Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 9, 2013

J. Merkle
secunet Security Networks
M. Lochter
Bundesamt fuer Sicherheit in der Informationstechnik (BSI)
November 5, 2012

Using the ECC Brainpool Curves for IKEv2 Key Exchange
draft-merkle-ikev2-ke-brainpool-01

Abstract

This document specifies the use of ECC Brainpool elliptic curve groups for key exchange in the Internet Key Exchange version 2 (IKEv2) protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 9, 2013.

Copyright Notice

Table of Contents

1. Introduction

In RFC 5639 [RFC5639], a new set of elliptic curve groups over finite prime fields for use in cryptographic applications was specified. These groups, denoted as ECC Brainpool curves, were generated in a verifiably pseudo-random way and comply with the security requirements of relevant standards from ISO [ISO1] [ISO2], ANSI [ANSI1], NIST [FIPS], and SecG [SEC2].

While the ASN.1 object identifiers defined in RFC 5639 allow usage of the ECC Brainpool curves in certificates and certificate revocation lists, their utilization for key exchange in IKEv2 [RFC4306] requires the definition and assignment of additional transform IDs in the respective IANA registry. This document specifies tranform IDs for four curves from RFC 5639. Furthermore, the encoding of the key exchange payload and derivation of the shared secret are defined, because previous RFCs specified this encoding only for the curves proposed therein.

2. IKEv2 Key Exchange using the ECC Brainpool Curves

2.1. Diffie-Hellman Group Transform IDs

In order to use the ECC Brainpool curves for key exchange within IKEv2, the Diffie-Hellman Group Transform IDs (Transform Type 4) listed in the following table are to be registered with IANA [IANA-IKE2]. The parameters associated with these curves are defined in RFC 5639 [RFC5639].

Curve	Transform ID
brainpoolP224r1	TBD1
brainpoolP256r1	TBD2
brainpoolP384r1	TBD3
brainpoolP512r1	TBD4

Table 1

The corresponding "twisted curves" defined in RFC 5639 can be used by implementations without having separate transform IDs defined: points (x,y) of any curve listed in Table 1 can be efficiently transformed to the corresponding point (x',y') on the twisted curve of same bit length - and vice versa - by setting (x',y') = (x*Z^2, y*Z^3) with

the coefficient Z specified for that curve in RFC 5639.

Test vectors for the groups defined by the ECC Brainpool curves are provided in Appendix A

2.2. Key Exchange Payload and Shared Secret

RFC4306 [RFC4306] only specifies the use of MODP groups and GF[2^N] elliptic curve groups for Diffie-Hellman key exchange with IKEv2. For Diffie-Hellman groups of elliptic curves defined over prime fields (ECP Diffie-Hellman groups), however, the format of key exchange payloads and the derivation of a shared secret has thus far not been specified generally but on a group-by-group basis. To accomodate for different bandwidth limitations, for the groups defined in this document, two different methods for encoding the key exchange payload, compressed and uncompressed, are specified.

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 be computed from the corresponding coordinate using the FieldElement-to-OctetString conversion method specified in [SEC1] and MUST have bit length as indicated in Table 2. This length is enforced by the FieldElement-to-OctetString conversion method, if necessary, by prepending the value with zeros.

Curves	Bit lengths
brainpoolP224r1	224
brainpoolP256r1	256
brainpoolP384r1	384
brainpoolP512r1	512

Table 2

From these components, the key exchange payload MUST be computed

using one of the two following encodings.

1. Uncompressed. This method equals the method specified in RFC 5903 [RFC5903] for the ECP curves proposed therein. The key exchange payload is defined as the concatenation of the x and y coordinates. Using this method, the bit length of the key exchange payload is twice the bit length of each component listed in Table 2. If a peer receives a key exchange payload for an ECC Brainpool curve having twice the bitlength indicated for that curve in Table 2, it MUST assume that the uncompressed encoding has been used.

2. Compressed. The key exchange payload is defined as x. Using this method, the bit length of the key exchange payload equals the bit length of each component listed in Table 2. If a peer receives a key exchange payload for an ECC Brainpool curve having the bitlength indicated for that curve in Table 2, it MUST assume that the compressed encoding has been used.

The Diffie-Hellman shared secret value MUST be computed from the x coordinate of the Diffie-Hellman common value using the FieldElement-to-OctetString conversion method specified in [SEC1] and MUST have bit length as indicated in the Table 2. The parties MUST verify that the Diffie-Hellman common value is not the "point at infinity", i.e. that the shared secret derived contains non-zero octets.

When compressed encoding is used, computation of the Diffie-Hellman common value, and hence, of the shared secret value from the x-coordinate transmitted in the key exchange payload requires recovery of a correspoding y-coordinate. Since there are up to two possible points on the elliptic curve having a given x-coordinate, the recovered y-component is not unique. However, as explained in [RFC6090], any of the two y-coordinates corresponding to the x-value transmitted in the key exchange payload can be used to compute the Diffie-Hellman common value.

3. Security Considerations

The security considerations of [RFC4306] apply accordingly.

The confidentiality, authenticity and integrity of a secure communication based on IKEv2 is limited by the weakest cryptographic primitive applied. In order to achieve a maximum security level when using one of the elliptic curves from Table 1 for key exchange, the

key derivation function, the algorithms and key lengths of symmetric encryption and message authentication as well as the algorithm, bit length and hash function used for signature generation should be chosen according to the recommendations of [NIST800-57] and [RFC5639]. Furthermore, the private Diffie-Hellman keys should be selected with the same bit length as the order of the group generated by the base point G and with approximately maximum entropy.

Implementations of elliptic curve cryptography for IKEv2 may be susceptible to side-channel attacks. Particular care should be taken for implementations that internally use the corresponding twisted curve to take advantage of an efficient arithmetic for the special parameters (A = -3): although the twisted curve itself offers the same level of security as the corresponding random curve (through mathematical equivalence), an arithmetic based on small curve parameters may be harder to protect against side-channel attacks. General guidance on resistence of elliptic curve cryptography implementations against side-channel-attacks is given in [BSI1] and [HMV].

4. IANA Considerations

Before this document can become an RFC, IANA is required to update the Transform Type 4 (Diffie-Hellman Group Transform) IDs in its Internet Key Exchange Version 2 (IKEv2) Parameters registry [IANA-IKE2]. In particular, numbers are to be assigned to the groups specified in Table 1. Another I-D is being submitted for publication as RFC [BP_IKE] requesting assignment for the same groups in the corresponding registry for IKEv1; in order to keep the registries for IKEv1 and IKEv2 in accordance, it is advisable to assign the same values in both registries.

5. Intellectual Property Rights

Although, the authors have no knowledge about any intellectual property rights which cover the general usage of the ECP groups defined herein, implementations based on these domain parameters may require use of inventions covered by patent rights. In particular, the compressed encoding method for the key exchange payload defined in Section 2.2 and techniques for an efficient arithmetic based on the special parameters of the twisted curves as explained in Section 2.1 may be covered by patents.

6. References

6.1. Normative References

[IANA-IKE2] Internet Assigned Numbers Authority, "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org/assignments/ikev2-parameters>.

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

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5639] Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, March 2010.

6.2. Informative References

[ANSI1] American National Standards Institute, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62, 2005.

[BSI1] Bundesamt fuer Sicherheit in der Informationstechnik, "Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations", July 2011.

[FIPS] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-2, December 1998.

[BP_IKE] Harkins, D., "Brainpool Elliptic Curves for the IKE Group Description Registry", draft-harkins-brainpool-ike-groups-00 (work in progress), August 2012.

[HMV] Hankerson, D., Menezes, A., and S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer Verlag, 2004.

[ISO1] International Organization for Standardization, "Information Technology - Security Techniques - Digital Signatures with Appendix - Part 3: Discrete Logarithm Based Mechanisms", ISO/IEC 14888-3, 2006.

[ISO2] International Organization for Standardization,

"Information Technology - Security Techniques - Cryptographic Techniques Based on Elliptic Curves - Part 2: Digital signatures", ISO/IEC 15946-2, 2002.

[NIST800-57] National Institute of Standards and Technology, "Recommendation for Key Management - Part 1: General (Revised)", NIST Special Publication 800-57, March 2007.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, June 2010.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, February 2011.

[SEC1] Certicom Research, "Elliptic Curve Cryptography", Standards for Efficient Cryptography (SEC) 1, September 2000.

[SEC2] Certicom Research, "Recommended Elliptic Curve Domain Parameters", Standards for Efficient Cryptography (SEC) 2, September 2000.

Appendix A. Test Vectors

This section provides some test vectors for example Diffie-Hellman key exchanges using each of the curves defined in Section 2 . In all of the following sections the following notation is used:

d_A: the secret key of party A

x_qA: the x-coordinate of the public key of party A

y_qA: the y-coordinate of the public key of party A

d_B: the secret key of party B

x_qB: the x-coordinate of the public key of party B

y_qB: the y-coordinate of the public key of party B

x_Z: the x-coordinate of the shared secret that results from completion of the Diffie-Hellman computation

y_Z: the y-coordinate of the shared secret that results from completion of the Diffie-Hellman computation

The field elements x_qA, y_qA, x_qB, y_qB, x_Z, y_Z are represented

as hexadecimal values using the FieldElement-to-OctetString conversion method specified in [SEC1].

A.1. 224 Bit Curve

Curve brainpoolP224r1

dA = 39F155483CEE191FBECFE9C81D8AB1A03CDA6790E7184ACE44BCA161

x_qA = A9C21A569759DA95E038704118426144032 7AFE33141CA04B82DC92E

y_qA = 98A0F75FBBF61D8E58AE5511B2BCDBE8E549B31E37069A2825F590C1

dB = 6060552303899E2140715816C45B57D9B42204FB6A5BF5BEAC10DB00

x_qB = 034A56C550FF88056144E6DD56070F54B0135976B5BF77827313F36B

y_qB = 75165AD99347DC86CAAB1CBB579E198EAF88DC35F927B358AA683681

x_Z = 1A4BFE705445120C8E3E026699054104510D119757B74D5FE2462C66

y_Z = BB6802AC01F8B7E91B1A1ACFB9830A95C079CEC48E52805DFD7D2AFE

A.2. 256 Bit Curve

Curve brainpoolP256r1

dA =
81DB1EE100150FF2EA338D708271BE38300CB54241D79950F77B063039804F1D

x_qA =
44106E913F92BC02A1705D9953A8414DB95E1AAA49E81D9E85F929A8E3100BE5

y_qA =
8AB4846F11CACCB73CE49CBDD120F5A900A69FD32C272223F789EF10EB089BDC

dB =
55E40BC41E37E3E2AD25C3C6654511FFA8474A91A0032087593852D3E7D76BD3

x_qB =
8D2D688C6CF93E1160AD04CC4429117DC2C41825E1E9FCA0ADDD34E6F1B39F7B

y_qB =
990C57520812BE512641E47034832106BC7D3E8DD0E4C7F1136D7006547CEC6A

x_Z =
89AFC39D41D3B327814B80940B042590F96556EC91E6AE7939BCE31F3A18BF2B

y_Z =
49C27868F4ECA2179BFD7D59B1E3BF34C1DBDE61AE12931648F43E59632504DE

A.3. 384 Bit Curve

Curve brainpoolP384r1

dA = 1E20F5E048A5886F1F157C74E91BDE2B98C8B52D58E5003D57053FC4B0BD6
5D6F15EB5D1EE1610DF870795143627D042

x_qA = 68B665DD91C195800650CDD363C625F4E742E8134667B767B1B47679358
8F885AB698C852D4A6E77A252D6380FCAF068

y_qA = 55BC91A39C9EC01DEE36017B7D673A931236D2F1F5C83942D049E3FA206
07493E0D038FF2FD30C2AB67D15C85F7FAA59

dB = 032640BC6003C59260F7250C3DB58CE647F98E1260ACCE4ACDA3DD869F74E
01F8BA5E0324309DB6A9831497ABAC96670

x_qB = 4D44326F269A597A5B58BBA565DA5556ED7FD9A8A9EB76C25F46DB69D19
DC8CE6AD18E404B15738B2086DF37E71D1EB4

y_qB = 62D692136DE56CBE93BF5FA3188EF58BC8A3A0EC6C1E151A21038A42E91
85329B5B275903D192F8D4E1F32FE9CC78C48

x_Z = 0BD9D3A7EA0B3D519D09D8E48D0785FB744A6B355E6304BC51C229FBBCE2
39BBADF6403715C35D4FB2A5444F575D4F42

y_Z = 0DF213417EBE4D8E40A5F76F66C56470C489A3478D146DECF6DF0D94BAE9
E598157290F8756066975F1DB34B2324B7BD

A.4. 512 Bit Curve

Curve brainpoolP512r1

dA = 16302FF0DBBB5A8D733DAB7141C1B45ACBC8715939677F6A56850A38BD87B
D59B09E80279609FF333EB9D4C061231FB26F92EEB04982A5F1D1764CAD5766542
2

x_qA = 0A420517E406AAC0ACDCE90FCD71487718D3B953EFD7FBEC5F7F27E28C6
149999397E91E029E06457DB2D3E640668B392C2A7E737A7F0BF04436D11640FD0
9FD

y_qA = 72E6882E8DB28AAD36237CD25D580DB23783961C8DC52DFA2EC138AD472
A0FCEF3887CF62B623B2A87DE5C588301EA3E5FC269B373B60724F5E82A6AD147F
DE7

dB = 230E18E1BCC88A362FA54E4EA3902009292F7F8033624FD471B5D8ACE49D1
2CFABBC19963DAB8E2F1EBA00BFFB29E4D72D13F2224562F405CB80503666B2542
9

x_qB = 9D45F66DE5D67E2E6DB6E93A59CE0BB48106097FF78A081DE781CDB31FC
E8CCBAAEA8DD4320C4119F1E9CD437A2EAB3731FA9668AB268D871DEDA55A54731
99F

y_qB = 2FDC313095BCDD5FB3A91636F07A959C8E86B5636A1E930E8396049CB48
1961D365CC11453A06C719835475B12CB52FC3C383BCE35E27EF194512B7187628
5FA

x_Z = A7927098655F1F9976FA50A9D566865DC530331846381C87256BAF322624
4B76D36403C024D7BBF0AA0803EAFF405D3D24F11A9B5C0BEF679FE1454B21C4CD
1F

y_Z = 7DB71C3DEF63212841C463E881BDCF055523BD368240E6C3143BD8DEF8B3
B3223B95E0F53082FF5E412F4222537A43DF1C6D25729DDB51620A832BE6A26680
A2

Authors' Addresses

Johannes Merkle
secunet Security Networks

Mergenthaler Allee 77
65760 Eschborn
Germany

Phone: +49 201 5454 3091
EMail: johannes.merkle@secunet.com

Manfred Lochter
Bundesamt fuer Sicherheit in der Informationstechnik (BSI)
Postfach 200363
53133 Bonn
Germany

Phone: +49 228 9582 5643
EMail: manfred.lochter@bsi.bund.de