

Additional Algorithms and Identifiers  
for use of Elliptic Curve Cryptography with PKIX  
(Explicit Identification of One-Way Hash Functions)  
<[draft-housley-pkix-ecc-pkalg-s-eccdsa-00.txt](#)>

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

Dan Brown from Certicom has submitted a specification for Additional Algorithms and Identifiers for use of Elliptic Curve Cryptography with PKIX. This document proposes a different approach for identifying the one-way hash function used with the ECDSA signature algorithm.

Internet-Draft

January 2005

## 1. Introduction

[RFC 3279](#) [[N1](#)] specifies the conventions for using many algorithms with certificates and CRLs. When ECDSA is used with SHA-1, [RFC 3279](#) says that the following object identifier ought to be employed:

ecdsa-with-SHA1 OBJECT IDENTIFIER ::= { id-ecSigType 1 }

Dan Brown from Certicom has submitted a specification for Additional Algorithms and Identifiers for use of Elliptic Curve Cryptography with PKIX [[I1](#)]. In his document, Dan proposes a different approach for identifying the one-way hash function used with the ECDSA signature algorithm.

The following new object identifier identifies the one-way hash function is the one recommended for the public key size:

ecdsa-with-Recommended OBJECT IDENTIFIER ::= { id-ecSigType recommended(2

In this case, the recommended one-way hash functions are given in the draft revision of X9.62 [[I2](#)]. The appropriate one-way has function is selected from SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The recommended one has the largest bit size that does not require bit truncation during the signing process. Bit truncation occurs when the one-way hash function output bit length is greater than the bit length of  $n$ , the order of the base point  $G$ .

This approach leads to potential ambiguity in the future. The concern is that additional one-way hash functions will be added to the "approved" set.

The alternative is to explicitly identify the one-way hash function that is employed with ECDSA.

### 1.1. Conventions Used In This Document

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 [RFC 2119](#) [[N2](#)].

### 1.2. Abstract Syntax Notation

All X.509 certificate [[N3](#)] extensions are defined using ASN.1

Internet-Draft

January 2005

## [2.](#) ECDSA with Explicit Identification of the One-Way Hash Function

To avoid potential ambiguity, this specification provides algorithm identifiers for ECDSA with the following one-way hash functions: SHA-224, SHA-256, SHA-384, and SHA-512. Note that the algorithm identifier for ECDSA with SHA-1 is already provided in [RFC 3279](#) [N1].

These algorithm identifiers have already been assigned by ANSI X9F1. They are:

```
ansi-X9-62 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) 10045 }
```

```
id-ecSigType OBJECT IDENTIFIER ::= { ansi-X9-62 signatures(4) }
```

```
id-ecdsa-with-SHA2 OBJECT IDENTIFIER ::= {id-ecSigType 3}
```

```
ecdsa-with-SHA224 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 1}
```

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 2}
```

```
ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 3}
```

```
ecdsa-with-SHA512 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 4}
```

## [3.](#) Security Considerations

This specification does not constrain the size of public keys or their parameters for use in the Internet PKI. However, the key size selected impacts the strength achieved when implementing cryptographic services. Selection of appropriate key sizes is critical to implementing appropriate security.

This specification does not identify particular elliptic curves for use in the Internet PKI. However, the particular curve selected impact the strength of the digital signatures. Some curves are cryptographically stronger than others!

In general, use of "well-known" curves, such as the "named curves" from ANSI X9.62 [I2], is a sound strategy. For additional

information, refer to X9.62 [Appendix H.1.3](#), "Key Length Considerations" and [Appendix A.1](#), "Avoiding Cryptographically Weak Keys".

#### [4.](#) IANA Considerations

Certificate extensions and extended key usage values are identified by object identifiers (OIDs). The OIDs used in this document are copied from the draft revision to X9.62 [[I2](#)]. These OIDs were assigned by ANSI X9F1. No further action by the IANA is necessary for this document or any anticipated updates.

Housley

[Page 3]

---

Internet-Draft

January 2005

#### [5.](#) References

Normative and informative references are provided.

##### [5.1.](#) Normative References

- [N1] Polk, W., Housley, R., and L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 3279](#), April 2002.
- [N2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [N3] ITU-T. Recommendation X.509: The Directory - Authentication Framework. 2000.
- [N4] CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.
- [N5] CCITT. Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

##### [5.2.](#) Informative References

- [I1] Brown, D., "Additional Algorithms and Identifiers for use of Elliptic Curve Cryptography with PKIX", Internet-Draft, July 2004, work in progress.  
<[draft-ietf-pkix-ecc-pkalgs-00.txt](#)>

- [I2] American National Standard for Financial Services. ANSI X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm. 1998. (An update is in the works.)

## [6.](#) ASN.1 Module

ECDSA-Algorithm-Identifiers  
{ TBD }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

ansi-X9-62 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) 10045 }

id-ecSigType OBJECT IDENTIFIER ::= { ansi-X9-62 signatures(4) }

id-ecdsa-with-SHA2 OBJECT IDENTIFIER ::= {id-ecSigType 3}

ecdsa-with-SHA224 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 1}

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 2}

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 3}

ecdsa-with-SHA512 OBJECT IDENTIFIER ::= {id-ecdsa-with-SHA2 4}

END

## [7.](#) IPR Considerations

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

Housley

[Page 5]

---

Internet-Draft

January 2005

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

#### [8](#). Author's Address

Russell Housley  
Vigil Security, LLC  
918 Spring Knoll Drive  
Herndon, VA 20170

[housley@vigilsec.com](mailto:housley@vigilsec.com)

## 9. Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.