The SODP (Secure Object Delivery Protocol) Server Interfaces:
NSA's Profile for Delivery of Certificates,
CRLs, and Symmetric Keys to Clients
draft-turner-sodp-profile-04.txt

Abstract

   This document specifies protocol interfaces profiled by the US NSA
   (United States National Security Agency) for NSS (National Security
   System) servers that provide public key certificates, CRLs
   (Certificate Revocation Lists), and symmetric keys to NSS clients.
   Servers that support these interfaces are referred to as SODP (Secure
   Object Delivery Protocol) 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: EST (Enrollment over Secure
   Transport) and its extensions as well as CMC (Certificate Management
   over CMS (Cryptographic Message Syntax)).

   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

Copyright Notice

Table of Contents

1. Introduction

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

      o EST (Enrollment over Secure Transport) [RFC7030] and its
        extensions [RFC8295], and
      o CMC (Certificate Management over CMS (Cryptographic Message
        Syntax)) [RFC5274][RFC6402] for both Simple PKI (Public Key
        Infrastructure) 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 NSA's
   Commercial National Security Algorithms. 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:

   o EST [RFC7030] and EST extensions [RFC8295];
   o PKI-related specifications [RFC2986], [RFC3739], [RFC5274],
     [RFC5280], [RFC5912], [RFC5913], [RFC5916], [RFC5917], [RFC6010],
     and [RFC6402];
   o Key-format-related specifications [RFC5915], [RFC5958],
     [RFC5959], [RFC6031], [RFC6032], [RFC6160], [RFC6161], [RFC6162],
     [RFC7191], [RFC7192], [RFC7292], and [RFC7906];
   o CMS-related (Cryptographic Message Syntax) RFCs [RFC5652],
     [RFC6268], and;
   o CNSA-related (Commercial National Security Algorithm) drafts
     [RFC8603], [ID.cnsa-smime-profile], [ID.cnsa-cmc-profile], and
     [ID.cnsa-tls-profile]. The profile defined herein does not
     support RSA-based or DHE-based algorithms.

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

1.2. Document Organization

   The document is organized as follows:

   o The remainder of this section describes the operational
     environment used by clients to retrieve secure objects.
   o Section 2 specifies the version of ASN.1 (Abstract Syntax
     Notation One) version used.
   o Section 3 specifies SODP's EST interface.
   o Section 4 specifies SODP's CMC interfaces; one section each for
     Simple PKI requests/responses and Full PKI requests/responses.
   o Sections 5-9 respectively specify TA, CA, and EE certificates as
     well as CRL.

1.3. Environment

   The environment is Client-Server-based from which clients obtain
   secure "objects" or "packages". Objects/packages vary based on the
   SOA (Source of Authority) 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 following example depicted in Figure 1, there are two SOAs:
one for symmetric keys, as depicted by the KTA (Key Trust Anchor),
and one for public key certificates, as depicted by the PKI TA (Trust
Anchor). 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 KSA (Key Source Authority) and a KDA (Key
Distribution Authority). 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 -
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 CAs (Certification
Authorities) and CAs in turn are responsible for creating,
distributing, and managing EEs (End-Entities) certificates; CAs
distribute PKI-related information through the /cacerts, /crls,
/eecerts, /fulcmc, /simpleenroll, /simplereenroll, /csrattrs EST and
EST extension services.

```
   +-----+                           +--------+
   | KTA |                           | PKI TA |
   +-----+                           +--------+
      |                                  |
      | Signs                            | Signs
      |                                  |
     +-------------+                     V
     |             |                  +----+
     V             V                  | CA |
   +-----+       +-----+              +----+
   | KSA |       | KDA |                 |
   +-----+       +-----+                 | Signs
      |             |                    |
      | Signs &   | Optionally        +---------------+
      | Encrypts  | Signs             |               |
      |             |                 V               V
      |             |            +-------------+ +-------------+
      |             V            | Certificate | | Certificate |
   +---|-------------+           +-------------+ | Revocation  |
   |   V             | CMS Content               | List        |
   | +-------------+ | Types                     +-------------+
   | | Key Package | |
```

```
   | +-------------+ |
     +-----------------+
```
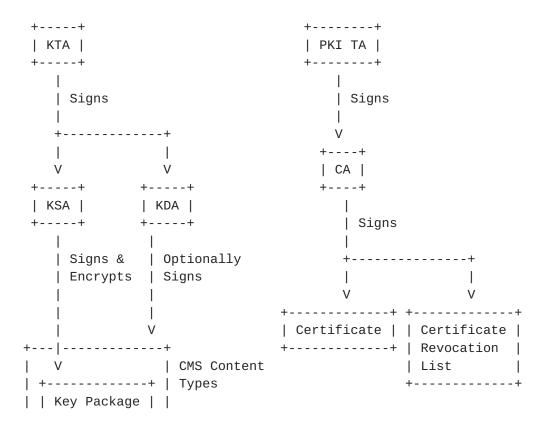

  Figure 1 - Operating Environment (Key and PKI Sources of Authority)

   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 '02/'08 ASN.1 (Abstract
   Syntax Notation One) version; '02/'08 ASN.1 modules can be found in
   [RFC5911], [RFC5912], and [RFC6268] (use RFC 6268 for the CMS syntax)
   while other specifications already include the '02/'08 ASN.1 along
   with the '88 ASN.1. See Section 1.1 of [RFC6268] for a discussion
   about the differences between the '02 and '08 ASN.1 versions.

3. EST Interface

   EST [RFC7030] and EST extensions [RFC8295] client options 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).

   Clients include an HTTP Accept header with each HTTP GET request to
   indicate the PAL Package Type supported ([RFC8295], Section 2.1.1).

3.2. Transport Layer Security

   TLS implementations are configured as specified in
   [ID.cnsa-tls-profile]; the notable exceptions are that RSA-based and
   DHE-based algorithms are not used.

3.3. Eligibility

   At the EST interface, servers enroll only clients that they have an
   established relationship with. To accomplish this, client
   owners/operators interact in person with the human acting as the RA
   (Registration Authority) to ensure the information included in the
   transmitted certificate request, which is sometimes called a CSR
   (Certificate Signing Request), is associated with a client. The
   mechanism by which the owner/operator interact 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 to-be sent CSR or a copy
   of an entire certificate that will be used to verify the certificate
   request.

3.4. Authentication

   Mutual authentication occurs via "Certificate TLS Authentication"
   ([RFC7030], Section 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. Clients reject all
   server attempts to authenticate that do not validate back to a 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
   EKU (Extended Key Usage) value ([RFC6402], Section 2.10).

   Clients that support processing the CMS Content Constraints extension
   [RFC6010] ensure returned CMS content is from an SOA or is from an
   entity authorized by an SOA for that CMS content; see Section 6.0 for
   SOA certificates.

3.6. EST and EST Extensions

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

3.6.1. /pal

   The PAL (Package Availability List) is limited to 32 entries, where
   the 32nd PAL entry links to an additional PAL (i.e., is 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 5.1 of [ID.cnsa-cmc-
profile], with two exceptions. First, the Change Subject Name and
the POP Link Witness V2 attributes, which are CMC-specific
requirements do not apply. Second, RSA-based algorithms are not
used.

Client requests include the tls-unique value in the challenge-
password attribute, as specified in [RFC7030], or the id-aa-
estIdentityLinking attribute, as specified in [RFC7894].

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 [ID.cnsa-cmc-profile] with the notable
exception that RSA-based algorithms are not 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), "P12", and "PKCS#12" files, are 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 both the 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: 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 a SODP server: additional encryption and origin authentication ([RFC8295], Section 5); server-provided Symmetric Key Content Type [RFC6032] encapsulated in an Encrypted Key Content Type using the EnvelopedData choice [RFC6033] with a 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:

  o Message Digest: See Section 5 of [ID.cnsa-smime-profile].
  o Digital Signature Algorithm: See Section 6.1 of
    [ID.cnsa-smime-profile].
  o Key Agreement: See Section 7.1 of [ID.cnsa-smime-profile].
  o Key Wrap: AES-256 Key Wrap with Padding [RFC6033] is used. AES-
    128 Key Wrap with Padding is not used.
  o Content Encryption: AES-256 Key Wrap with Padding [RFC6033] is
    used. AES-128 Key Wrap with Padding is not used.

    /serverkeygen/return is not used at this time.

3.6.10. /eecerts, /firmware, /tamp

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

4. CMC Interface

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

4.1. RFC 5273 Transport Protocols

   Clients use only the HTTPS-based transport; the TLS implementation
   and configuration is as specified in [ID.cnsa-tls-profile]; the
   notable exceptions are that RSA-based and DHE-based algorithms are
   not 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 enroll only clients that they have an
   established relationship with. To accomplish this, client
   owners/operators interact in person with the human acting as the RA
   (Registration Authority) to ensure the information included in the
   transmitted certificate request, which is sometimes called a CSR
   (Certificate Signing Request), is associated with a client. The
   mechanism by which the owner/operator interact 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 to-be sent CSR or a copy
   of an entire certificate that will be used to verify the certificate
   request.

4.3. Authentication

   Mutual authentication occurs via client and server signing of CMC
   protocol elements, as required by [ID.cnsa-cmc-profile]. All such
   signatures must be 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
   EKU (Extended Key Usage) value [RFC6402], Section 2.10.

   Clients that support processing the CMS Content Constraints extension
   [RFC6010] ensure returned CMS content is from an SOA or is from an
   entity authorized by an SOA for that CMS content; see Section 6.0 for
   SOA certificates

4.5. Full PKI Requests/Responses

Requests are as specified in [ID.cnsa-cmc-profile] with the notable exception that RSA-based algorithms are not used.

Additional attributes for returned CMC 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 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].

RSA-based algorithms are not 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].

RSA-based algorithms are not 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:

   o Name Constraints: permittedSubtrees constraints are applied 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 is not
     uniform amongst these three name forms.

   o 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
     critical.

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

   o 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 CP (Certificate Policy) OID (Object IDentifier) 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. 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](#)].

RSA-based algorithms are not 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 key 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, 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:

   o Device Owner [RFC5916]
   o Clearance Sponsor [RFC5917]
   o Clearance [RFC5913]

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

   o The Authority Information Access extension with only one instance
     of the accessMethod id-caIssuers and the accessLocation's
     GeneralName using the uniformResourceIdentifier choice.

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

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

RSA-based algorithms are not 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 extensions.

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](#)].

RSA-based algorithms are not 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:

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

   o 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 uniformResourceIdenifier 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 uniformResourceIdenifier choice and the scheme is an HTTP/HTTPS scheme; all other fields are omitted.

[10](#). IANA Considerations

None.

[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 referred to throughout this document and those
specifications should be consulted for security considerations
related to implemented protocol 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>.

   [RFC7894] Pritikin, M. and C. Wallace, "Alternative Challenge
             Password Attributes for Enrollment over Secure Transport",
             RFC 7894, DOI 10.17487/RFC7894, June 2016,
             <https://www.rfc-editor.org/info/rfc7894>.

   [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>.

   [XML]   Bray, T., Paoli, J., Sperberg-McQueen, 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/>.

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

   [ID.cnsa-smime-profile] Jenkins, M., "Using CNSA Suite Algorithms in
             Secure/Multipurpose Internet Mail Extensions(S/MIME)",
             work-in-progress, <https://www.ietf.org/internet-
             drafts/draft-jenkins-smime-profile-01>.

   [ID.cnsa-cmc-profile] Jenkins, M. and L. Zieglar, "Commercial
             National Security Algorithm (CNSA) Suite Profile of
             Certificate Management over CMS", work-in-progress,
             <https://www.ietf.org/internet-drafts/draft-jenkins-cmc-
             profile-05>.

   [ID.cnsa-tls-profile] Authors, "Commercial National Security
             Algorithm (CNSA) Suite Profile of TLS", work-in-progress,
             <https://www.ietf.org/internet-drafts/draft-cooley-cnsa-

dtls-tls-profile-00>.

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>.

          None.

Authors' Addresses

   Michael Jenkins
   National Security Agency

   EMail: mjjenki@nsa.gov

   Sean Turner
   sn3rd

   EMail: sean@sn3rd.com