

IKE Authentication Using ECDSA
<[draft-ietf-ipsec-ike-auth-ecdsa-02.txt](#)>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). 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/1id-abstracts.txt>

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

Abstract

This document describes how the Elliptic Curve Digital Signature Algorithm (ECDSA) may be used as the authentication method within the Internet Key Exchange (IKE) protocol. ECDSA may provide benefits including computational efficiency, small signature sizes, and minimal bandwidth, compared to other available digital signature methods. This document adds ECDSA capability to IKE without introducing any changes to existing IKE operation.

Table of Contents

| | | |
|--------------------|------------------------------------|-------------------|
| 1. | Introduction | 2 |
| 2. | ECDSA | 2 |
| 3. | Specifying ECDSA within IKE | 3 |
| 4. | Security Considerations | 4 |
| 5. | Intellectual Property Rights | 4 |
| 6. | Acknowledgments | 4 |
| 7. | References | 5 |
| 8. | Authors' Addresses | 6 |

INTERNET-DRAFT

15 March 2001

1. Introduction

The Internet Key Exchange, or IKE [[RFC2409](#)], is a key agreement and security negotiation protocol; it is used for key establishment in IPSec. In Phase 1 of IKE, both parties must authenticate each other using a negotiated authentication method. One option for the authentication method is digital signatures using public key cryptography. Currently, there are two digital signature methods defined for use within Phase 1: RSA signatures and DSA (DSS) signatures. This document introduces ECDSA signatures as a third method.

For any given level of security against the best attacks known, ECDSA signatures are smaller than RSA signatures and ECDSA keys require less bandwidth than DSA keys; there are also advantages of computational speed and efficiency in many settings. Additional efficiency may be gained by simultaneously using ECDSA for IKE authentication and using elliptic curve groups for the IKE key exchange. Implementers of IPSec and IKE may therefore find it desirable to use ECDSA as the Phase 1 authentication method.

2. ECDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the DSA (also called DSS) signature method [[FIPS186-2](#)]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is defined in the ANSI X9.62 standard [[ANSIX962](#)]; compatible specifications include FIPS 186-2 [[FIPS186-2](#)], IEEE P1363 [[IEEEP1363](#)], and SEC 1 [[SEC1](#)]. The use of ECDSA in X.509 certificates is described in IETF PKIX [[PKIX-ALG](#)].

ECDSA signatures are smaller than RSA signatures of similar cryptographic strength; see [[KEYS](#)] for a security analysis of key sizes across public key algorithms. ECDSA public keys (and certificates) are smaller than similar strength DSA keys, resulting in improved communications efficiency. Furthermore, on many platforms ECDSA operations can be computed faster than similar strength RSA or DSA operations. These advantages of signature size, bandwidth, and computational efficiency make ECDSA an attractive choice for many IKE implementations.

Recommended elliptic curve domain parameters for use with ECDSA are given in FIPS 186-2 [[FIPS186-2](#)] and SEC 2 [[SEC2](#)]. A subset of these parameters are recommended in [[ECC-GR](#)] for use in the IKE key exchange.

Like DSA, ECDSA incorporates the use of a hash function; currently, the only hash function defined for use with ECDSA is the SHA-1 message digest algorithm [[FIPS180-1](#)].

[3](#). Specifying ECDSA within IKE

The IKE key negotiation protocol consists of two phases, Phase 1 and Phase 2. Within Phase 1, the two negotiating parties authenticate each other, using either pre-shared keys, digital signatures, or public-key encryption. For digital signatures and public-key encryption methods, there are multiple options. The authentication method is specified as an attribute in the negotiated Phase 1 Security Association (SA).

Until now, there have been a total of seven specific authentication methods in Phase 1. We now add an eighth option: ECDSA signatures, specified by attribute value 8 in the SA. The new list of IANA-assigned attribute numbers for Phase 1 authentication is:

| | |
|----------------------------------|---|
| - Authentication Method | |
| pre-shared key | 1 |
| DSS signatures | 2 |
| RSA signatures | 3 |
| Encryption with RSA | 4 |
| Revised encryption with RSA | 5 |
| Encryption with El-Gamal | 6 |
| Revised encryption with El-Gamal | 7 |
| ECDSA signatures | 8 |

values 9-65000 are reserved to IANA. Values 65001-65535 are for private use among mutually consenting parties.

Phase 1 can be either Main Mode or Agressive Mode. The use and specification of ECDSA signatures as the authentication method applies to both modes. The sequence of Phase 1 message payloads is the same with ECDSA signatures as with DSS or RSA signatures.

When ECDSA is used in IKE, the signature payload shall contain an encoding of the computed signature, consisting of a pair of integers r

and s, encoded as a byte string using the ASN.1 syntax "ECDSA-Sig-Value" with DER encoding rules as specified in ANSI X9.62 [[ANSIX962](#)].

Note also that, like the other digital signature methods, ECDSA authentication requires the parties to know and trust each other's public key. This can be done by exchanging certificates, possibly within the Phase 1 negotiation, if the public keys of the parties are not already known to each other. The use of Internet X.509 public key infrastructure certificates [[PKIX-CERT](#)] is recommended; the representation of ECDSA keys in X.509 certificates is specified in [[PKIX-ALG](#)].

Blake-Wilson, Fahn

[Page 3]

INTERNET-DRAFT

15 March 2001

Since ECDSA requires the use of the SHA-1 hash function, implementers may find it convenient to specify SHA-1 as the value of the hash algorithm attribute when using ECDSA as the authentication method. Implementers may also find it convenient to use ECDSA authentication in conjunction with an elliptic curve group for the IKE Diffie-Hellman key agreement; see [[ECC-GR](#)] for specific curves for the key agreement.

[4](#). Security Considerations

Implementors should ensure that appropriate security measures are in place when they deploy ECDSA within IKE. In particular, the security of ECDSA requires the careful selection of both key sizes and elliptic curve domain parameters. Selection guidelines for these parameters and some specific recommended curves that are considered safe are provided in ANSI X9.62 [[ANSIX962](#)], FIPS 186-2 [[FIPS186-2](#)], and SEC 2 [[SEC2](#)].

[5](#). Intellectual Property Rights

The IETF has been notified of intellectual property rights claimed in regard to the specification contained in this document. For more information, consult the online list of claimed rights (<http://www.ietf.org/ipr.html>).

The IETF takes no position regarding the validity or scope of any

intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

[6](#). Acknowledgments

The authors would like to thank Paul Lambert and Prakash Panjwani for their comments and suggestions.

Blake-Wilson, Fahn

[Page 4]

INTERNET-DRAFT

15 March 2001

[7](#). References

- [ANSIX962] ANSI X9.62-1999, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", American National Standards Institute, 1998.
- [ECC-GR] S. Blake-Wilson, M. Salter, and Y. Poeluev, "Additional ECC Groups for IKE", IPSEC Working Group Internet-Draft [draft-ietf-ipsec-ike-ecc-groups-03.txt](#). September 1999.
- [FIPS180-1] FIPS 180-1, "Secure Hash Standard", National Institute of Standards and Technology, 1995.
- [FIPS186-2] FIPS 186-2, "Digital Signature Standard", National Institute of Standards and Technology, 2000.
- [IEEEP1363] IEEE P1363, "Standard Specifications for Public Key Cryptography", Institute of Electrical and Electronics Engineers, 2000.

- [KEYS] A. Lenstra and E. Verheul, "Selecting Cryptographic Key Sizes", October 1999. Presented at Public Key Cryptography Conference, Melbourne, Australia, January 2000. Available at <<http://www.cryptosavvy.com/>>.
- [PKIX-ALG] L. Bassham, R. Housley and W. Polk, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", PKIX Working Group Internet-Draft, [draft-ietf-pkix-ipki-pkalgs-02.txt](#), March 2001.
- [PKIX-CERT] W. Ford, R. Housley, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", PKIX Working Group Internet-Draft, [draft-ietf-pkix-new-part1-05.txt](#), March 2001.
- [RFC2409] D. Harkins and D. Carrel, "The Internet Key Exchange", IETF [RFC 2409](#), November 1998.
- [SEC1] SEC 1, "Elliptic Curve Cryptography", Standards for Efficient Cryptography Group, 2000.
- [SEC2] SEC 2, "Recommended Elliptic Curve Domain Parameters", Standards for Efficient Cryptography Group, 2000.

Blake-Wilson, Fahn

[Page 5]

INTERNET-DRAFT

15 March 2001

[8.](#) Author's Address

Simon Blake-Wilson
Certicom Corp.
sblake-wilson@certicom.com

Paul Fahn
Certicom Corp.
pfahn@certicom.com

[9.](#) Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

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.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.