Network Working Group
INTERNET-DRAFT
Expires: April 10, 2007

D. Brown, Certicom
October 10, 2006

Additional ECC Groups For IKE and IKEv2
<draft-ietf-ipsec-ike-ecc-groups-10.txt>

Status of this Memo

Abstract

This document describes additional elliptic curve groups for use in IKE (as defined in RFC 2409) and IKEv2 (as defined in RFC 3406). These groups are defined to align IKE and IKEv2 with other ECC implementations and standards, and in addition, many of them provide higher strength than the previousley defined Oakley groups.

1. Introduction

This document describes groups for use in elliptic curve Diffie-Hellman in IKE in addition to the Oakley groups included in [IKE], [IKEv2], and [MODP-IKE]. The document assumes that the reader is familiar with the IKE protocol and the concept of Oakley Groups, as defined in RFC 2409 [IKE] and IKEv2 [IKEv2]. The ECC groups given here are among the fifteen groups that NIST recommends in FIPS 186-2 [FIPS-186-2].

RFC2409 [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. Both elliptic curve groups (Oakley Groups 3 and 4) are defined over GF[2^N] with N composite.

Additional groups that can be used with IKE and IKEv2 are defined in [MODP-IKE].

This document describes all fifteen elliptic curve groups recommended by NIST in [FIPS-186-2].

The reasons for supporting the 15 NIST ellipitc curve groups are for better alignment with other standards, such as [FIPS 186-2], [X9.62], [X9.63], and [SEC-2]. Some of these groups also afford efficiency advantages in hardware applications since the underlying arithmetic is binary field arithmetic. The groups described are capable of providing security consistent with both the new Advanced Encryption Standard [FIPS-197] and with Triple DES [SP-800-67].

These groups could also be defined with the New Group Mode but including them in this document will encourage interoperability of IKE and IKEv2 implementations based on elliptic curve groups.

2. The Additional Elliptic Curve Groups

The groups given in this document are capable of providing security consistent with AES keys of 128, 192, and 256 bits, and also with 3DES keys of lengths 168, whose corresponding strengths is often rated at **112 bits.** Additionally a lower security level, of 80 bits, is also supported for backwards compatability. The following table, based on tables from [HOF] and [LEN], gives approximate comparable key sizes for security stregnths for selected ECC key sizes by comparison symmetric key sizes. The estimates are based on the running times of the best algorithms known today.

Strength	ECC2N	ECP
80	163	192
112	233	224
128	283	256
192	409	384
256	571	521

Table 1: Comparable key sizes

Thus, for example, when securing a 192-bit symmetric key, it is prudent to use either 409-bit ECC2N or 384-bit ECP. With smaller ECC key sizes the symmetric keys would be underprotected.

The fifteen groups described in this document use elliptic curves over GF[2^N] with N prime or over GF[P] with P prime. This addresses concerns expressed by many experts regarding curves defined over GF[2^N] with N composite -- concerns highlighted by the recent attacks on such curves due to Gaudry, Hess, and Smart [WEIL] and due to Jacobson, Menezes and Stein [JMS].

Seven of the groups described here have been assigned identifiers by IANA [IANA] and the remaining eight might later be assigned identifiers by IANA. A brief summary of the IANA identified groups for IKE follows. Groups with IANA numbers 1 through 4 are identified in [IKE]. The group with IANA number 5 is identified in [MODP-IKE]. The group with IANA number 6, [X9.62] and [SEC 2], with object identifier sect163r1, but it is not one of the fifteen curves that NIST recommends [FIPS-186-2]. Nevertheless, it is included here for backwards interoperability with existing implementations. The remaining NIST recommended groups are suggested and anticipated to be assigned IANA numbers as specified in Table 2.

id	Group Type	Group Description	NIST Name	SEC 2 OID
22	2 ECP	ECPRGF192Random	P-192	secp192r1
23	3 EC2N	EC2NGF163Random	B-163	sect163r2
7	3 EC2N	EC2NGF163Koblitz	K-163	sect163k1
6	3 EC2N	EC2NGF163Random2	none	sect163r1
24	2 ECP	ECPRGF224Random	P-224	secp224r1
25	3 EC2N	EC2NGF233Random	B-233	sect233r1
26	3 EC2N	EC2NGF233Koblitz	K-233	sect233k1
19	2 ECP	ECPRGF256Random	P-256	secp256r1
8	3 EC2N	EC2NGF283Random	B-283	sect283r1
9	3 EC2N	EC2NGF283Koblitz	K-283	sect283k1
20	2 ECP	ECPRGF384Random	P-384	secp384r1
10	3 EC2N	EC2NGF409Random	B-409	sect409r1
11	3 EC2N	EC2NGF409Koblitz	K-409	sect409k1
21	2 ECP	ECPRGF521Random	P-521	secp521r1

12	3 EC2N	EC2NGF571Random	B-571	sect571r1
13	3 EC2N	EC2NGF571Koblitz	K-571	sect571k1

Table 2. Recommended Groups and Names

Generally, three curves are defined at each strength. Two curves chosen verifiably at random, which helps security in that the elliptic curve is thereby unlikely to belong to some rare but weak classe of curves. One verifiably random is defined over a prime field, and another over a prime field. The third curve is Koblitz curve defined over a binary field. These curves are special curves with some efficient implementation properties due to the special structure of the curve [KOB] and [SOL]. Generally speaking, curves defined over prime field are more efficient than those over binary fields when implemented software, because typical platforms for software have built-in 32-bit integer multipliers or better. In hardware implementations, binary fields potentially offer more efficient implementation.

For elliptic curve groups, the data in the KE payload when using this group is the octet string representation specified in [SEC1], [X9.62], [X9.63], [FIPS-186-2], and [IEEE-1363] of the point on the curve chosen by taking the randomly chosen secret Ka and computing Ka*G, where * is the repetition of the group addition.

In this representation, a leading octet with value 02,03, or 04, indicates whether the point is compressed and uncompressed, and if compressed, which of the two choices for the y-coordinate. The coordinates are represented as octet strings consisting of initial padding of zero bits, if needed, followed by a bit string of length corresponding to the field size. For binary fields, a polynomial basis representation is used, with irreducible polynomials specified in this document in the corresponding subsection describing the group.

If the initiator chooses secret i and the responder chooses secret r, then the KEi is i*G and KEr is r*G. The formatting of KEr is identical to that for KEi.

The raw shared secret is the x-coordinate (only) of (ir)*G, using the same representation of field elements as octet strings that is used the x-coordinate inside of KEi and KEr.

Implementations of this document MUST support one of the groups in Table 2. The groups in Table 2 are arranged to 5 classes, corresponding to approximately equivalent security strength. To encourage interoperability, implementations that support one of these classes, SHOULD support the one group in that class that is defined over a prime field (which will be one of P-192, P-224, P-256, P-384, or P-521). Implementations SHOULD support one of P-256 or P-384. Implementations MAY support any set of groups.

The groups are now described in greater detail. The order follows the proposed id number of the group, which does match not the order of Table 2 (based on security) for historical reasons.

2.1 Group EC2NGF163Random2

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 6 (six). The curve is based on the Galois Field GF[2^163]. The field size is 163. **The irreducible polynomial used to represent the field is:**

u^163 + u^7 + u^6 + u^3 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + ax^2 + b.

Group Curve a:

07b6882c aaefa84f 9554ff84 28bd88e2 46d2782a e2

Group Curve b:

0713612d cddcb40a ab946bda 29ca91f7 3af958af d9

Group Generator G:

03036997 9697ab43 89778956 6789567f 787a7876 a654

The order of the generator G defined above is the prime:

03ffffff ffffffff ffffff48 aab689c2 9ca71027 9b

The curve order is twice this prime.

The group was chosen verifiably at random using SHA-1 as specified in [X9.62] from the seed:

24b7b137 c8a14d69 6e676875 6151756f d0da2e5c

However, for historical reasons, the method to generate the group from the seed differs slightly from the method described in [X9.62]. Specifically the coefficient Group Curve b produced from the seed is the reverse of the coefficient that would have been produced by the method described in [X9.62].

2.2 Group EC2NGF163Koblitz

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 7 (seven). The curve is based on the Galois Field GF[2^163]. The field size is **163. The irreducible polynomial used to represent the field is:**

u^163 + u^7 + u^6 + u^3 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + x^2 + 1.

Group Generator G:

0302fe13 c0537bbc 11acaa07 d793de4e 6d5e5c94 eee8

The order of the generator G is the prime:

04000000 00000000 00000201 08a2e0cc 0d99f8a5 ef

The curve order is twice this prime.

2.3 Group EC2NGF283Random

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 8 (eight). The curve is based on the Galois Field GF[2^283]. The field size is **283. The irreducible polynomial used to represent the field is:**

u^283 + u^12 + u^7 + u^5 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + x^2 + b.

Group Curve b:

027b680a c8b8596d a5a4af8a 19a0303f ca97fd76 45309fa2 a581485a

f6263e31 3b79a2f5

Group Generator G:

0305f939 258db7dd 90e1934f 8c70b0df ec2eed25 b8557eac 9c80e2e1
98f8cdbe cd86b120 53

The order of the generator G is the prime:

03ffffff ffffffff ffffffff ffffffff ffffef90 399660fc 938a9016
5b042a7c efadb307

The curve order is twice this prime.

The group was chosen verifiably at random in normal basis
representation using SHA-1 as specified in [X9.62] from the seed:

77e2b073 70eb0f83 2a6dd5b6 2dfc88cd 06bb84be

2.4 Group EC2NGF283Koblitz

IKE and IKEv2 implementations MAY support an EC2N group with the
following characteristics. This group is assigned id 9 (nine). The
curve is based on the Galois Field GF[2^283]. The field size is
283. **The irreducible polynomial used to represent the field is:**

u^283 + u^12 + u^7 + u^5 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + 1.

Group Generator G:

02050321 3f78ca44 883f1a3b 8162f188 e553cd26 5f23c156 7a168769
13b0c2ac 24584928 36

The order of the generator G is the prime:

01ffffff ffffffff ffffffff ffffffff ffffe9ae 2ed07577 265dff7f
94451e06 1e163c61

The curve order is four times this prime.

2.5 Group EC2NGF409Random

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 10 (ten). The curve is based on the Galois Field GF[2^409]. The field size is 409. **The irreducible polynomial used to represent the field is:**

u^409 + u^87 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + x^2 + b.

Group Curve b:

021a5c2c 8ee9feb5 c4b9a753 b7b476b7 fd6422ef 1f3dd674 761fa99d
6ac27c8a 9a197b27 2822f6cd 57a55aa4 f50ae317 b13545f

Group Generator G:

03015d48 60d088dd b3496b0c 60647562 60441cde 4af1771d 4db01ffe
5b34e597 03dc255a 868a1180 515603ae ab60794e 54bb7996 a7

The order of the generator G is the prime:

10000000 00000000 00000000 00000000 00000000 00001e2a
ad6a612f 33307be5 fa47c3c9 e052f838 164cd37d 9a21173

The curve order is twice this prime.

The curve was chosen verifiably at random in normal basis representation using SHA-1 as specified in [X9.62] from the seed:

4099b5a4 57f9d69f 79213d09 4c4bcd4d 4262210b

2.6 Group EC2NGF409Koblitz

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 11 (eleven). The curve is based on the Galois Field GF[2^409]. The field size is 409. **The irreducible polynomial used to represent the field is:**

u^409 + u^87 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + 1.

Group Generator G:

030060f0 5f658f49 c1ad3ab1 890f7184 210efd09 87e307c8 4c27accf
b8f9f67c c2c46018 9eb5aaaa 62ee222e b1b35540 cfe90237 46

The order of the generator G is the prime:

7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffe5f83
b2d4ea20 400ec455 7d5ed3e3 e7ca5b4b 5c83b8e0 1e5fcf

The curve order is four times this prime.

2.7 Group EC2NGF571Random

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 12 (twelve). The curve is based on the Galois Field GF[2^571]. The field size is **571. The irreducible polynomial used to represent the field is:**

u^571 + u^10 + u^5 + u^2 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + x^2 + b.

Group Curve b:

2f40e7e2 221f295d e297117b 7f3d62f5 c6a97ffc b8ceff1c d6ba8ce4
a9a18ad8 4ffabbd8 efa59332 be7ad675 6a66e294 afd185a7 8ff12aa5
20e4de73 9baca0c7 ffeff7f2 955727a

Group Generator G:

03030300 1d34b856 296c16c0 d40d3cd7 750a93d1 d2955fa8 0aa5f40f
c8db7b2a bdbde539 50f4c0d2 93cdd711 a35b67fb 1499ae60 038614f1
394abfa3 b4c850d9 27e1e776 9c8eec2d 19

The order of the generator G is the prime:

3fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff fffffffe 661ce18f f5598730 8059b186 823851ec 7dd9ca11
61de93d5 174d66e8 382e9bb2 fe84e47

The curve order is twice this prime.

The group was chosen verifiably at random in normal basis representation using SHA-1 as specified in [X9.62] from the seed:

2aa058f7 3a0e33ab 486b0f61 0410c53a 7f132310

2.8 Group EC2NGF571Koblitz

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 13 (thirteen). The curve is based on the Galois Field GF[2^571]. The field size is 571. The irreducible polynomial used to represent the field is:

u^571 + u^10 + u^5 + u^2 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + 1.

Group Generator G:

02026eb7 a859923f bc821896 31f8103f e4ac9ca2 970012d5 d4602480
4801841c a4437095 8493b205 e647da30 4db4ceb0 8cbbd1ba 39494776
fb988b47 174dca88 c7e29452 83a01c89 72

The order of the generator G is the prime:

20000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000001 31850e1f 19a63e4b 391a8db9 17f4138b 630d84be
5d639381 e91deb45 cfe778f6 37c1001

The group order is four times this prime.

2.9 Group ECPRGF384Random

IKE and IKEv2 implementations MAY support an ECP group with the following characteristics. This group is assigned id 22 (twenty-two). The curve is based on the integers modulo the generalized Mersenne prime p given by

p = 2^192 - 2^64 - 1.

The equation for the elliptic curve is:

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

Group Curve b:

64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1

Group Generator G:

03188da8 0eb03090 f67cbf20 eb43a188 00f4ff0a fd82ff10 12

The order of the generator G is the prime:

ffffffff ffffffff ffffffff 99def836 146bc9b1 b4d22831

The group was chosen verifiably at random using SHA-1 as specified in [X9.62] from the seed:

3045ae6f c8422f64 ed579528 d38120ea e12196d5

2.10 Group EC2NGF163Random

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 23 (twenty-three). The curve is based on the Galois Field GF[2^163]. The field size is 163. The irreducible polynomial used to represent the field is:

u^163 + u^7 + u^6 + u^3 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + x^2 + b.

Group Curve b:

020a6019 07b8c953 ca1481eb 10512f78 744a3205 fd

Group Generator G:

0303f0eb a16286a2 d57ea099 1168d499 4637e834 3e36

The order of the generaotr G above is the prime:

04000000 00000000 00000292 fe77e70c 12a4234c 33

The curve order is twice this prime.

The group was chosen verifiably at random in normal basis representation using SHA-1 as specified in [X9.62] from the seed:

85e25bfe 5c86226c db12016f 7553f9d0 e693a268

2.11 Group ECPRGF224Random

IKE and IKEv2 implementations MAY support an ECP group with the following characteristics. This group is assigned id 24 (twenty-four). The curve is based on the integers modulo the generalized Mersenne prime p given by

p = 2^224 - 2^96 + 1.

The equation for the elliptic curve is:

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

Group Curve b:

b4050a85 0c04b3ab f5413256 5044b0b7 d7bfd8ba 270b3943 2355ffb4

Group Generator G:

02b70e0c bd6bb4bf 7f321390 b94a03c1 d356c211 22343280 d6115c1d 21

The order of the generator G is the prime:

ffffffff ffffffff ffffffff ffff16a2 e0b8f03e 13dd2945 5c5c2a3d

The group was chosen verifiably at random using SHA-1 as specified in [X9.62] from the seed:

bd713447 99d5c7fc dc45b59f a3b9ab8f 6a948bc5

2.12 Group EC2NGF233Random

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 25 (twenty-five). The curve is based on the Galois Field GF[2^233]. The field size is 233. The irreducible polynomial used to represent the field is:

u^233 + u^74 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + x^2 + b.

Group Curve b:

0066647e de6c332c 7f8c0923 bb58213b 333b20e9 ce4281fe 115f7d8f 90ad

Group Generator G:

0300fac9 dfcbac83 13bb2139 f1bb755f ef65bc39 1f8b36f8 f8eb7371 fd558b

The order of the generator G above is the prime:

01000000 00000000 00000000 00000013 e974e72f 8a692203 1d2603cf e0d7

The curve order is twice this prime.

The group was chosen verifiably at random in normal basis representation using SHA-1 as specified in [X9.62] from the seed:

74d59ff0 7f6b413d 0ea14b34 4b20a2db 049b50c3

2.13 Group EC2NGF233Koblitz

IKE and IKEv2 implementations MAY support an EC2N group with the following characteristics. This group is assigned id 26 (twenty-six). The curve is based on the Galois Field GF[2^233]. The field size is 233. The irreducible polynomial used to represent the field is:

u^233 + u^74 + 1.

The equation for the elliptic curve is:

y^2 + xy = x^3 + 1.

Group Generator G:

02017232 ba853a7e 731af129 f22ff414 9563a419 c26bf50a 4c9d6eef ad6126

The order of the generator G is the prime:

80000000 00000000 00000069d 5bb915bc d46efb1a d5f173ab df

The curve order is four times this prime.

3. Test Vectors

What follows is a set of test vectors, in the form:

<SEC 2 name for elliptic curve group>

i = <initiator secret value>

r = <responder secret value>

KEi = <initiator key exchange payload>

KEr = <responder key exchange payload>

Z = <raw shared secret>

Here are the test vectors:

secp192r1

i = 7092e5fd 43a17f6a 33753259 89284eba 093564e1 944e176d

r = d6185566 ec0b1f52 cc562765 60907cb1 a8683d84 49b882ce

KEi = 00000021 00160000 03841c98 8076d857 fdda4ccf 3bae5cf5 f521336a
650fdc7d c4

KEr = 00000021 00160000 03445a52 f30ce615 c53e1175 c04db6f0 bb7a03d3
096e2c20 9e

Z = cac49383 d8bf6b5f d8e5d5b7 69c0a91f 68f9b5d0 91b831d8

secp224r1

i = 626167f5 e4365260 7a9cc400 35c6dca7 256fa372 1a68baf4 e40f86e1

r = 38524a05 e71d0233 61bfdb29 0b69d15b 7d8390aa 5ac837a0 c82d9f63

KEi = 00000025 00180000 029167b2 a96e1cbd e468976e 364d4d31 10c8f58f
579c44a0 be3c98a1 a8

KEr = 00000025 00180000 02dc7765 dea1a085 f3f077f1 38854fe0 850ca89c
2e32d037 7bde2458 15

Z = 7b1bf042 33c15681 ba530222 1a2ce34b 18a92dbb b37cc0a7 72a91516

secp256r1

i = 9d3ae814 8192a83f 20530cb2 5edb11e8 b7ea1358 3a70ca34 5b0f571b
91317abe

r = 922d3e7c 675bb9b4 d9613ff2 1793991b 3623844f 072e53d2 8a6baff8
9cf85ab4

KEi = 00000029 00130000 03084cc4 7b198b64 0da01bc1 0dfcfa03 4db89dbb
072ea0ae 9cd6eac6 0900ffc4 92

KEr = 00000029 00130000 02b9528b 7eb56463 4315ebe2 f1e3e4fa bd671d8e
6f487b6e e35796a6 a6daaed1 f7

Z = 52c8f824 e13b4065 1b0ec4ad 8dbdb116 b15aebc4 8fbc0360 d84ff8cd
c3c73e6c

secp384r1

i = 52d3051d 6675ed1e 52a4e922 4fb2ad9a 910358bb 9a72ddf7 d96a2383
bad90ef8 15f83a94 edfe52a0 1193f843 d29f1958

r = f13ba470 9dee2f45 32b251bf b3b1b87b 1adac356 299e4ea9 472356ac
a6ddad29 0b00f221 4740f693 c6a03c2d c52bd419

KEi = 00000039 00140000 032991ae 8b27d708 0db61914 0023dc72 41cdbcd8
130de451 f9268c42 0674b816 9973f89b e2f3d9f3 082cb049 511457db 35

KEr = 00000039 00140000 0270a447 c2e24022 c3a52f95 634a1705 2a02831c
ca790e6f 0c1feff9 515a38cf d7c487ab d9e19e8f 4ef49b8a 4b268b1a 0f

Z = f3cde42e 0e9dd289 82294ac1 af62cbd1 429f2899 11b3e053 5a81ebb5
13a2903b c53f0ecd 5c511083 5e5a4a90 3629b0c5

secp521r1

i = ea78946a bd68bb79 a55f8f99 93cf5389 fbb0a10d 3b580624 29c6322a
987c957f 8854a5a4 ec636d70 2a7b0753 7341f631 9cc6d03c 447da5e9
f59d2846 0caa98db eb

r = e68807bb dc90cca2 7848c6bc 38426ddf 5b19c09d 144d0417 06bc9ed1
afade9e8 1585faf9 e173f340 001016ef 82ea5b4a 8b785fee 0c403a6e
39228df6 2a337e47 9c

KEi = 0000004b 00150000 0300584c 2476258d d61c0987 61710976 c4b50fc4
c47177f4 2562f2d5 75bf933c 7699122b c37c77da 0a7079e0 a4c2d131
8d337642 41e4c562 c7ff7bad 5cf0ce1e dddfa0

KEr = 0000004b 00150000 02011483 326d756d 8600c5d8 c6a0bc60 c80297c3
7e3368f4 5bbcf4d5 db78ad4b 1b1d8584 b019416f 92e8e65f 5fe370fb
35558a61 32790304 2ae79809 5c5638e0 93a0b4

Z = 006ea860 d9c8518c e2de03a0 0a9d4c66 48cd33cb 665302c9 e41163e9
b6b7eded f892c9c8 5c63d7c2 cc76e3c2 f3cfe2fd 8cd13314 658f6f4d
a6198dd9 fd99cd42 de1b

sect163r1

i = 647f8bc4 fa3fa625 b41456b9 1c899269 ffe277bc

r = ef8fa305 ed836a8f df206e65 94f086f9 762e6f69

KEi = 0000001e 00060000 0300e772 d9e512e9 71a512b9 406edce9 99b50bee
78b2

KEr = 0000001e 00060000 020115ed 6148869f 8be39923 0825b220 7ee9e494
9381

Z = 01d75dd0 142db15a 25b6f802 4bab20ee 78f90f40 9f

sect163r2

i = 027e06da 864be386 2c261654 c15ec556 8e45eb7f b6

r = 03a7c88f a7363f8f f9ff1d28 13027089 bd96e07c 48

KEi = 0000001e 00170000 0302ed80 fc3986c4 a978b09c 34dcbc37 6a7975b9
2276

KEr = 0000001e 00170000 0201aed6 520fb246 8fb424de c3c31c4a 1fc0e1cf
702a

Z = 07befaa4 0951cf0d 1c972d4d f6297d5c 30b726cf 98

sect163k1

i = 0137fb36 360a457b 6a23b29e 11a4760a 17788180 8a

r = 010c489b bb3b602a 7df626e9 f0625294 b1d795a0 32

KEi = 0000001e 00070000 0305be09 5b082931 8fa0e3e0 096e31bf b829b8ee
95ec

KEr = 0000001e 00070000 0205d9c9 45eb02de c3b7ad1b ace077bf 37753e33
26b3

Z = 07b13e8c 9452ab89 11368072 5df13128 c055c9d3 ce

sect233r1

i = 5b038de5 0df0f1f4 9a06c1fb 46c45d5a c63e4541 b99df194 21c33b79 02

r = 3b48a626 65e29c5f 78ff6b77 14c1bb82 ad210c8c 29572eac cbdc3abb ce

KEi = 00000027 00190000 0301334d 9878fa49 d0dbbf59 78f49e57 aeaad93a
1c3fbd7a 17acc369 dd68d1

KEr = 00000027 00190000 030158db 2605ce54 3cc42202 48bcce6c c055d8d4
ee4ea1e4 9ef1b9dd 823797

Z = 00b0dcfc 6d66c3d1 d987f8b0 75edc927 63257bfc baa7af34 b8f6242d
5d3c

sect233k1

i = 4ea153c3 05784cf0 23a54756 a99281e1 a8105ab8 5bb63898 0d07de46 a2

r = 424a8945 1d6cd439 305e44f0 6fc574ec 8268b626 560a44ee 85b624d5 89

KEi = 00000027 001a0000 03014e27 1e22edf7 df456f59 b366b846 2c5f6ef2
6bddfb67 ed764a5b 39e6dc

KEr = 00000027 001a0000 02014b56 33f29fdf 353ebb63 75ddffec 46f162f4
19d7962a 8d04fdb9 3e38ee

Z = 00f3ef41 79b17ceb 7e041581 727d01cf 3d7423ec 249f44d3 53d1e2de
7412

sect283r1

i = 0294203a b7551182 dec6b777 f4d1c65b db752752 17a356a7 efad1303
55aa3f17 aeb3852f

r = 03314912 0a7d8d98 4f2c3346 d9ec8896 2f5b0545 1d5ead84 3dd278de
df49bd84 24009110

KEi = 0000002d 00080000 0201959e 200deaa6 2d055e1d 4e141ed7 dcdfde81
05708644 31cc5a28 0a229418 b8dfc4c1 86

KEr = 0000002d 00080000 03034237 aff2fae3 1d2bed60 3ba7e0aa 9cbefee1
313bec69 05f40e27 0cf448c3 6ec7d959 81

Z = 066c0249 c890ffed a0ce0fd3 bd76a650 6423f868 5e649d03 5842bf25
a388ec4e dd207eff

sect283k1

i = 09024924 08f4d64e 351eabe7 b9da659f 089a20a2 d19f62b9 2499a3eb
f2410637 4ab51b

r = 0e2a59cb 494b4978 4436e053 2cf25ee4 44225ffd 39139bba 2e19d3ba
e482f651 368716

KEi = 0000002d 00090000 02044e95 ad563972 553e8c29 c89e4f57 155c1799
38ec1b86 4487e287 fe94a48b a59de2f4 4b

KEr = 0000002d 00090000 030658a1 8c6946e1 9f17a1f8 eb44b461 0d0052c9

Z = 0194027a d85e4075 d89247b2 e3c3500d ebff0dce 5ad63a02 a07652df
b7da3b75 afe11e88

sect409r1

i = 18624d82 5f61d687 d6f7707f f35a23b3 29feea91 3ec45afe 81d79e4a
09b7d026 e8da7fb4 0f972a53 d6fa1e6f 0de235c7 81254b

r = f73eec0f 98ab794f 0633f4ee 84cca2f8 dc1a1fde be850337 6418029c
5cf14e34 788d8ea3 2857128c 67297413 902e9dd7 b8c730

KEi = 0000003d 000a0000 02016f9e 561b996d 1d3ac272 0e7cace8 6cc96d58
c2518814 ff922096 38daee25 6e405590 cbd7a05c 2a4e24da ec0bf005
777e89eb 49

KEr = 0000003d 000a0000 0300ea45 1ad0be01 cdeba8f3 b7c12708 10f8725f
03e76768 bd07cd78 cbd7a1c4 d354abba 3615658e f81e397d 99b6c261
a77f7103 f5

Z = 00beb0ec d7886e0b c13dead1 43621dd1 7133dbda e112b0f9 168ee853
e259c5b0 26b4582f 6ccb69cd e62c7000 fbb3545d 2d89e25f

sect409k1

i = 600b86e2 0b7a66d8 af5cd1e3 a22adbcf 1f6e6556 3dd932af 6589d095
3b517a56 6f6230de 70f36839 9c13533e cba32924 90cbfb

r = 77d67725 0e919500 a410cbb0 2c6842d9 c12fa8a8 b57f539d a192a025
b92b4166 e317b757 64a42358 54ed3dac 477483de 03e2f2

KEi = 0000003d 000b0000 0300964b 2b145579 51de6ffe a67eec42 39a26600
22a45b26 59db5d92 4251c400 5b0d4de3 47b6fde7 6fc43bce 546d7cd4
f977d579 7a

KEr = 0000003d 000b0000 03016ecd 20beea51 7ae36a40 e330d8a5 6812559f
5e5ffd16 fa6716f9 53814d9b f37570d7 9b180687 b5a385bf b9420f25
50e4b613 8e

Z = 00a1f44a 752e980f 3db78ee5 62786949 afa2e586 7d8cc9cf 078c8f54
a7de9107 af70fc87 6f5bd1e1 94c53e7a 56043397 ef2c8b50

sect571r1

i = e422d840 0d8e6299 90c7ca8b 26b74a0d 873d8d6d 906f4af6 e44c6176
63327773 f0a1c5f0 355ac9dc b2c4c0b6 a13e38e1 8b35cda6 65a1e513
4be36044 d3d38778 9e01c2be 6d0713

r = 01e58461 bb4f5bbb 737dfe61 7150968b 2a9773e7 f4425ac5 a40a9ef4
280f97d7 a057b2df 91b3ccf7 7beb2990 596e998f d57b3c42 a46e694f
af1923a6 b1899a70 6ce4b346 424b1b7d

KEi = 00000051 000c0000 0302c17e 8482e65e 8eafd4eb e150bf93 fd8797db
78b7c365 39724d69 79c7b2b9 428be38e 0bbf94f6 43bd6647 477a33e5
89cb491b 1f2015f9 bb5e5999 153de52d 8150e50e c557c720 da

KEr = 00000051 000c0000 03030e89 d2c1aa8a 278e43b8 53066adf 742fdd74
91414d90 7a74c011 371bdf64 dc38502f 2e18ae79 ac702400 5398959d
e999e259 65294561 024ff0b5 10855f27 263dd0d1 cff78cbe b3

Z = 0579791f f1725f09 c70e7378 278137c0 7dcb5c41 2b30f7ae 681a8681
41404ea9 5d945f26 d4d0da1b a3860291 5b67184e 23288e4f 3021b578
02821d44 94868987 1e68cfc2 82862cc5

sect571k1

i = 01fb96e0 fb6f5c57 03b258e0 32ee9cf3 fc5eb27b 37bfc797 cf7954ef
82e37cfa 551e5492 08af3365 882343cf fc7fca72 949b3346 ff49cd32
51a3a172 00a0eef8 b64bce70 a5087cad

r = 2b25d3d5 fd86cb53 a0fef2fb 4ffc4e20 f1ac33a1 47d69d45 31676dfd
8a92a6b9 bf6c3437 9189eba8 7679bdee 05e0f8a4 5790fb77 e4fc47c7
babe4170 839a93be b58e214c 1a8470

KEi = 00000051 000d0000 0301e4dc 1f82924e a99921ba bda3ee48 792836ec
1d033578 e7a3d372 f9360118 2b511589 d2a84d9f ab6e86d5 ea8f00dd
df5c8b1c 22bbd9bc 96b191da 5bab247a f9e666e6 824ffe2b 72

KEr = 00000051 000d0000 02049667 3c15e735 aba12ea6 a1413c4e a6e50edd
ec8f21b2 22df4092 5f483d85 e779f48e 3439f881 18e325f6 e3aa6e4e
e2855440 79ed2ea4 d8680b5d 9c06ab23 2944e62e 93e1cf8f 9b

Z = 066c0d8b cf8c17f2 7d7367bf 0e8a9c29 31fa258b e3b7861a 6c021a5b
b52d214a b1923528 0e9c6b61 bf72c20a 8d64c26a 9a4b9ff0 75fd3be6
be03c33c 56e6cf3f f7517e5b 08dcbe65

4. Security Considerations

Since this document describes some groups for use within IKE and IKEv2, many of the security considerations contained within RFC 2409 apply here as well.

Many of the groups described in this document offer higher strength than the groups in RFC 2409. This allows the IKE and IKEv2 to offer security comparable with the AES algorithms.

In addition, since all the groups are defined over GF[P] with P prime or GF[2^N] with N prime, they address the concerns expressed regarding the elliptic curve groups included in RFC 2409, which are curves defined over GF[2^N] with N composite. The work of Gaudry, Hess, and Smart [WEIL] reveal some of the weaknesses in such groups.

5. IANA Considerations

It is propose that the id column Table 2 be defined as the IANA numbers that MUST be used in IKE and IKEv2 to identify the groups specified in this document.

6. 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.

7. Acknowledgments

Tero Kivinen, Eric Fung, Alfred Hoenes and Russ Housley provided valuable comments and suggestions.

8. References

[ECP-IKE] D. Fu, J. Solinas, ECP Groups for IKE and IKEv2, draft-ietf-ipsec-ike-ecp-groups-03.txt, work in progress.

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

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

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

[IANA-IKEv2] Internet Assigned Numbers Authority. Internet Key Exchange Version 2 (IKEv2) Parameters - Diffie-Hellman Transform Ids. http://www.iana.org/assignments/ikev2-parameters

[IEEE-1363] Institute of Electrical and Electronics Engineers. IEEE 1363-2000, Standard for Public Key Cryptography. IEEE Microprocessor Standards Committee. August 2001. See: http://grouper.ieee.org/groups/1363/index.html

[KOB] N. Koblitz, CM curves with good cryptographic properties. Proceedings of Crypto '91. Pages 279-287. Springer-Verlag, 1992.

[FIPS-186-2] National Institute of Standards and Technology. Digital Signature Standard (DSS), FIPS PUB 186-2, January 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[FIPS-197] National Institute of Standards and Technology. Advanced Encryption Standard (AES), FIPS PUB 197, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[SP-800-56] E. Barker, D. Johnson, and M. Smid, NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. March 2006. http://csrc.nist.gov/publications/nistpubs/800-56A/sp800-56A_May-3-06.pdf

[SP-800-67] W. C. Barker, NIST Special Publication 800-67, Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher. May 2004. http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

[HOF] P. Hoffman and H. Orman, Determining strengths for public keys used for exchanging symmetric keys, Internet-draft. August 2000.

[LEN] A. Lenstra and E. Verhuel, Selecting cryptographic key sizes. See: http://www.cryptosavvy.com.

[JMS] M. Jacobson, A. Menezes and A. Stein, Solving Elliptic Curve Discrete Logarithm Problems Using Weil Descent, Combinatorics and Optimization Research Report 2001-31, May 2001. See: http://www.cacr.math.uwaterloo.ca/.

[MODP-IKE] T. Kivinen and M. Kojo, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), rfc3526.txt, May 2003.

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

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

[SOL] J. Solinas, An improved algorithm for arithmetic on a family of elliptic curves, Proceedings of Crypto '97, Pages 357-371,

Springer-Verlag, 1997.

[WEIL] Gaudry, P., Hess, F., Smart, Nigel P. Constructive and Destructive Facets of Weil Descent on Elliptic Curves, HP Labs Technical Report No. HPL-2000-10, 2000. See: http://www.hpl.hp.com/techreports/2000/HPL-2000-10.html

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

[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.

9. Author's Addresses

Daniel R. L. Brown
Certicom Corp.
5520 Explorer Drive, 4th Floor,
Mississauga, Ontario, L4W 5L1
Canada
dbrown@certicom.com

10. Full Copyright Statement