Independent Submission
Request for Comments: 9152
Category: Informational
ISSN: 2070-1721

M. Jenkins
NSA
S. Turner
sn3rd

April 2022

Secure Object Delivery Protocol (SODP) Server Interfaces: NSA's Profile for Delivery of Certificates, Certificate Revocation Lists (CRLs), and Symmetric Keys to Clients

Abstract

This document specifies protocol interfaces profiled by the United States National Security Agency (NSA) for National Security System (NSS) servers that provide public key certificates, Certificate Revocation Lists (CRLs), and symmetric keys to NSS clients. Servers that support these interfaces are referred to as Secure Object Delivery Protocol (SODP) servers. The intended audience for this profile comprises developers of client devices that will obtain key management services from NSA-operated SODP servers. Interfaces supported by SODP servers include Enrollment over Secure Transport (EST) and its extensions as well as Certificate Management over CMS (CMC).

This profile applies to the capabilities, configuration, and operation of all components of US National Security Systems (SP 800-59). It is also appropriate for 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.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see 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/rfc9152.

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction

This document specifies protocol interfaces profiled by the United States National Security Agency (NSA) for National Security System (NSS) servers that provide public key certificates, Certificate Revocation Lists (CRLs), and symmetric keys to NSS clients. Servers that support these interfaces are referred to as Secure Object Delivery Protocol (SODP) servers. The purpose of this document is to

indicate options from, and requirements in addition to, the base specifications listed in Section 1.1 that are necessary for client interoperability with NSA-operated SODP servers. Clients are always devices and need not implement all of the interfaces specified herein; clients are free to choose which interfaces to implement based on their operational requirements. Interfaces supported by SODP servers include:

* Enrollment over Secure Transport (EST) [RFC7030] and its extensions [RFC8295], and

* Certificate Management over CMS (CMC) [RFC5274] [RFC6402] for both Simple Public Key Infrastructure (PKI) requests and responses (i.e., PKCS#10 requests and PKCS#7 responses) and Full PKI requests and responses.

This profile applies to the capabilities, configuration, and operation of all components of US National Security Systems [SP-800-59]. It is also appropriate for 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 profile conforms to the existing requirements of the NSA's Commercial National Security Algorithms (CNSAs). As operational needs evolve over time, this profile will be updated to incorporate new commercial algorithms and protocols as they are developed and approved for use.

1.1. Documents to be Familiar With

Familiarity with the follow specifications is assumed:

* EST and EST extensions: [RFC7030] and [RFC8295]

* PKI-related specifications: [RFC2986], [RFC3739], [RFC5274], [RFC5280], [RFC5912], [RFC5913], [RFC5916], [RFC5917], [RFC6010], and [RFC6402]

* Key-format-related specifications: [RFC5915], [RFC5958], [RFC5959], [RFC6031], [RFC6032], [RFC6160], [RFC6161], [RFC6162], [RFC7191], [RFC7192], [RFC7292], and [RFC7906]

* CMS-related (Cryptographic Message Syntax) documents: [RFC5652] and [RFC6268]

* CNSA-related documents: [RFC8603], [RFC8755], [RFC8756], and [RFC9151]

The requirements from RFCs apply throughout this profile and are generally not repeated here. This document is purposely written without using the requirements language described in [RFC2119] and [RFC8174].

1.2. Document Organization

The document is organized as follows:

* The remainder of this section describes the operational environment used by clients to retrieve secure objects.

* Section 2 specifies the Abstract Syntax Notation One (ASN.1) version used.

* Section 3 specifies SODP's EST interface.

* Section 4 specifies SODP's CMC interfaces.

* Sections 5-7 specify Trust Anchor (TA), Certification Authority (CA), and End-Entity (EE) certificates, respectively.

* Sections 8 and 9 specify Relying Party Applications and CRL Profile, respectively.

1.3. Environment

Clients obtain secure "objects" or "packages" from the client-server-based environment. Objects/packages vary based on the Source of Authority (SOA), but all objects are "secured" minimally through the use of one or more digital signatures and zero or more layers of encryption, as profiled in this document. An SOA is the authority for the creation of objects that the client will recognize as valid. An SOA can delegate its authority to other actors; delegation occurs through the issuance of certificates. An object or package is the generic term for certificates, certificate status information, and keys (both asymmetric and symmetric). All of the objects except for the certificates and certificate status information are directly encapsulated in and protected by CMS content types. CMS content types that provide security are referred to as "CMS-protecting content types". All others are simply referred to as "CMS content types". All secured objects are distributed either as CMS packages or as part of a CMS package.

In the example depicted in Figure 1, there are two SOAs: one for symmetric keys, as depicted by the Key Trust Anchor (KTA), and one for public key certificates, as depicted by the PKI Trust Anchor (TA). The KTA is responsible for the creation and distribution of symmetric keys. The KTA delegates the creation and distribution responsibilities to separate entities through the issuance of certificates to a Key Source Authority (KSA) and a Key Distribution Authority (KDA). The KSA generates the keys, digitally signs the keys, and encrypts the key for the end client using CMS content types for each step. The KDA distributes the KSA-generated and KSA-protected key to the client; the key may also be signed by the KDA. The resulting CMS package is provided to the client through the EST extension's /symmetrickey service. The PKI TA is responsible for the creation, distribution, and management of public key certificates. The PKI TA delegates these responsibilities to Certification Authorities (CAs), and CAs, in turn, are responsible for creating, distributing, and managing End-Entity (EE) certificates. CAs distribute PKI-related information through the /cacerts, /crls, /eecerts, /fullcmc, /simpleenroll, /simplereenroll, and /csrattrs EST

and EST extension services.

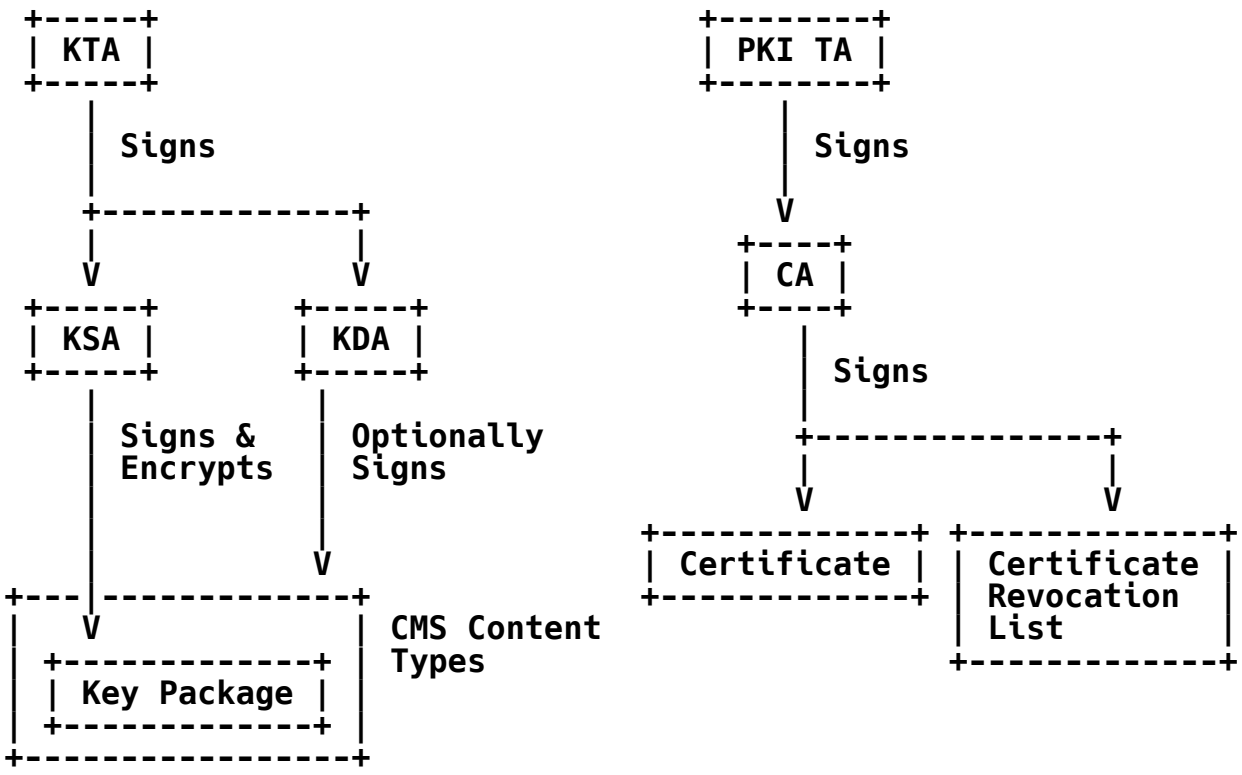

Figure 1: Operating Environment (Key and PKI Sources of Authority)

For clients that support the CMC interface and not the EST interface, the environment includes only the PKI TAs.

2. Abstract Syntax Notation One

Implementations of this specification use the 2002/2008 ASN.1 version; 2002/2008 ASN.1 modules can be found in [RFC5911], [RFC5912], and [RFC6268] (use [RFC6268] for the CMS syntax), while other specifications already include the 2002/2008 ASN.1 along with the 1988 ASN.1. See Section 1.1 of [RFC6268] for a discussion about the differences between the 2002 and 2008 ASN.1 versions.

3. EST Interface

Client options for EST [RFC7030] and EST extensions [RFC8295] are specified in this section.

3.1. Hypertext Transfer Protocol Layer

Clients that receive redirection responses (3xx status codes) will terminate the connection ([RFC7030], Section 3.2.1).

Per Section 2.2 of [RFC8295], clients indicate the format ("application/xml" or "application/json") of the PAL information ([RFC8295], Section 2.1.1) via the HTTP Accept header.

3.2. Transport Layer Security

TLS implementations are configured as specified in [RFC9151]; the notable exception is that only EC-based algorithms are used.

3.3. Eligibility

At the EST interface, servers only enroll clients that they have established a prior relationship with independently of the EST service. To accomplish this, client owners/operators interact in person with the human acting as the Registration Authority (RA) to ensure the information included in the transmitted certificate request, which is sometimes called a Certificate Signing Request (CSR), is associated with a client. The mechanism by which the owner/operator interacts with the RA as well as the information provided is beyond the scope of this document. The information exchanged by the owner/operator might be something as simple as the subject name included in the CSR to be sent or a copy of the certificate that will be used to verify the certificate request, which is provided out of band.

3.4. Authentication

Mutual authentication occurs via "Certificate TLS Authentication" ([RFC7030], Section 2.2.1). Clients provide their certificate to servers in the TLS Certificate message, which is sent in response to the server's TLS Certificate Request message. Both servers and clients reject all attempts to authenticate based on certificates that cannot be validated back to an installed TA.

3.5. Authorization

Clients always use an explicit TA database ([RFC7030], Section 3.6.1). At a minimum, clients support two TAs: one for the PKI and one for symmetric keys.

Clients check that the server's certificate includes the id-kp-cmcRA Extended Key Usage (EKU) value ([RFC6402], Section 2.10).

Clients that support processing of the CMS Content Constraints extension [RFC6010] ensure returned CMS content is from an SOA or an entity authorized by an SOA for that CMS content; see Section 7.1 for SOA certificates.

3.6. EST and EST Extensions

This section profiles SODP's interfaces for EST [RFC7030] and EST extensions [RFC8295].

3.6.1. /pal

The Package Availability List (PAL) is limited to 32 entries, where the 32nd PAL entry links to an additional PAL (i.e., PAL Package Type 0001).

The PAL is XML [XML].

3.6.2. /cacerts

The CA certificates located in the explicit TA database are distributed to the client when it is registered. This TA distribution mechanism is out of scope.

CA certificates provided through this service are as specified in Sections 5 and 6 of this document.

3.6.3. /simpleenroll

CSRs follow the specifications in Section 4.2 of [RFC8756], except that the CMC-specific ChangeSubjectName and the POP Link Witness V2 attributes do not apply. Only EC-based algorithms are used.

Client certificates provided through this service are as specified in Section 7 of this document.

The HTTP content type of "text/plain" ([RFC2046], Section 4.1) is used to return human-readable errors.

3.6.4. /simplereenroll

There are no additional requirements for requests beyond those specified in Sections 3.4 and 3.6.3 of this document.

The HTTP content type of "text/plain" ([RFC2046], Section 4.1) is used to return human-readable errors.

3.6.5. /fullcmc

Requests are as specified in [RFC8756] with the notable exception that only EC-based algorithms are used.

Additional attributes for returned CMS packages can be found in [RFC7906].

Certificates provided through this service are as specified in Section 7 of this document.

3.6.6. /serverkeygen

PKCS#12 [RFC7292] -- sometimes referred to as "PFX" (Personal Information Exchange) or "P12" -- is used to provide server-generated asymmetric private keys and the associated certificate to clients. This interface is a one-way interface as the RA requests these from the server.

PFXs [RFC7292] are exchanged using both password privacy mode and integrity password mode. The PRF algorithm for PBKDF2 (the KDF for PBES2 and PBMAC1) is HMAC-SHA-384, and the PBES2 encryption scheme is AES-256.

The HTTP content type of "text/plain" ([RFC2046], Section 4.1) is used to return human-readable errors.

/serverkeygen/return is not supported at this time.

3.6.7. /csrattrs

Clients use this service to retrieve partially filled PKIRequests with no public key or proof-of-possession signature, i.e., their values are set to zero length, either a zero length BIT STRING or OCTET STRING. The pKCS7PDU attribute, defined in [RFC2985], includes the partially filled PKIRequest as the only element in the CsrAttrs sequence. Even though the CsrAttrs syntax is defined as a set, there is only ever exactly one instance of values present.

3.6.8. /crls

CRLs provided through this service are as specified in Section 9 of this document.

3.6.9. /symmetrickeys

Clients that claim to support SODP interoperation will be able to process the following messages from an SODP server:

* additional encryption and origin authentication ([RFC8295], Section 5); and

* server-provided Symmetric Key Content Type [RFC6032] encapsulated in an Encrypted Key Content Type using the EnvelopedData choice [RFC6033] with an SOA certificate that includes the CMS Content Constraints extension (see Section 7.1).

Client-supported algorithms to decrypt the server-returned symmetric key are as follows:

* Message Digest: See Section 4 of [RFC8755].

* Digital Signature Algorithm: See Section 5 of [RFC8755].

* Key Agreement: See Section 6.1 of [RFC8755].

* Key Wrap: AES-256 Key Wrap with Padding [RFC6033] is used. AES-128 Key Wrap with Padding is not used.

* Content Encryption: AES-256 Key Wrap with Padding [RFC6033] is used. AES-128 Key Wrap with Padding is not used.

/symmetrickeys/return is not used at this time.

3.6.10. /eecerts, /firmware, /tamp

/eecerts, /firmware, and /tamp are not used at this time.

4. CMC Interface

Client options for CMC [RFC5274] [RFC6402] are specified in this section.

4.1. RFC 5273 Transport Protocols

Clients only use the HTTPS-based transport. The TLS implementation and configuration are as specified in [RFC9151], with the notable exception that only EC-based algorithms are used.

Clients that receive HTTP redirection responses (3xx status codes) will terminate the connection ([RFC7030], Section 3.2.1).

4.2. Eligibility

At the CMC interface, servers only enroll clients that they have established a prior relationship with independently of the EST service. To accomplish this, client owners/operators interact in person with the human acting as the Registration Authority (RA) to ensure the information included in the transmitted certificate request, which is sometimes called a Certificate Signing Request (CSR), is associated with a client. The mechanism by which the owner/operator interacts with the RA as well as the information provided is beyond the scope of this document. The information exchanged by the owner/operator might be something as simple as the subject name included in the CSR to be sent or a copy of the certificate that will be used to verify the certificate request, which is provided out of band.

4.3. Authentication

Mutual authentication occurs via client and server signing of CMC protocol elements, as required by [RFC8756]. All such signatures are validated against an installed TA; any that fail validation are rejected.

4.4. Authorization

Clients support the simultaneous presence of as many TAs as are required for all of the functions of the client, and only these TAs.

Clients check that the server's certificate includes the id-kp-cmcRA Extended Key Usage (EKU) value ([RFC6402], Section 2.10).

Clients that support processing of the CMS Content Constraints extension [RFC6010] ensure returned CMS content is from an SOA or an entity authorized by an SOA for that CMS content; see Section 7.1 for SOA certificates.

4.5. Full PKI Requests/Responses

Requests are as specified in [RFC8756] with the notable exception that only EC-based algorithms are used.

Additional attributes for returned CMS packages can be found in [RFC7906].

Certificates provided through this service are as specified in Section 7 of this document.

5. Trust Anchor Profile

Clients are free to store the TA in the format of their choosing; however, servers provide TA information in the form of self-signed CA certificates. This section documents requirements for self-signed certificates in addition to those specified in [RFC8603], which in turn specifies requirements in addition to those in [RFC5280].

Only EC-based algorithms are used.

Issuer and subject names are composed of only the following naming attributes: country name, domain component, organization name, organizational unit name, common name, state or province name, distinguished name qualifier, and serial number.

In the Subject Key Identifier extension, the keyIdentifier is the 64 low-order bits of the subject's subjectPublicKey field.

In the Key Usage extension, the nonRepudiation bit is never set.

6. Non-Self-Signed Certification Authority Certificate Profile

This section documents requirements for non-self-signed CA certificates in addition to those specified in [RFC8603], which in turn specifies requirements in addition to those in [RFC5280].

Only EC-based algorithms are used.

Subject names are composed of only the following naming attributes: country name, domain component, organization name, organizational unit name, common name, state or province name, distinguished name qualifier, and serial number.

In the Authority Key Identifier extension, the keyIdentifier choice is always used. The keyIdentifier is the 64 low-order bits of the issuer's subjectPublicKey field.

In the Subject Key Identifier extension, the keyIdentifier is the 64 low-order bits of the subject's subjectPublicKey field.

In the Key Usage extension, the nonRepudiation bit is never set.

The Certificate Policies extension is always included, and policyQualifiers are never used.

Non-self-signed CA certificates can also include the following:

Name Constraints: permittedSubtrees constraints are included, and excludedSubstree constraints are not. Of the GeneralName choices, issuers support the following: rfc822Name, dNSName, uniformResourceIdentifier, and iPAddress (both IPv4 and IPv6) as well as hardwareModuleName, which is defined in [RFC4108]. Note that rfc822Name, dNSName, and uniformResourceIdentifier are defined as IA5 strings, and the character sets allowed are not uniform amongst these three name forms.

CRL Distribution Points: A distributionPoint is always the fullName choice. The uniformResourceIdentifier GeneralName choice is always included, but others can also be used as long as the first element in the sequence of CRLDistributionPoints is the uniformResourceIdentifier choice. The reasons and cRLIssuer fields are never populated. This extension is never marked as critical.

Authority Information Access: Only one instance of AccessDescription is included. accessMethod is id-caIssuers, and accessLocation's GeneralName is always the uniformResourceIdentifier choice.

Extended Key Usage: EST servers and RAs include the id-kp-cmcRA EKU, and the CAs include the id-kp-cmcCA, which are both specified in [RFC6402].

Issuers include the Authority Clearance Constraints extension [RFC5913] in non-self-signed CA certificates that are issued to non-SOAs; values for the Certificate Policy (CP) Object Identifier (OID) and the supported classList values are found in the issuer's CP. Criticality is determined by the issuer, and a securityCategories is never included. Only one instance of Clearance is generated in the AuthorityClearanceConstraints sequence.

Issuers include a critical CMS Content Constraints extension [RFC6010] in CA certificates used to issue SOA certificates; this is necessary to enable enforcement of scope of the SOA authority. The content types included depend on the packages the SOA sources but include key packages (i.e., Encrypted Key Packages, Symmetric Key Packages, and Asymmetric Key Packages).

7. End-Entity Certificate Profile

This section documents requirements for EE signature and key establishment certificates in addition to those listed in [RFC8603], which in turn specifies requirements in addition to those in [RFC5280].

Only EC-based algorithms are used.

Subject names are composed of the following naming attributes: country name, domain component, organization name, organizational unit name, common name, state or province name, distinguished name qualifier, and serial number.

In the Authority Key Identifier extension, the keyIdentifier choice is always used. The keyIdentifier is the 64 low-order bits of the issuer's subjectPublicKey field.

In the Subject Key Identifier extension, the keyIdentifier is the 64 low-order bits of the subject's subjectPublicKey field.

In the Key Usage extension, signature certificates only assert digitalSignature, and key establishment certificates only assert keyAgreement.

The Certificate Policies extension is always included, and policyQualifiers are never used.

When included, the non-critical CRL Distribution Point extension's distributionPoint is always identified by the fullName choice. The uniformResourceIdentifier GeneralName choice is always included, but others can also be used as long as the first element in the sequence of distribution points is the URI choice and it is an HTTP/HTTPS scheme. The reasons and cRLIssuer fields are never populated.

The following subsections provide additional requirements for the different types of EE certificates.

7.1. Source of Authority Certificate Profile

This section specifies the format for SOA certificates, i.e., certificates issued to those entities that are authorized to create, digitally sign, encrypt, and distribute packages; these certificates are issued by non-PKI TAs.

The Subject Alternative Name extension is always included. The following choices are supported: rfc822Name, dNSName, ediPartyName, uniformResourceIdentifier, or iPAddress (both IPv4 and IPv6). This extension is never critical.

A critical CMS Content Constraints extension [RFC6010] is included in SOA signature certificates. The content types included depend on the packages the SOA sources (e.g., Encrypted Key Packages, Symmetric Key Packages, and Asymmetric Key Packages).

7.2. Client Certificate Profile

This section specifies the format for certificates issued to clients.

A non-critical Subject Directory Attributes extension is always included with the following attributes:

* Device Owner [RFC5916]

* Clearance Sponsor [RFC5917]

* Clearance [RFC5913]

The following extensions are also included at the discretion of the CA:

* The Authority Information Access extension with only one instance of AccessDescription included. accessMethod is id-caIssuers, and accessLocation's GeneralName is always the uniformResourceIdentifier choice.

* A non-critical Subject Alternative Name extension that includes the hardwareModuleName form [RFC4108], rfc822Name, or uniformResourceIdentifier.

* A critical Subject Alternative Name extension that includes

dNSName, rfc822Name, ediPartyName, uniformResourceIdentifier, or iPAddress (both IPv4 and IPv6).

8. Relying Party Applications

This section documents requirements for Relying Parties (RPs) in addition to those listed in [RFC8603], which in turn specifies requirements in addition to those in [RFC5280].

Only EC-based algorithms are used.

RPs support the Authority Key Identifier and the Subject Key Identifier extensions.

RPs should support the following extensions: CRL Distribution Points, Authority Information Access, Subject Directory Attribute, Authority Clearance Constraints, and CMS Content Constraints.

Within the Subject Directory Attribute extension, RPs should support the Clearance Sponsor, Clearance, and Device Owner attributes.

RPs support the id-kp-cmcRA and id-kp-cmcCA EKUs.

Failure to support extensions in this section might limit the suitability of a device for certain applications.

9. CRL Profile

This section documents requirements for CRLs in addition to those listed in [RFC8603], which in turn specifies requirements in addition to those in [RFC5280].

Only EC-based algorithms are used.

Two types of CRLs are produced: complete base CRLs and partitioned base CRLs.

crlEntryExtensions are never included, and the reasons and cRLIssuer fields are never populated.

All CRLs include the following CRL extensions:

* The Authority Key Identifier extension: The keyIdentifier is the 64 low-order bits of the issuer's subjectPublicKey field.

* As per [RFC5280], the CRL Number extension.

The only other extension included in partitioned base CRLs is the Issuing Distribution Point extension. The distributionPoint is always identified by the fullName choice. The uniformResourceIdentifier GeneralName choice is always included, but others can also be used as long as the first element in the sequence of distribution points is the uniformResourceIdentifier choice and the scheme is an HTTP/HTTPS scheme. All other fields are omitted.

10. IANA Considerations

This document has no IANA actions.

11. Security Considerations

This entire document is about security. This document profiles the use of many protocols and services: EST, CMC, and PKCS#10/#7/#12 as well as certificates, CRLs, and their extensions [RFC5280]. These have been cited throughout this document, and the specifications identified by those citations should be consulted for security considerations related to implemented protocols and services.

12. References

12.1. Normative References

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[RFC2985] Nystrom, M. and B. Kaliski, "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, DOI 10.17487/RFC2985, November 2000, <https://www.rfc-editor.org/info/rfc2985>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/info/rfc2986>.

[RFC3739] Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, DOI 10.17487/RFC3739, March 2004, <https://www.rfc-editor.org/info/rfc3739>.

[RFC4108] Housley, R., "Using Cryptographic Message Syntax (CMS) to Protect Firmware Packages", RFC 4108, DOI 10.17487/RFC4108, August 2005, <https://www.rfc-editor.org/info/rfc4108>.

[RFC5274] Schaad, J. and M. Myers, "Certificate Management Messages over CMS (CMC): Compliance Requirements", RFC 5274, DOI 10.17487/RFC5274, June 2008, <https://www.rfc-editor.org/info/rfc5274>.

[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>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC5911] Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, DOI 10.17487/RFC5911, June 2010, <https://www.rfc-editor.org/info/rfc5911>.

[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>.

[RFC5913] Turner, S. and S. Chokhani, "Clearance Attribute and Authority Clearance Constraints Certificate Extension", RFC 5913, DOI 10.17487/RFC5913, June 2010, <https://www.rfc-editor.org/info/rfc5913>.

[RFC5915] Turner, S. and D. Brown, "Elliptic Curve Private Key Structure", RFC 5915, DOI 10.17487/RFC5915, June 2010, <https://www.rfc-editor.org/info/rfc5915>.

[RFC5916] Turner, S., "Device Owner Attribute", RFC 5916, DOI 10.17487/RFC5916, June 2010, <https://www.rfc-editor.org/info/rfc5916>.

[RFC5917] Turner, S., "Clearance Sponsor Attribute", RFC 5917, DOI 10.17487/RFC5917, June 2010, <https://www.rfc-editor.org/info/rfc5917>.

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

[RFC5959] Turner, S., "Algorithms for Asymmetric Key Package Content Type", RFC 5959, DOI 10.17487/RFC5959, August 2010, <https://www.rfc-editor.org/info/rfc5959>.

[RFC6010] Housley, R., Ashmore, S., and C. Wallace, "Cryptographic Message Syntax (CMS) Content Constraints Extension", RFC 6010, DOI 10.17487/RFC6010, September 2010, <https://www.rfc-editor.org/info/rfc6010>.

[RFC6031] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Symmetric Key Package Content Type", RFC 6031, DOI 10.17487/RFC6031, December 2010, <https://www.rfc-editor.org/info/rfc6031>.

[RFC6032] Turner, S. and R. Housley, "Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6032, DOI 10.17487/RFC6032, December 2010, <https://www.rfc-editor.org/info/rfc6032>.

[RFC6033] Turner, S., "Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6033, DOI 10.17487/RFC6033, December 2010, <https://www.rfc-editor.org/info/rfc6033>.

[RFC6160] Turner, S., "Algorithms for Cryptographic Message Syntax

(CMS) Protection of Symmetric Key Package Content Types", RFC 6160, DOI 10.17487/RFC6160, April 2011, <https://www.rfc-editor.org/info/rfc6160>.

[RFC6161] Turner, S., "Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Encrypted Key Package Content Type", RFC 6161, DOI 10.17487/RFC6161, April 2011, <https://www.rfc-editor.org/info/rfc6161>.

[RFC6162] Turner, S., "Elliptic Curve Algorithms for Cryptographic Message Syntax (CMS) Asymmetric Key Package Content Type", RFC 6162, DOI 10.17487/RFC6162, April 2011, <https://www.rfc-editor.org/info/rfc6162>.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI 10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/info/rfc6268>.

[RFC6402] Schaad, J., "Certificate Management over CMS (CMC) Updates", RFC 6402, DOI 10.17487/RFC6402, November 2011, <https://www.rfc-editor.org/info/rfc6402>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC7191] Housley, R., "Cryptographic Message Syntax (CMS) Key Package Receipt and Error Content Types", RFC 7191, DOI 10.17487/RFC7191, April 2014, <https://www.rfc-editor.org/info/rfc7191>.

[RFC7192] Turner, S., "Algorithms for Cryptographic Message Syntax (CMS) Key Package Receipt and Error Content Types", RFC 7192, DOI 10.17487/RFC7192, April 2014, <https://www.rfc-editor.org/info/rfc7192>.

[RFC7292] Moriarty, K., Ed., Nystrom, M., Parkinson, S., Rusch, A., and M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, DOI 10.17487/RFC7292, July 2014, <https://www.rfc-editor.org/info/rfc7292>.

[RFC7906] Timmel, P., Housley, R., and S. Turner, "NSA's Cryptographic Message Syntax (CMS) Key Management Attributes", RFC 7906, DOI 10.17487/RFC7906, June 2016, <https://www.rfc-editor.org/info/rfc7906>.

[RFC8295] Turner, S., "EST (Enrollment over Secure Transport) Extensions", RFC 8295, DOI 10.17487/RFC8295, January 2018, <https://www.rfc-editor.org/info/rfc8295>.

[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>.

[RFC8755] Jenkins, M., "Using Commercial National Security Algorithm Suite Algorithms in Secure/Multipurpose Internet Mail Extensions", RFC 8755, DOI 10.17487/RFC8755, March 2020, <https://www.rfc-editor.org/info/rfc8755>.

[RFC8756] Jenkins, M. and L. Zieglar, "Commercial National Security Algorithm (CNSA) Suite Profile of Certificate Management over CMS", RFC 8756, DOI 10.17487/RFC8756, March 2020, <https://www.rfc-editor.org/info/rfc8756>.

[RFC9151] Cooley, D., "Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3", RFC 9151, DOI 10.17487/RFC9151, April 2022, <https://www.rfc-editor.org/info/rfc9151>.

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

[XML] Bray, T., Paoli, J., Sperberg-McQueen, C.M., Maler, E., and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <https://www.w3.org/TR/2008/REC-xml-20081126/>.

12.2. Informative 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>.

[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>.

Authors' Addresses

Michael Jenkins
National Security Agency
Email: mjjenki@cyber.nsa.gov

Sean Turner
sn3rd
Email: sean@sn3rd.com