IPSec Working Group
INTERNET-DRAFT
Expires November 27, 2005

J. Solinas, NSA

May 27, 2005

ECC Groups For IKEv2
<draft-ietf-ipsec-ikev2-ecc-groups-01.txt>

Status of this Memo

Abstract

This document describes ECC groups for use as Diffie-Hellman groups in the Internet Key Exchange version 2 (IKEv2) protocol. These new groups are defined to align IKEv2 with other standards, particularly NIST standards, and with and to provide more efficient implementation than in previously defined groups.

1. Introduction

This document describes default groups for use in elliptic curve Diffie-Hellman in IKEv2 in addition to the groups already so defined.

The IKEv2 document [IKEv2] defines Diffie-Hellman groups 1 and 2 from [IKE] for use in IKEv2. The IKEv2 algorithms document [ALGS] defines group 2 as well as group 14 from [RFC-3526] for IKEv2. (The numbering of the groups is as in [IANA].) All three of these groups are MODP modular exponentiation groups.

This document defines ECP type elliptic curve groups for use in IKEv2. This is done for four reasons:

1. To enable IKEv2 to be implemented in a way that enjoys the computational and bandwidth advantages of elliptic curves over modular exponentiation groups.

2. To align IKEv2 with existing ECC standards, particularly those of NIST.

3. To provide a common elliptic curve environment for users of IKE and IKEv2.

4. The groups proposed are capable of providing security consistent with the new Advanced Encryption Standard.

In addition, it is anticipated that the availability of standardized groups will result in optimizations for a particular curve and field size as well as allowing precomputation that could result in faster implementations.

In summary, due to the performance advantages of elliptic curve groups in IKEv2 implementations and the need for further alignment with other standards, this document defines three elliptic curves for IKEv2.

2. ECC Groups

IKEv2 implementations SHOULD support the following three Diffie-Hellman groups.

Group Number	Group Type	Bit Length	Defined
19	ECP	256	[IKE-ECP]
20	ECP	384	[IKE-ECP]
21	ECP	521	[IKE-ECP]

The details of the three groups are given in [IKE-ECP], in which they are defined for use in the original version of IKE. The group numbers correspond to the anticipated IANA identifiers. For a full list of Diffie-Hellman groups, see [IANA] or {ECG5].

3. Alignment with Other Standards

The following table summarizes the appearance of these three elliptic curve groups in other standards.

Standard		Group 19	Group 20	Group 21
NIST	[DSS]	P-256	P-384	P-521
ISO/IEC	[ISO-15946-1]	P-256		
ISO/IEC	[ISO-18031]	P-256	P-384	P-521
ANSI	[X9.62-1998]	Sect. J.5.3, Example 1		
ANSI	[X9.62-2003]	Sect. J.6.5.3	Sect. J.6.6	Sect. J.6.7
ANSI	[X9.63]	Sect. J.5.4, Example 2	Sect. J.5.5	Sect. J.5.6
SECG	[SEC2]	secp256r1	secp384r1	secp521r1

See also [NIST], [ISO-14888-3], [ISO-15946-2], [ISO-15946-3], and [ISO-15946-4].

4. Security Considerations

Since this document proposes new groups for use within IKEv2, many of the security considerations contained within [IKEv2] apply here as well.

The groups proposed in this document correspond to the symmetric key sizes 128 bits, 192 bits, and 256 bits. This allows the IKE key exchange to offer security comparable with the AES algorithms [AES].

5. IANA Considerations

This document has no actions for IANA.

6. References

6.1 Normative

[IKEv2] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, 2004, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-17.txt

[IKE-ECP] J. Solinas, ECP Groups For IKE, May 2005, draft-ietf-ipsec-ike-ecp-groups-01.txt.

6.2 Informative

[AES] U.S. Department of Commerce/National Institute of Standards and Technology, Advanced Encryption Standard (AES), FIPS PUB 197, November 2001. (http://csrc.nist.gov/publications/fips/index.html)

[ALGS] J. Schiller, Cryptographic Algorithms for use in the Internet Key Exchange Version 2, draft-ietf-ipsec-ikev2-algorithms-05.txt, April 2004.

[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)

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

[ISO-14888-3] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC First Committee Draft 14888-3 (2nd ed.), Information Technology: Security Techniques: Digital Signatures with Appendix: Part 3 - Discrete Logarithm Based Mechanisms.

[ISO-15946-1] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-1: 2002-12-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 1 - General.

[ISO-15946-2] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-2: 2002-12-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 2 - Digital Signatures.

[ISO-15946-3] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-3: 2002-12-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 3 - Key Establishment.

[ISO-15946-4] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 15946-4: 2004-10-01, Information Technology: Security Techniques: Cryptographic Techniques based on Elliptic Curves: Part 4 - Digital Signatures giving Message Recovery.

[ISO-18031] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC Final Committee Draft 18031, Information Technology: Security Techniques: Random Bit Generation, October 2004.

[NIST] U.S. Department of Commerce/National Institute of Standards and Technology. Recommendation for Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication 800-56. (http://csrc.nist.gov/CryptoToolkit/KeyMgmt.html)

[RFC-3526] T. Kivinen and M. Kojo, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), RFC 3526, May 2003.

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

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

[X9.62-2003] American National Standards Institute, ANS X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, Revised-Draft-2003-02-26, February 2003.

[X9.63] American National Standards Institute. ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography. November 2001.

7. Author's Address

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

Comments are solicited and should be addressed to the author.