IPSec Working Group
INTERNET-DRAFT
Expires October 2, 2005
J. Solinas, NSA
March 31, 2005

# IKE Authentication Using ECDSA

<draft-ietf-ipsec-ike-auth-ecdsa-03.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 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.

## 1. Introduction

The Internet Key Exchange, or IKE [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 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.

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. ECDSA

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the DSA (DSS) signature method [DSS]. It is defined in the ANSI X9.62 standard [X9.62]. Other compatible specifications include FIPS 186-2 [DSS], IEEE 1363 [IEEE-1363], IEEE 1363A [IEEE-1363A], and SEC1 [SEC1].

Like DSA, ECDSA incorporates the use of a hash function. [SHS] specifies hash functions that are appropriate for use with ECDSA. Implementations of IKE using ECDSA SHOULD use one of these hash functions.

ECDSA signatures are smaller than RSA signatures of similar cryptographic strength. 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 more quickly than similar strength RSA or DSA operations (see [LV] for a security analysis of key sizes across public key algorithms). These advantages of signature size, bandwidth, and computational efficiency may make ECDSA an attractive choice for many IKE implementations.





Recommended elliptic curve domain parameters for use with ECDSA are given in FIPS 186-2 [DSS], ANSI X9.62 [X9.62], and SEC 2 [SEC2].

Implementations of IKE using ECDSA MAY use one of these domain parameters. A subset of these parameters are recommended in [IKE-ECP] for use in the IKE key exchange. These parameters MAY be used for ECDSA as well.

## 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 IANA-assigned attribute number for Phase 1 authentication using ECDSA is 8 (see [IANA]).

Phase 1 can be either Main Mode or Aggressive 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 [X9.62].

As with 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-3280] is recommended; the representation of ECDSA keys in X.509 certificates is specified in [RFC-3279]. This representation SHOULD be used if X.509 certificates are used.

Implemententers may find it convenient, when using ECDSA as the authentication method, to specify the hash used by ECDSA as the value of the hash algorithm attribute. 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 [IKE-ECP] for some 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 [X9.62], FIPS 186-2 [DSS], and SEC 2 [SEC2].

## 5. IANA Considerations

This document has no actions for IANA.

## 6. References

### 6.1 Normative

[IKE] D. Harkins and D. Carrel, The Internet Key Exchange, RFC 2409, November 1998.

[RFC-3279] Bassham, L., Housley, R., and Polk, W., RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key

Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2002. (http://www.ietf.org/rfc/rfc3279.txt)

[RFC-3280] Housley, R., Polk, W., Ford, W. and D. Solo, RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2002. (http://www.ietf.org/rfc/rfc3279.txt)

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

## 6.2 Informative

[DSS] U.S. Department of Commerce/National Institute of Standards and Technology, Digital Signature Standard (DSS), FIPS PUB 186-2, January 2000. (http://csrc.nist.gov/publications/fips/index.html)

[IANA] Internet Assigned Numbers Authority, Internet Key Exchange (IKE) Attributes. (http://www.iana.org/assignments/ipsec-registry)

[IEEE-1363] Institute of Electrical and Electronics Engineers. IEEE 1363-2000, Standard for Public Key Cryptography. (http://grouper.ieee.org/groups/1363/index.html)





[IEEE-1363A] Institute of Electrical and Electronics Engineers. IEEE 1363A-2004, Standard for Public Key Cryptography - Amendment 1: Additional Techniques. (http://grouper.ieee.org/groups/1363/index.html)

[IKE-ECP] J. Solinas, ECP Groups For IKE, 2005. (draft-ietf-ipsec-ike-ecc-groups-05.txt)

[LV] A. Lenstra and E. Verheul, "Selecting Cryptographic Key Sizes", Journal of Cryptology 14 (2001), pp. 255-293.

[SEC1] Standards for Efficient Cryptography Group. SEC 1 - Elliptic Curve Cryptography, v. 1.0, 2000. (http://www.secg.org)

[SEC2] Standards for Efficient Cryptography Group. SEC 2 - Recommended Elliptic Curve Domain Parameters, v. 1.0, 2000. (http://www.secg.org)

[SHS] FIPS 180-2, "Secure Hash Standard", National Institute of Standards and Technology, 2002.





## 7. Author's Address

Jerome A. Solinas
National Security Agency
jsolinas@orion.ncsc.mil

Comments are solicited and should be addressed to the author.

Expires October 2, 2005