IPSec Working Group
INTERNET-DRAFT
Expires: April 14, 2001

S. Blake-Wilson and P. Fahn
Certicom Corp.

October 15, 2000

IKE Authentication Using ECDSA
<draft-ietf-ipsec-ike-auth-ecdsa-01.txt>

Status of this Memo

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 provides authentication and non-repudiation with benefits of 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.

1. Introduction

The Internet Key Exchange, or IKE [RFC2409, IKE], 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, 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 [FIPS-186]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is defined in the ANSI X9.62 standard [X9.62]; a compatible specification, along with test vectors, can be found in the documents of the Standards for Efficient Cryptography Group at <http://www.secg.org>. A profile for the use of ECDSA in X.509 certificates [EPKIX] describes the means to carry ECDSA keys in X.509 certificates.

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 implementions.

Recommended elliptic curve domain parameters for use with ECDSA are given in [SEC2]. A subset of these 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 [FIPS-180].

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 using the ASN.1 syntax "ECDSA-Sig-Value" as specified in ANSI X9.62 [X9.62] and PKIX [EPKIX].

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 [RFC 2459] is recommended; the representation of ECDSA keys in X.509 certificates is specified in [EPKIX].

Since ECDSA requires the use of the SHA-1 hash function, implemententers 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.

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 [X9.62], [NIST-ECC], and [SEC2].

Intellectual Property Rights

To be provided.

[NOTE: The readers should be aware of the possibility that implementation of this draft may require use of inventions covered by patent rights.]

Acknowledgments

The author would like to thank Simon Blake-Wilson, Prakash Panjwani, and Paul Lambert for their comments and suggestions.

References

[IKE] Harkins, D. and Carrel, D., "The Internet Key Exchange", draft-ietf-ipsec-ike-01.txt, May 1999.

[RFC2409] Harkins, D. and Carrel, D., "The Internet Key Exchange" (RFC 2409). November, 1998.

[X9.62] American National Standards Institute. ANSI X9.62-1998, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm". January, 1999.

[KEYS] Lenstra, A.K. and Verheul, E.R., "Selecting Cryptographic Key Sizes", October 1999. Presented at Public Key Cryptography Conference, Melbourne, Australia, January, 2000. Available at <http://www.cryptosavvy.com/>.

[FIPS-180] Federal Information Processing Standards Publication (FIPS PUB) 180-1, "Secure Hash Standard", April 17, 1995.

[FIPS-186] Federal Information Processing Standards Publication (FIPS PUB) 186, "Digital Signature Standard", May 19, 1994.

[NIST-ECC] National Institute for Standards and Technology, "Recommended Elliptic Curves for Federal Government Use", July 1999, <http://csrc.nist.gov/encryption/NISTReCur.pdf>

[SEC1] Standards for Efficient Cryptography Group, "SEC 1: Elliptic Curve Cryptography", Version 0.5, September, 1999. <http://www.secg.org>

[SEC2] Standards for Efficient Cryptography Group, "SEC 2: Recommended Elliptic Curve Domain Parameters", Version 0.6, October, 1999. <http://www.secg.org>

[ECC-GR] Panjwani, P. and Poeluev, Y., "Additional ECC Groups for IKE", draft-ietf-ipsec-ike-ecc-groups-01.txt. September, 1999.

[RFC 2459] R. Housley, W. Ford, W. Polk and D. Solo "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", January, 1999.

[EPKIX] Bassham, L., Johnson, D., and Polk, W., "Representation of Elliptic Curve Digital Signature Algorithm (ECDSA) Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates", draft-ietf-pkix-ipki-ecdsa-02.txt. October, 1999.

Author's Address

Paul Fahn
Certicom Corp.
25801 Industrial Blvd.
Hayward, CA 94545

e-mail: pfahn@certicom.com

Full Copyright Statement

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.