Network Working Group
Request for Comments: 4753
Category: Informational

D. Fu
J. Solinas
NSA

January 2007

ECP Groups for IKE and IKEv2

Status of This Memo

Copyright Notice

Abstract

This document describes new Elliptic Curve Cryptography (ECC) groups for use in the Internet Key Exchange (IKE) and Internet Key Exchange version 2 (IKEv2) protocols in addition to previously defined groups. Specifically, the new curve groups are based on modular arithmetic rather than binary arithmetic. These new groups are defined to align IKE and IKEv2 with other ECC implementations and standards, particularly NIST standards. In addition, the curves defined here can provide more efficient implementation than previously defined ECC groups.

Table of Contents

1. Introduction

This document describes default Diffie-Hellman groups for use in IKE and IKEv2 in addition to the Oakley groups included in [IKE] and the additional groups defined since [IANA-IKE]. This document assumes that the reader is familiar with the IKE protocol and the concept of Oakley Groups, as defined in RFC 2409 [IKE].

RFC 2409 [IKE] defines five standard Oakley Groups: three modular exponentiation groups and two elliptic curve groups over GF[2^N]. One modular exponentiation group (768 bits - Oakley Group 1) is mandatory for all implementations to support, while the other four are optional. Thirteen additional groups subsequently have been defined and assigned values by IANA. All of these additional groups are optional. Of the eighteen groups defined so far, eight are MODP groups (exponentiation groups modulo a prime), and ten are EC2N groups (elliptic curve groups over GF[2^N]). See [RFC3526] for more information on MODP groups.

The purpose of this document is to expand the options available to implementers of elliptic curve groups by adding three ECP groups (elliptic curve groups modulo a prime). The reasons for adding such groups include the following.

- The groups proposed afford efficiency advantages in software applications since the underlying arithmetic is integer arithmetic modulo a prime rather than binary field arithmetic. (Additional computational advantages for these groups are presented in [GMN].)

- The groups proposed encourage alignment with other elliptic curve standards. The proposed groups are among those standardized by NIST, the Standards for Efficient Cryptography Group (SECG), ISO, and ANSI. (See Section 5 for details.)

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

These groups could also be defined using the New Group Mode, but including them in this RFC will encourage interoperability of IKE implementations based upon elliptic curve groups. In addition, the availability of standardized groups will result in optimizations for a particular curve and field size and allow precomputation that could result in faster implementations.

In summary, due to the performance advantages of elliptic curve groups in IKE implementations and the need for further alignment with other standards, this document defines three elliptic curve groups based on modular arithmetic.

2. Requirements Terminology

The keywords "MUST" and "SHOULD" that appear in this document are to be interpreted as described in [RFC2119].

3. Additional ECC Groups

The notation adopted in RFC 2409 [IKE] is used below to describe the new groups proposed.

3.1. 256-bit Random ECP Group

IKE and IKEv2 implementations SHOULD support an ECP group with the following characteristics. The curve is based on the integers modulo the generalized Mersenne prime p given by

p = 2^(256)-2^(224)+2^(192)+2^(96)-1

The equation for the elliptic curve is:

y^2 = x^3 - 3 x + b

Field Size:
256

Group Prime/Irreducible Polynomial:
FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

Group Curve b:
5AC635D8 AA3A93E7 B3EBBD55 769886BC 651D06B0 CC53B0F6 3BCE3C3E 27D2604B

Group Order:
FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

The group was chosen verifiably at random using SHA-1 as specified in [IEEE-1363] from the seed:

C49D3608 86E70493 6A6678E1 139D26B7 819F7E90

The generator for this group is given by g=(gx,gy) where

gx:
6B17D1F2 E12C4247 F8BCE6E5 63A440F2 77037D81 2DEB33A0 F4A13945 D898C296

gy:
4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16 2BCE3357 6B315ECE CBB64068 37BF51F5

3.2. 384-bit Random ECP Group

IKE and IKEv2 implementations SHOULD support an ECP group with the following characteristics. The curve is based on the integers modulo the generalized Mersenne prime p given by

p = 2^(384)-2^(128)-2^(96)+2^(32)-1

The equation for the elliptic curve is:

y^2 = x^3 - 3 x + b

Field Size:
384

Group Prime/Irreducible Polynomial:
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE
FFFFFFFF 00000000 00000000 FFFFFFFF

Group Curve b:
B3312FA7 E23EE7E4 988E056B E3F82D19 181D9C6E FE814112 0314088F 5013875A
C656398D 8A2ED19D 2A85C8ED D3EC2AEF

Group Order:
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF
581A0DB2 48B0A77A ECEC196A CCC52973

The group was chosen verifiably at random using SHA-1 as specified in [IEEE-1363] from the seed:

A335926A A319A27A 1D00896A 6773A482 7ACDAC73

The generator for this group is given by g=(gx,gy) where

gx:
AA87CA22 BE8B0537 8EB1C71E F320AD74 6E1D3B62 8BA79B98 59F741E0 82542A38
5502F25D BF55296C 3A545E38 72760AB7

gy:
3617DE4A 96262C6F 5D9E98BF 9292DC29 F8F41DBD 289A147C E9DA3113 B5F0B8C0
0A60B1CE 1D7E819D 7A431D7C 90EA0E5F

3.3. 521-bit Random ECP Group

IKE and IKEv2 implementations SHOULD support an ECP group with the following characteristics. The curve is based on the integers modulo the Mersenne prime p given by

$$p = 2^{521}-1$$

The equation for the elliptic curve is:

$$y^2 = x^3 - 3x + b$$

Field Size:
521

Group Prime/Irreducible Polynomial:
01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFF

Group Curve b:
0051953E B9618E1C 9A1F929A 21A0B685 40EEA2DA 725B99B3 15F3B8B4 89918EF1
09E15619 3951EC7E 937B1652 C0BD3BB1 BF073573 DF883D2C 34F1EF45 1FD46B50
3F00

Group Order:
01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFA5186 8783BF2F 966B7FCC 0148F709 A5D03BB5 C9B8899C 47AEBB6F B71E9138
6409

The group was chosen verifiably at random using SHA-1 as specified in [IEEE-1363] from the seed:

D09E8800 291CB853 96CC6717 393284AA A0DA64BA

The generator for this group is given by g=(gx,gy) where

gx:
00C6858E 06B70404 E9CD9E3E CB662395 B4429C64 8139053F B521F828 AF606B4D
3DBAA14B 5E77EFE7 5928FE1D C127A2FF A8DE3348 B3C1856A 429BF97E 7E31C2E5
BD66

gy:
01183929 6A789A3B C0045C8A 5FB42C7D 1BD998F5 4449579B 446817AF BD17273E
662C97EE 72995EF4 2640C550 B9013FAD 0761353C 7086A272 C24088BE 94769FD1
6650

4. Security Considerations

Since this document proposes new groups for use within IKE and IKEv2, many of the security considerations contained within [IKE] and [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. Alignment with Other Standards

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

Standard		256-bit Random ECP Group	384-bit Random ECP Group	521-bit Random ECP Group
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	[X9.62-2005]	Sect. L.6.4.3	Sect. L.6.5.2	Sect. L.6.6.2
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].

6. IANA Considerations

IANA has updated its registries of Diffie-Hellman groups for IKE in [IANA-IKE] and for IKEv2 in [IANA-IKEv2] to include the groups defined above.

In [IANA-IKE], the groups appear as new entries in the list of Diffie-Hellman groups given by Group Description (attribute class 4). The descriptions are "256-bit random ECP group", "384-bit random ECP

group", and "521-bit random ECP group". In each case, the group type (attribute class 5) has the value 2 (ECP, elliptic curve group over GF[P]).

In [IANA-IKEv2], the groups appear as new entries in the list of IKEv2 transform type values for Transform Type 4 (Diffie-Hellman groups).

7. ECP Key Exchange Data Formats

In an ECP key exchange, the Diffie-Hellman public value passed in a KE payload consists of two components, x and y, corresponding to the coordinates of an elliptic curve point. Each component MUST have bit length as given in the following table.

Diffie-Hellman group	component bit length
256-bit Random ECP Group	256
384-bit Random ECP Group	384
521-bit Random ECP Group	528

This length is enforced, if necessary, by prepending the value with zeros.

The Diffie-Hellman public value is obtained by concatenating the x and y values.

The format of the Diffie-Hellman shared secret value is the same as that of the Diffie-Hellman public value.

8. Test Vectors

The following are examples of the IKEv2 key exchange payload for each of the three groups specified in this document.

We denote by g^n the scalar multiple of the point g by the integer n; it is another point on the curve. In the literature, the scalar multiple is typically denoted ng; the notation g^n is used in order to conform to the notation used in [IKE] and [IKEv2].

8.1. 256-bit Random ECP Group

IANA assigned the ID value 19 to this Diffie-Hellman group.

We suppose that the initiator's Diffie-Hellman private key is

```
i:
 C88F01F5 10D9AC3F 70A292DA A2316DE5 44E9AAB8 AFE84049 C62A9C57 862D1433
```

Then the public key is given by g^i=(gix,giy) where

```
gix:
 DAD0B653 94221CF9 B051E1FE CA5787D0 98DFE637 FC90B9EF 945D0C37 72581180

giy:
 5271A046 1CDB8252 D61F1C45 6FA3E59A B1F45B33 ACCF5F58 389E0577 B8990BB3
```

The KEi payload is as follows.

```
 00000048 00130000 DAD0B653 94221CF9 B051E1FE CA5787D0 98DFE637 FC90B9EF
 945D0C37 72581180 5271A046 1CDB8252 D61F1C45 6FA3E59A B1F45B33 ACCF5F58
 389E0577 B8990BB3
```

We suppose that the response Diffie-Hellman private key is

```
r:
 C6EF9C5D 78AE012A 011164AC B397CE20 88685D8F 06BF9BE0 B283AB46 476BEE53
```

Then the public key is given by g^r=(grx,gry) where

```
grx:
 D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C 736FC755 4494BF63

gry:
 56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83 53E74F33 039872AB
```

The KEr payload is as follows.

```
 00000048 00130000 D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C
 736FC755 4494BF63 56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83
 53E74F33 039872AB
```

The shared secret value g^ir=(girx,giry) where

girx:
D6840F6B 42F6EDAF D13116E0 E1256520 2FEF8E9E CE7DCE03 812464D0 4B9442DE

giry:
522BDE0A F0D8585B 8DEF9C18 3B5AE38F 50235206 A8674ECB 5D98EDB2 0EB153A2

These are concatenated to form

g^ir:
D6840F6B 42F6EDAF D13116E0 E1256520 2FEF8E9E CE7DCE03 812464D0 4B9442DE
522BDE0A F0D8585B 8DEF9C18 3B5AE38F 50235206 A8674ECB 5D98EDB2 0EB153A2

This is the value that is used in the formation of SKEYSEED.

8.2. 384-bit Random ECP Group

IANA assigned the ID value 20 to this Diffie-Hellman group.

We suppose that the initiator’s Diffie-Hellman private key is

i:
099F3C70 34D4A2C6 99884D73 A375A67F 7624EF7C 6B3C0F16 0647B674 14DCE655
E35B5380 41E649EE 3FAEF896 783AB194

Then the public key is given by g^i=(gix,giy) where

gix:
667842D7 D180AC2C DE6F74F3 7551F557 55C7645C 20EF73E3 1634FE72 B4C55EE6
DE3AC808 ACB4BDB4 C88732AE E95F41AA

giy:
9482ED1F C0EEB9CA FC498462 5CCFC23F 65032149 E0E144AD A0241815 35A0F38E
EB9FCFF3 C2C947DA E69B4C63 4573A81C

The KEi payload is as follows.

00000068 00140000 667842D7 D180AC2C DE6F74F3 7551F557 55C7645C 20EF73E3
1634FE72 B4C55EE6 DE3AC808 ACB4BDB4 C88732AE E95F41AA 9482ED1F C0EEB9CA
FC498462 5CCFC23F 65032149 E0E144AD A0241815 35A0F38E EB9FCFF3 C2C947DA
E69B4C63 4573A81C

We suppose that the response Diffie-Hellman private key is

r:
41CB0779 B4BDB85D 47846725 FBEC3C94 30FAB46C C8DC5060 855CC9BD A0AA2942
E0308312 916B8ED2 960E4BD5 5A7448FC

Then the public key is given by g^r=(grx,gry) where

grx:
E558DBEF 53EECDE3 D3FCCFC1 AEA08A89 A987475D 12FD950D 83CFA417 32BC509D
0D1AC43A 0336DEF9 6FDA41D0 774A3571

gry:
DCFBEC7A ACF31964 72169E83 8430367F 66EEBE3C 6E70C416 DD5F0C68 759DD1FF
F83FA401 42209DFF 5EAAD96D B9E6386C

The KEr payload is as follows.

00000068 00140000 E558DBEF 53EECDE3 D3FCCFC1 AEA08A89 A987475D 12FD950D
83CFA417 32BC509D 0D1AC43A 0336DEF9 6FDA41D0 774A3571 DCFBEC7A ACF31964
72169E83 8430367F 66EEBE3C 6E70C416 DD5F0C68 759DD1FF F83FA401 42209DFF
5EAAD96D B9E6386C

The shared secret value g^ir=(girx,giry) where

girx:
11187331 C279962D 93D60424 3FD592CB 9D0A926F 422E4718 7521287E 7156C5C4
D6031355 69B9E9D0 9CF5D4A2 70F59746

giry:
A2A9F38E F5CAFBE2 347CF7EC 24BDD5E6 24BC93BF A82771F4 0D1B65D0 6256A852
C983135D 4669F879 2F2C1D55 718AFBB4

These are concatenated to form

g^ir:
11187331 C279962D 93D60424 3FD592CB 9D0A926F 422E4718 7521287E 7156C5C4
D6031355 69B9E9D0 9CF5D4A2 70F59746 A2A9F38E F5CAFBE2 347CF7EC 24BDD5E6
24BC93BF A82771F4 0D1B65D0 6256A852 C983135D 4669F879 2F2C1D55 718AFBB4

This is the value that is used in the formation of SKEYSEED.

8.3. 521-bit Random ECP Group

IANA assigned the ID value 21 to this Diffie-Hellman group.

We suppose that the initiator’s Diffie-Hellman private key is

i:
0037ADE9 319A89F4 DABDB3EF 411AACCC A5123C61 ACAB57B5 393DCE47 608172A0
95AA85A3 0FE1C295 2C6771D9 37BA9777 F5957B26 39BAB072 462F68C2 7A57382D
4A52

Then the public key is given by g^i=(gix,giy) where

gix:
0015417E 84DBF28C 0AD3C278 713349DC 7DF153C8 97A1891B D98BAB43 57C9ECBE
E1E3BF42 E00B8E38 0AEAE57C 2D107564 94188594 2AF5A7F4 601723C4 195D176C
ED3E

giy:
017CAE20 B6641D2E EB695786 D8C94614 6239D099 E18E1D5A 514C739D 7CB4A10A
D8A78801 5AC405D7 799DC75E 7B7D5B6C F2261A6A 7F150743 8BF01BEB 6CA3926F
9582

The KEi payload is as follows.

0000008C 00150000 0015417E 84DBF28C 0AD3C278 713349DC 7DF153C8 97A1891B
D98BAB43 57C9ECBE E1E3BF42 E00B8E38 0AEAE57C 2D107564 94188594 2AF5A7F4
601723C4 195D176C ED3E017C AE20B664 1D2EEB69 5786D8C9 46146239 D099E18E
1D5A514C 739D7CB4 A10AD8A7 88015AC4 05D7799D C75E7B7D 5B6CF226 1A6A7F15
07438BF0 1BEB6CA3 926F9582

We suppose that the response Diffie-Hellman private key is

r:
0145BA99 A847AF43 793FDD0E 872E7CDF A16BE30F DC780F97 BCCC3F07 8380201E
9C677D60 0B343757 A3BDBF2A 3163E4C2 F869CCA7 458AA4A4 EFFC311F 5CB15168
5EB9

Then the public key is given by g^r=(grx,gry) where

grx:
00D0B397 5AC4B799 F5BEA16D 5E13E9AF 971D5E9B 984C9F39 728B5E57 39735A21
9B97C356 436ADC6E 95BB0352 F6BE64A6 C2912D4E F2D0433C ED2B6171 640012D9
460F

gry:
015C6822 6383956E 3BD066E7 97B623C2 7CE0EAC2 F551A10C 2C724D98 52077B87
220B6536 C5C408A1 D2AEBB8E 86D678AE 49CB5709 1F473229 6579AB44 FCD17F0F
C56A

The KEr payload is as follows.

0000008c 00150000 00D0B397 5AC4B799 F5BEA16D 5E13E9AF 971D5E9B 984C9F39
728B5E57 39735A21 9B97C356 436ADC6E 95BB0352 F6BE64A6 C2912D4E F2D0433C
ED2B6171 640012D9 460F015C 68226383 956E3BD0 66E797B6 23C27CE0 EAC2F551
A10C2C72 4D985207 7B87220B 6536C5C4 08A1D2AE BB8E86D6 78AE49CB 57091F47
32296579 AB44FCD1 7F0FC56A

The shared secret value g^ir=(girx,giry) where

```
girx:
 01144C7D 79AE6956 BC8EDB8E 7C787C45 21CB086F A64407F9 7894E5E6 B2D79B04
 D1427E73 CA4BAA24 0A347868 59810C06 B3C715A3 A8CC3151 F2BEE417 996D19F3
 DDEA

giry:
 01B901E6 B17DB294 7AC017D8 53EF1C16 74E5CFE5 9CDA18D0 78E05D1B 5242ADAA
 9FFC3C63 EA05EDB1 E13CE5B3 A8E50C3E B622E8DA 1B38E0BD D1F88569 D6C99BAF
 FA43
```

These are concatenated to form

```
g^ir:
 01144C7D 79AE6956 BC8EDB8E 7C787C45 21CB086F A64407F9 7894E5E6 B2D79B04
 D1427E73 CA4BAA24 0A347868 59810C06 B3C715A3 A8CC3151 F2BEE417 996D19F3
 DDEA01B9 01E6B17D B2947AC0 17D853EF 1C1674E5 CFE59CDA 18D078E0 5D1B5242
 ADAA9FFC 3C63EA05 EDB1E13C E5B3A8E5 0C3EB622 E8DA1B38 E0BDD1F8 8569D6C9
 9BAFFA43
```

This is the value that is used in the formation of SKEYSEED.

9. References

9.1. Normative References

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

[IANA-IKEv2] IKEv2 Parameters. (http://www.iana.org/assignments/ikev2-parameters)

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

[IKEv2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[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)

[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)

[GMN] J. Solinas, Generalized Mersenne Numbers, Combinatorics and Optimization Research Report 99-39, 1999. (http://www.cacr.math.uwaterloo.ca/)

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

[ISO-14888-3] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 14888-3:2006, 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 18031:2005, Information Technology: Security Techniques: Random Bit Generation.

[NIST] U.S. Department of Commerce/National Institute of Standards and Technology. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, NIST Special Publication Publication 800-56A, March 2006. (http://csrc.nist.gov/CryptoToolkit/KeyMgmt.html)

[RFC3526] Kivinen, T. 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, X9.62-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm. January 1999.

[X9.62-2005] American National Standards Institute, X9.62:2005: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

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

Authors' Addresses

David E. Fu
National Information Assurance Research Laboratory
National Security Agency

EMail: defu@orion.ncsc.mil

Jerome A. Solinas
National Information Assurance Research Laboratory
National Security Agency

EMail: jasolin@orion.ncsc.mil

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.