                  Internet X.509 Public Key Infrastructure:
              Additional Algorithms and Identifiers for DSA and ECDSA

Abstract

   This document updates RFC 3279 to specify algorithm identifiers and
   ASN.1 encoding rules for the Digital Signature Algorithm (DSA) and
   Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures
   when using SHA-224, SHA-256, SHA-384, or SHA-512 as the hashing
   algorithm. 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). This document
   also identifies all four SHA2 hash algorithms for use in the Internet
   X.509 PKI.

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 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc5758.

Copyright Notice

Table of Contents

1. Introduction

   This specification defines the contents of the signatureAlgorithm,
   signatureValue, and signature fields within Internet X.509
   certificates and CRLs when these objects are signed using DSA or
   ECDSA with a SHA2 hash algorithm. These fields are more fully
   described in RFC 5280 [RFC5280]. This document also identifies all
   four SHA2 hash algorithms for use in the Internet X.509 PKI.

   This document profiles material presented in the "Secure Hash
   Standard" [FIPS180-3], "Public Key Cryptography for the Financial
   Services Industry: The Elliptic Curve Digital Signature Standard
   (ECDSA)" [X9.62], and the "Digital Signature Standard" [FIPS186-3].

   This document updates RFC 3279 [RFC3279] Sections 2.1, 2.2.2, and
   2.2.3. Note that RFC 5480 [RFC5480] updates Sections 2.3.5, 3 (ASN.1
   Module), and 5 (Security Considerations) of RFC 3279.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

2. Hash Functions

This section identifies four additional hash algorithms for use with
DSA and ECDSA in the Internet X.509 certificate and CRL profile
[RFC5280]. SHA-224, SHA-256, SHA-384, and SHA-512 produce a 224-bit,
256-bit, 384-bit, and 512-bit "hash" of the input, respectively, and
are fully described in the "Secure Hash Standard" [FIPS180-3].

The listed one-way hash functions are identified by the following
object identifiers (OIDs):

    id-sha224 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
        country(16) us(840) organization(1) gov(101) csor(3)
        nistalgorithm(4) hashalgs(2) 4 }

    id-sha256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
        country(16) us(840) organization(1) gov(101) csor(3)
        nistalgorithm(4) hashalgs(2) 1 }

    id-sha384 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
        country(16) us(840) organization(1) gov(101) csor(3)
        nistalgorithm(4) hashalgs(2) 2 }

    id-sha512 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
        country(16) us(840) organization(1) gov(101) csor(3)
        nistalgorithm(4) hashalgs(2) 3 }

When one of these OIDs appears in an AlgorithmIdentifier, all
implementations MUST accept both NULL and absent parameters as legal
and equivalent encodings.

Conforming certification authority (CA) implementations SHOULD use
SHA-224, SHA-256, SHA-384, or SHA-512 when generating certificates or
CRLs, but MAY use SHA-1 if they have a stated policy that requires
the use of this weaker algorithm.

3. Signature Algorithms

This section identifies OIDs for DSA with SHA-224 and SHA-256 as well
as ECDSA with SHA-224, SHA-256, SHA-384, and SHA-512. The contents
of the parameters component for each signature algorithm vary;
details are provided for each algorithm.

3.1. DSA Signature Algorithm

   The DSA is defined in the Digital Signature Standard (DSS)
   [FIPS186-3]. DSA was developed by the U.S. Government, and can be
   used in conjunction with a SHA2 hash function such as SHA-224 or
   SHA-256. DSA is fully described in [FIPS186-3].

   When SHA-224 is used, the OID is:

   id-dsa-with-sha224 OBJECT IDENTIFIER ::= { joint-iso-ccitt(2)
       country(16) us(840) organization(1) gov(101) csor(3)
       algorithms(4) id-dsa-with-sha2(3) 1 }.

   When SHA-256 is used, the OID is:

   id-dsa-with-sha256 OBJECT IDENTIFIER ::= { joint-iso-ccitt(2)
       country(16) us(840) organization(1) gov(101) csor(3)
       algorithms(4) id-dsa-with-sha2(3) 2 }.

   When the id-dsa-with-sha224 or id-dsa-with-sha256 algorithm
   identifier appears in the algorithm field as an AlgorithmIdentifier,
   the encoding SHALL omit the parameters field. That is, the
   AlgorithmIdentifier SHALL be a SEQUENCE of one component, the OID id-
   dsa-with-sha224 or id-dsa-with-sha256.

   Encoding rules for DSA signature values are specified in [RFC3279].

   Conforming CA implementations that generate DSA signatures for
   certificates or CRLs MUST generate such DSA signatures in accordance
   with all the requirements in Sections 4.1, 4.5, and 4.6 of
   [FIPS186-3].

   Conforming CA implementations that generate DSA signatures for
   certificates or CRLs MAY generate such DSA signatures in accordance
   with all the requirements and recommendations in [FIPS186-3], if they
   have a stated policy that requires conformance to [FIPS186-3].

3.2. ECDSA Signature Algorithm

   The Elliptic Curve Digital Signature Algorithm (ECDSA) is defined in
   "Public Key Cryptography for the Financial Services Industry: The
   Elliptic Curve Digital Signature Standard (ECDSA)" [X9.62]. The
   ASN.1 OIDs used to specify that an ECDSA signature was generated
   using SHA-224, SHA-256, SHA-384, or SHA-512 are, respectively:

```
   ecdsa-with-SHA224 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }

   ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }

   ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

   ecdsa-with-SHA512 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }
```

When the ecdsa-with-SHA224, ecdsa-with-SHA256, ecdsa-with-SHA384, or
ecdsa-with-SHA512 algorithm identifier appears in the algorithm field
as an AlgorithmIdentifier, the encoding MUST omit the parameters
field. That is, the AlgorithmIdentifier SHALL be a SEQUENCE of one
component, the OID ecdsa-with-SHA224, ecdsa-with-SHA256, ecdsa-with-
SHA384, or ecdsa-with-SHA512.

Conforming CA implementations MUST specify the hash algorithm
explicitly using the OIDs specified above when encoding ECDSA/SHA2
signatures in certificates and CRLs.

Conforming client implementations that process ECDSA signatures with
any of the SHA2 hash algorithms when processing certificates and CRLs
MUST recognize the corresponding OIDs specified above.

Encoding rules for ECDSA signature values are specified in RFC 3279
[RFC3279], Section 2.2.3, and RFC 5480 [RFC5480].

Conforming CA implementations that generate ECDSA signatures in
certificates or CRLs MUST generate such ECDSA signatures in
accordance with all the requirements specified in Sections 7.2 and
7.3 of [X9.62] or with all the requirements specified in Section
4.1.3 of [SEC1].

Conforming CA implementations that ECDSA signatures in certificates
or CRLs MAY generate such ECDSA signatures in accordance with all the
requirements and recommendations in [X9.62] or [SEC1] if they have a
stated policy that requires conformance to [X9.62] or [SEC1].

4. ASN.1 Module

The OIDs of the SHA2 hash algorithms are in the RFC 4055 [RFC4055]
ASN.1 module and the OIDs for DSA with SHA-224 and SHA-256 as well as
ECDSA with SHA-224, SHA-256, SHA-384, and SHA-512 are defined in the
RFC 5480 [RFC5480] ASN.1 module.

5. Security Considerations

   NIST has defined appropriate use of the hash functions in terms of
   the algorithm strengths and expected time frames for secure use in
   Special Publications (SPs) 800-78-1 [SP800-78-1], 800-57 [SP800-57],
   and 800-107 [SP800-107]. These documents can be used as guides to
   choose appropriate key sizes for various security scenarios.

   ANSI also provides security considerations for ECDSA in [X9.62].
   These security considerations may be used as a guide.

6. References

6.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
                Requirement Levels", BCP 14, RFC 2119, March 1997.

   [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, April 2002.

   [RFC4055]   Schaad, J., Kaliski, B., and R. Housley, "Additional
                Algorithms and Identifiers for RSA Cryptography for use
                in the Internet X.509 Public Key Infrastructure
                Certificate and Certificate Revocation List (CRL)
                Profile", RFC 4055, June 2005.

   [RFC5480]   Turner, S., Brown, D., Yiu, K., Housley, R., and T.
                Polk, "Elliptic Curve Cryptography Subject Public Key
                Information", RFC 5480, March 2009.

   [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, May 2008.

   [FIPS180-3] Federal Information Processing Standards Publication
                (FIPS PUB) 180-3, Secure Hash Standard (SHS), October
                2008.

   [FIPS186-3] Federal Information Processing Standards Publication
                (FIPS PUB) 186-3, Digital Signature Standard (DSS), June
                2009.

   [SEC1]   Standards for Efficient Cryptography Group (SECG), SEC
                1: Elliptic Curve Cryptography, Version 2.0, 2009.

   [X9.62]   X9.62-2005, "Public Key Cryptography for the Financial
                  Services Industry: The Elliptic Curve Digital Signature
                  Standard (ECDSA)", November, 2005.

6.2. Informative References

   [SP800-107]   Quynh Dang, NIST, "Recommendation for Applications Using
                  Approved Hash Algorithms", February 2009.

   [SP800-78-1]   W. Timothy Polk, Donna, F. Dodson, William E. Burr,
                  NIST, "Cryptographic Standards and Key Sizes for
                  Personal Identity Verification", August 2007.

   [SP800-57]   Elaine Barker, William Barker, William E. Burr, NIST,
                  "Recommendation for Key Management", August 2005.

7. Acknowledgements

   The authors of this document would like to acknowledge great inputs
   for this document from Alfred Hoenes, Sean Turner, Katrin Hoeper, and
   many others from IETF community. The authors also appreciate many
   great revision suggestions from Russ Housley and Paul Hoffman.

Authors' Addresses

   Quynh Dang
   NIST
   100 Bureau Drive, Stop 8930
   Gaithersburg, MD 20899-8930
   USA

   EMail: quynh.dang@nist.gov

   Stefan Santesson
   3xA Security (AAA-sec.com)
   Bjornstorp 744
   247 98 Genarp
   Sweden

   EMail: sts@aaa-sec.com

   Kathleen M. Moriarty
   RSA, The Security Division of EMC
   174 Middlesex Turnpike
   Bedford, MA 01730
   USA

   EMail: Moriarty_Kathleen@emc.com

   Daniel R. L. Brown
   Certicom Corp.
   5520 Explorer Drive
   Mississaug, ON L4W 5L1
   USA

   EMail: dbrown@certicom.com

   Tim Polk
   NIST
   100 Bureau Drive, Stop 8930
   Gaithersburg, MD 20899-8930
   USA

   EMail: tim.polk@nist.gov