL5u4L+ttn
H2IsSXi7VZgeM0Jj8tvuc/dggG1fmuiMiTlbsoTiw5l3818Z7LgrzmBZLGYG+cFD
uf2UNZ4onaCO/Q3GGrsgk7BjaoMvCtvCs46x3fWrGQlTettyPx4lB+safSHaiCLm
8LqzFW+V83LSy21IuLp7qkB/gf66FcJ3nYZYvH2JLns6lgSf8TpQSFolTZG27d72
Lk3ldxFtdvQjX5HwD3lZevMyJBHEiDAhJjvxeQ8EBq2CbepYTqpOCn97XKWr3nap
qcfZ4+vWhIACq9pMW0mQKcXLWxwGYeiaz6TqnTEWaiE62SIluDmdTOOGdqjd2LTb
iPleYcMdh9+pMTN6s1A+8s2toJ2YX2zi8NgnucI3f420+IQTXyJtm4G9HOV1rrWV
0cvQxuN47IxxbYxdQHl9WD1cY3fMLqJjqXEwL1kq7IKx5bnWv/sh5pf8cEWax+jS
gXOx9bx2yrS+nzm1LfI+xTLjrjz9dKE2WlxN9t7S1WZhdIguS2l8KS/gKtbYk5lB
vHt//MMchO0WwAh4+1dhnoN60em3rZqFHMO6o+QYtgD2NSfiJx0Q3EQdEQWi298K
WZic88o6syYt0cQ8/CHzPDlif/S9kXTvAoPaSiJAYJ9qn4uP8eQemdUXVWIcYAF9
x0HbGZ4pAbqgX0HzYe2dDJzvMouwiomx5AbJL01CKgGEKazxQaChybSD2YcaUx9/
1IUSLnnzLIgGc2LuFrzHi+cJlroCtVarb8DPdmRiDh615GlCTe1WltkdjQdAesW9
059DB+SdtiYrM2p52Yrs7lFz8ZGw6JBC2xFVVxsBEPwR/3e0CQFt+IzPchbfCRIJ
vUnvM7nFjTVgd4CP7pgYvrs6YelbagmwCh44gOlxRnehGXrDBFeld+ZaAXfSkpD2
mVCHPzCKNz03HmsdpHE8axUHAfY9Q5aj9zDPCCwyo8pnblnaUS6WvJdBS3xfl6PP
RiCeZJYI9wwDS7SDCdtsu5QjTv97+y+EZgqW+eFY/w08hGKca2CffjnPM/MDL8fQ
i2/zmmLMM8S9tPy4gJ3+nsLw0J4Hcaj5H6dkTWP5a84+RAo/BViQDQwgfU7HUtDl
t2HTalIIN5EVPM9B7O+IVtwUKhJVywUBI4nA/sreQNLQlqMfB0pYlvqy73iW8HMl
yC4gO9gCz+fKsCkaJX8Vli39Urspw/y/sXzYD3YhBSguidmCDsvNAx/DcbQPdVLl
tJOMrO3VMFq5M4T9PNrc5oRtwma+k61nf9vQCJVkWiwTf+IFtdzQv01uk8I7jDux
XDoo6MOW7VniYlKOlY214cHyNFu/Wszx7uw9bGGZ8sjkBV/q1XQ8/98bIL01MMAn
+KRuc0WB4rkVUseg58j9e4730gzE6SJpTnBix4qipmF8C1p0jQ/A5WbcGHt0O3Kr
GlOzSe9QqnaA5xFTkKsk0S78ZkHPs8yurPnrHhn3vFQAFtqw1Ct0xzX7CP9nFINa
62u3tGMo4ra41AwTaoy7MMH7bELfI8TwviXfKzkRu4LD5/kESHfP0F49bhl/s8Qv
xOxRX53Hj4ifIXmNoBc+F3O09aJxcOaZxP1M8mNkIyLDcnFSQ0KlkONZd1D/oQku
x/Z+F/Ki1n4sdfKrnjZ4q1e+xZFxcCy6A5GAl/SeFrz6gPQiKrV1FVfZsJKesTXb
JpZ3KJyJmdubVdQpFV9Uig1YqJUTlRdsa7Aqo/oa7C60Dgjqj+GMWc99YADzv7fk
XwimAu/O15yNb1bXyTXp5c/S9SjK5jbvxCZS1U0E7FBzh9xwHxrbB79M6exXmH+8
yDGefuY6tMR3kzlWV2cFhI0DAtm/BGv+cYq+toquRLDd2x9qJuVQ1f8Dgdgbnz+m
vBtStUmTsCf9WdR9aeljNQub3qHUcAwIQUt21s3IZYy7mm7k8eIwE52jx2cWD329
rNyqnBcBpicU+krBJz8He58vR1bM8JY46Vh8H2xzEDwRaCo8X3T+N66L6evGBjBv
YjxcbC3HWyRtzHU/19TmcmSKrQNnrc3LLXyCSanv6Lm+8myYQk4mRgRYpSvJiJuk
kX8iCRJSKtFONiLYU7w4k60RGcXnyYMAtLawrJYyytAIaeTSKYZ0dEm+SrK/8i/C
Uv0VPI0HEjqYx0lngR2xXej0Qnmg90S4lZ/hN0FbybGJkHtmluuO3BvXc7LrwUJB
6C0ounTqfHeHdls2ED2HCFKU5mCVwRvJJ8FCqjJi7cpvBE4ROj094Ng6wP+5mpSx
efMBFDqZNFmO2azxqXe1LVnhKZYbE4CLEJQ+wlHbwSQGAkeWm65dJTSvS2Xziutl
fKVefKLWHUEgEwte6mey679sRPt2MVhe0jNtb5w6QXA0EW+ZjEKd1isUebCs1N46
```

```
sNjSl4iaF2g+eaiwStenPGPFKcFldnR+wt64Sc4mX9JiLQ9czGxTwKR1BVLRUjiu
chd8AmdrdjjncqO4cF6vopjAwXqgbeyQUY3VmYs5BWrrDIc3W0sAkSx9im3BIxBE
JlpH93+PhhzCp5+eSPZCzdE82eiV3gA87Nuho8B/9xc7StzS9dSbEhkPbRM4cgYh
65SIh4+h3vbXoIiq40e7aegwWYLSOm3HJpWSpFgH69ul0btRACjvb8jOnA/ZjeCz
FNuQ3fkmr7CISK4icSav1eBNXEHmC/Jcm7tpgglaWGO5DIoiN6qicSql2ad7n9X0
F429Tt4IaqQgzqaFx/oFx9gDdwzdQDIRQyqMUCJL+qHR8ZRCP9W4oN0BcW4wNP+m
doDmwQSL8MM4FJiu6/0FmNGWfrS/Uc6qtGZxMJ96Rbbt0W6PsGyl9U/uvOplXiRD
c0tQjshoDyNI7d3/hJebMQ27LNtpaww0cz6uadL1vqiZvntAgvT+NfU9o7G04mx5
twsprTA9Vp28JOnmpW3Mgxh71ZijX91xcilxRY9BUs6GmVzxQAwesZfaOhRKpwJI
2E5jEpnaKOneDReQOvXamgF8FRK/AEh9Y4yJC7l3lQEnsjNzS6uo8yTuwdMMo54m
/iQjO4K0Gl5y3J6ROnuFZA0wLmtVU36iT7cQ5HehAUqy138clKan5Wbix+U3bYks
crFTz9ZnD3f4vwcgmJlg7y5ywHKeeSrKove8gttT92jj7U84ZIMb3aV43NsIqTQ1
9vGcdoVezVmjyIlQW72gZAa019t64XVXE5DOBUug9iJwC3ighEaHtKcNiMZBxZPL
dzfRrzdIuUfbmXqYNoLLJ2qa3oAkOinrq72wQA2mUOWkcqMZy/NSji8dEO99ChVs
SQhTVYSFXHNTzj4Y5QSSppnbTXvHqZnOqpBIc3ph9ZJz2rQmdKE5dOOC+TLgCO+8
L59t4do98KVGtheVuGsTffOhMY23R6BFqiBT1vA866LneiaMxsfLDyFa30YGxbIt
pTu3Af0PVRteWABwlKN/SI5KZ6QUXeC6tvmb595h2GeDrLcB62LFIrhIOpZV+xpK
xGMw83gFpqsM5zOgiPfi40ob/WY8FL7uINEylduX/9nCvHrI5LokxbIuFvhTr7RX
ViUm9TZI6wwg+Ttz/929IIEM9VWJfUYbBbYl35aZ6gl5YHLYN5Ko8XWjXG1Ut/My
FzUaLZblXvzNVDBJr28aQtmYUnJzdHK3cpWAHTFa5IO3ttQUAAtZzny8HXIkq3TW
LJwgsQp4b6l2jWw3AjW9b5nu0UU28TRgehJXJ2gFJhR1PJ8NPrdduCpsHaewQcT0
Pa6OUVQ3Za0KySigPwTtVFnEnx09cJdf+URT/xWfAxN7QWvA94+jJysDOTePvZFl
TXSpn0VqpCXcTPl+WfxOk3yJj3GOpplmXmolpMCm+iX3aFyKAvV7Sc2J4Xd4lRup
IXhu9HriBOUOIVK/BM0MaV3X8ldxn9gB4PMQzBUt/Zl4/9wfj6kxDQ+f9CyhPU+y
UZJo8OzYX8RVoUzIEukFfgWTX/l2mYUYKSRgFF2zeflLfOQicYrCZkXSQRRdWUwK
tSurvcZQ+Ic3QubUlnLPRfDUvw3FF5/xuRJcqHSJnlYHz4+YmtrX23/H0DoKFM1a
ZgzrAnag1Fbm6L6h8Mcjs0+GkBpaFo4HDSTR7gOYnw==
-----END CERTIFICATE-----
```

Acknowledgments

Thanks to Russ Housley, Panos Kampanakis, Michael StJohns, and Corey Bonnell for their helpful suggestions and reviews.

This document uses a lot of text from similar documents, including: [SP800208], [RFC3279] and [RFC8410], as well as [RFC9708]. Thanks goes to the authors of those documents. "Copying always makes things easier and less error prone" [RFC8411].

Authors' Addresses

Daniel Van Geest
CryptoNext Security
Email: daniel.vangeest@cryptonext-security.com

Kaveh Bashiri
BSI
Email: kaveh.bashiri.ietf@gmail.com

Scott Fluhrer
Cisco Systems
Email: sfluhrer@cisco.com

Stefan-Lukas Gazdag
genua GmbH
Email: ietf@gazdag.de

Stavros Kousidis
BSI
Email: kousidis.ietf@gmail.com