Network Working Group
Internet-Draft
Intended status: Informational
Expires: 23 October 2025

M. Jenkins
A. Becker
NSA-CCSS

21 April 2025

Commercial National Security Algorithm Suite Certificate and Certificate Revocation List Profile
draft-jenkins-cnsa2-pkix-profile-02

Abstract

This document specifies a profile of X.509 v3 Certificates and X.509 v2 Certificate Revocation Lists (CRLs) for applications that use Commercial National Security Algorithm (CNSA) Suite published by the United States Government.

The profile applies to the capabilities, configuration, and operation of all components of US National Security Systems that employ such X.509 certificates. US National Security Systems are described in NIST Special Publication 800-59. It is also appropriate for all other US Government systems that process high-value information.

The profile is made publicly available for use by developers and operators of these and any other system deployments.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 October 2025.

Copyright Notice

Table of Contents

1. Introduction

This document specifies a base profile for X.509 v3 Certificates and X.509 v2 Certificate Revocation Lists (CRLs) for use by applications that support the United States National Security Agency's Commercial National Security Algorithm (CNSA) Suite [annccnsa]. The profile applies to the capabilities, configuration, and operation of all components of US National Security Systems that employ such X.509 certificates. US National Security Systems are described in NIST Special Publication 800-59 [SP80059]. The profile is also appropriate for all other US Government systems that process high-value information. It is made publicly available for use by developers and operators of these and any other system deployments.

This document does not define any cryptographic algorithm; instead, it defines a CNSA-compliant profile of "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280]. It applies to all CNSA Suite solutions that make use of X.509 v3 Certificates or X.509 v2 CRLs. The reader is assumed to have familiarity with RFC 5280. All MUST-level requirements of RFC 5280 apply throughout this profile and are generally not repeated here. In cases where a MUST-level requirement is repeated for emphasis, the text notes the requirement is "in adherence with RFC 5280". This profile contains changes that elevate some SHOULD-level options in RFC 5280 to MUST-level and also contains changes that elevate some MAY-level options in RFC 5280 to SHOULD-level or MUST-level. All options from RFC 5280 that are not listed in this profile remain at the requirement level of RFC 5280.

[EDNOTE: Need to address how prior CNSA guidance will be superseded.]

2. Terminology

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. The Commercial National Security Algorithm Suite

The National Security Agency (NSA) profiles commercial cryptographic algorithms and protocols as part of its mission to support secure, interoperable communications for US Government National Security Systems. To this end, it publishes guidance both to assist with transitioning the United States Government to new algorithms and to provide vendors, and the Internet community in general, with information concerning their proper use and configuration within the scope of US Government National Security Systems.

The Commercial National Security Algorithm (CNSA) Suite is the set of approved commercial algorithms that can be used by vendors and IT users to meet cybersecurity and interoperability requirements for NSS. The first suite of CNSA Suite algorithms, "Suite B", established a baseline for use of commercial algorithms to protect classified information. The next suite, "CNSA 1.0", served as a bridge between the original set and a fully post-quantum cryptographic capability. The current suite, "CNSA 2.0", establishes fully PQ protection [annccnsa].

Pursuant to the "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" [NSM-10], the National Institute for Standards and Technology (NIST) has standardized several post-quantum asymmetric algorithms. From these, NSA has selected two: ML-DSA-87 [FIPS204], a standardized version of CRYSTALS-Dilithium, for signing; and ML-KEM-1024 [FIPS203], a standardized version of CRYSTALS-Kyber, for key management. With SHA384 (or SHA512), AES-256, and LMS/XMSS, these comprise the CNSA Suite 2.0.

The NSA is authoring a set of RFCs, including this one, to provide updated guidance for using CNSA 2.0 algorithms in certain IETF protocols. These RFCs can be used in conjunction with other RFCs and cryptographic guidance (e.g., NIST Special Publications) to properly protect Internet traffic and data-at-rest for US Government National Security Systems.

4. General Requirements

The goal of this document is to define a base set of requirements for certificates and CRLs to support interoperability among CNSA Suite solutions. Specific communities, such as those associated with US National Security Systems, may define community profiles that further restrict certificate and CRL contents by mandating the presence of extensions that are optional in this base profile, defining new optional or critical extension types, or restricting the values and/or presence of fields within existing extensions. However, communications between distinct communities MUST conform with the requirements specified in this document when interoperability is desired. Applications may add requirements for additional non-critical extensions, but they MUST NOT assume that a remote peer will be able to process them.

Every CNSA Suite certificate MUST use the X.509 v3 format and contain one of the following:

* A ML-DSA-87 signature verification key.

* A ML-KEM-1024 public encapsulation key.

The signature applied to all CNSA Suite certificates and CRLs MUST be made with a ML-DSA-87 signing key. The ML-DSA algorithm incorporates an internal hashing function, so there is no need to apply hashing algorithm before signing (aka "pre-hashing"). Where an application or implementation make it more efficient to pre-hash, then the External-mu mechanism allowed by FIPS 204 and described in Section 8 of I-D.ietf-lamps-dilithium-certificates may be used. Any other hashing outside of ML-DSA or ML-KEM SHOULD use SHA-384 or MAY use SHA-512. No other hashing algorithms comply with CNSA 2.0.

The reader is also assumed to have familiarity with these documents:

* draft-ietf-lamps-dilithium-certificates [I-D.ietf-lamps-dilithium-certificates] for the algorithm identifier, and the syntax and semantics for the Subject Public Key Information field in certificates that support ML-DSA-87 and

* draft-ietf-lamps-kyber-certificates [I-D.ietf-lamps-kyber-certificates] for the algorithm identifier, and the syntax and semantics for the Subject Public Key Information field in certificates that support ML-KEM-1024.

[EDNOTE: Any requirements regarding the External-mu mechanism will appear here in a subesequent version. We expect to use the same identifier for ML-DSA whether or not the External-mu mechanism is used.]

5. CNSA Suite Object Identifiers

The object identifiers for use of CNSA 2.0 Suite in certificates and crls are defined in [list of RFCs including draft-ietf-lamps-dilithium-certificates, draft-ietf-lamps-kyber-certificates]. These OIDs are used to identify both the algorithm associated with the public key (as part of the Subject Public Key Info field), and the signature on a certificate or crl (as part of the signatureAlgorithm field in a Certificate or CertificateList and part of the signature field in a TBSCertificate and TBSCertList). They are repeated here for convenience:

```
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) 19 }

id-alg-ml-kem-1024 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
   country(16) us(840) organization(1) gov(101) csor(3)
   nistAlgorithm(4) kems(4) 3 }
```

6. CNSA Suite Base Certificate Required Values

This section specifies changes to the basic requirements in [RFC5280] for applications that create or use CNSA Suite certificates. Note that RFC 5280 has varying mandates for marking extensions as critical or non-critical. This profile changes some of those mandates for extensions that are included in CNSA Suite certificates.

6.1. signature and signatureAlgorithm

ML-DSA-87 is indicated by the id-ML-DSA-87 OID in the AlgorithmIdentifier of the signature field in a TBSCertificate and TBSCertList, and of the signatureAlgorithm field in a Certificate and CertificateList.

The parameters MUST be absent in all AlgorithmIdentifiers.

6.2. signatureValue

ML-DSA digital signature generation is described in [FIPS204]. It is converted from a byte string to a DER encoded BIT STRING in the signatureValue field of a Certificate or CertificateList.

6.3. version

For this profile, version MUST be ’v3’, with INTEGER value 2.

6.4. subjectPublicKeyInfo

For ML-DSA-87 signature verification keys, the algorithm ID id-ML-DSA-87 MUST be used.

For ML-KEM-1024 key management keys, the algorithm ID id-alg-ml-kem-1024 MUST be used.

In either case, the parameters of the AlgorithmIdentifier in this field MUST be absent.

7. Certificate Extensions for Particular Types of Certificates

Different types of certificates in this profile have different required and recommended extensions. Those are listed in this section. Those extensions from RFC 5280 not explicitly listed in this profile remain at the requirement levels of RFC 5280.

7.1. CNSA Suite Self-Signed CA Certificates

In adherence with [RFC5280], self-signed CA certificates in this profile MUST contain the subjectKeyIdentifier, keyUsage, and basicConstraints extensions.

The keyUsage extension MUST be marked as critical. The keyCertSign and cRLSign bits MUST be set. The digitalSignature and nonRepudiation bits MAY be set. All other bits MUST NOT be set.

In adherence with [RFC5280], the basicConstraints extension MUST be marked as critical. The cA boolean MUST be set to indicate that the subject is a CA, and the pathLenConstraint MUST NOT be present.

7.2. CNSA Suite Non-Self-Signed CA Certificates

Non-self-signed CA Certificates in this profile MUST contain the authorityKeyIdentifier, keyUsage, and basicConstraints extensions. If there is a policy to be asserted, then the certificatePolicies extension MUST be included.

The keyUsage extension MUST be marked as critical. The keyCertSign and CRLSign bits MUST be set. The digitalSignature and nonRepudiation bits MAY be set. All other bits MUST NOT be set.

In adherence with [RFC5280], the basicConstraints extension MUST be marked as critical. The cA boolean MUST be set to indicate that the subject is a CA, and the pathLenConstraint subfield is OPTIONAL.

If a policy is asserted, the certificatePolicies extension MUST be marked as non-critical, MUST contain the OIDs for the applicable certificate policies, and SHOULD NOT use the policyQualifiers option. If a policy is not asserted, the certificatePolicies extension MUST be omitted.

Relying party applications conforming to this profile MUST be prepared to process the policyMappings, policyConstraints, and inhibitAnyPolicy extensions, regardless of criticality, following the guidance in [RFC5280] when they appear in non-self-signed CA certificates.

7.3. CNSA Suite End-Entity Signature and Key Establishment Certificates

In adherence with [RFC5280], end-entity certificates in this profile MUST contain the authorityKeyIdentifier and keyUsage extensions. If there is a policy to be asserted, then the certificatePolicies extension MUST be included. End-entity certificates SHOULD contain the subjectKeyIdentifier extension.

The keyUsage extension MUST be marked as critical.

For end-entity digital signature certificates, the keyUsage extension MUST be set for digitalSignature. The nonRepudiation bit MAY be set. All other bits in the keyUsage extension MUST NOT be set.

For end-entity key establishment certificates, the keyUsage extension MUST be set for keyEncipherment. The encipherOnly or decipherOnly bit MAY be set. All other bits in the keyUsage extension MUST NOT be set.

If a policy is asserted, the certificatePolicies extension MUST be marked as non-critical, MUST contain the OIDs for the applicable certificate policies, and SHOULD NOT use the policyQualifiers option. If a policy is not asserted, the certificatePolicies extension MUST be omitted.

8. CNSA Suite CRL Requirements

This CNSA Suite CRL profile is a profile of [RFC5280]. There are changes in the requirements from [RFC5280] for the signatures on CRLs of this profile.

The signatures on CRLs in this profile MUST follow the same rules from this profile that apply to signatures in the certificates. See Section 4.

9. Requirements for Other Revocation Notification Methods

Revocation notification methods of any type must enable authentication of the issuing CA as the source of the revocation information. Specifically, an OCSP response MUST be signed conformant with Section 4, and with a key that binds the response to the issuing CA.

10. Security Considerations

This document introduces no security considerations beyond those in [RFC5280], of which it is a profile.

11. IANA Considerations

This document has no IANA actions.

12. References

12.1. Normative References

[annccnsa] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", September 1984, <https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF>.

[FIPS203] National Institute of Standards and Technology, "Module-Lattice-Based Key Establishment Mechanism Standard", Federal Information Processing Standard 203, DOI 10.6028/NIST.FIPS.203.ipd, August 2023, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf>.

[FIPS204] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard", Federal Information Processing Standard 204, DOI 10.6028/NIST.FIPS.204.ipd, August 2023, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf>.

[I-D.ietf-lamps-dilithium-certificates] Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-07, 2 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-07>.

[I-D.ietf-lamps-kyber-certificates] Turner, S., Kampanakis, P., Massimo, J., and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)", Work in Progress, Internet-Draft, draft-ietf-lamps-kyber-certificates-10, 16 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-kyber-certificates-10>.

[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>.

[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>.

[RFC8603] Jenkins, M. and L. Zieglar, "Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile", RFC 8603, DOI 10.17487/RFC8603, May 2019, <https://www.rfc-editor.org/info/rfc8603>.

12.2. Informative References

[NSM-10] United States, The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems", NSM 10, May 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>.

[SP80059] National Institute of Standards and Technology, "Guideline for Identifying an Information System as a National Security System", Special Publication 59, DOI 10.6028/NIST.SP.800-59, August 2003, <https://csrc.nist.gov/publications/detail/sp/800-59/final>.

Authors' Addresses

Michael Jenkins
NSA Center for Cybersecurity Standards
Email: mjjenki@cyber.nsa.gov

Alison Becker
NSA Center for Cybersecurity Standards
Email: aebecke@uwe.nsa.gov