                    IKE and IKEv2 Authentication Using
              the Elliptic Curve Digital Signature Algorithm (ECDSA)

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

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) and Internet Key Exchange version 2
   (IKEv2) protocols. 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 and IKEv2 without
   introducing any changes to existing IKE operation.

Table of Contents

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 the initial set of exchanges, both parties must
   authenticate each other using a negotiated authentication method. In
   the original version of IKE, this occurs in Phase 1; in IKEv2, it
   occurs in the exchange called IKE-AUTH. 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 and IKE-AUTH: RSA signatures and
   Digital Signature Algorithm (DSA) Digital Signature Standard (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 [LV]; there are also advantages of
   computational speed and efficiency in many settings. Additional
   efficiency may be gained by simultaneously using ECDSA for IKE/IKEv2
   authentication and using elliptic curve groups for the IKE/IKEv2 key
   exchange. Implementers of IPsec and IKE/IKEv2 may therefore find it
   desirable to use ECDSA as the Phase 1/IKE-AUTH authentication method.

2. Requirements Terminology

   The key word "SHALL" in this document is to be interpreted as
   described in [RFC2119].

3. 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 [X9.62-2003]. Other compatible
   specifications include FIPS 186-2 [DSS], IEEE 1363 [IEEE-1363], IEEE
   1363A [IEEE-1363A], and SEC1 [SEC].

   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 and IKEv2 implementations.

4. Specifying ECDSA within IKE and IKEv2

   The original 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.

   The IKEv2 key negotiation protocol begins with two exchanges,
   IKE-SA-INIT and IKE-AUTH. When not using extensible authentication,
   the IKE-AUTH exchange includes a digital signature or Message
   Authentication Code (MAC) on a block of data.

   The IANA-assigned attribute number for authentication using generic
   ECDSA in IKE is 8 (see [IANA-IKE]), but the corresponding list of
   IKEv2 authentication methods does not include ECDSA (see
   [IANA-IKEv2]). Moreover, ECDSA cannot be specified for IKEv2
   independently of an associated hash function since IKEv2 does not
   have a transform type for hash functions. For this reason, it is
   necessary to specify the hash function as part of the signature
   algorithm. Furthermore, the elliptic curve group must be specified
   since the choice of hash function depends on it as well. As a
   result, it is necessary to specify three signature algorithms, named
   ECDSA-256, ECDSA-384, and ECDSA-521. Each of these algorithms
   represents an instantiation of the ECDSA algorithm using a particular
   elliptic curve group and hash function. The three hash functions are
   specified in [SHS]. For reasons of consistency, this document
   defines the signatures for IKE in the same way.

Digital Signature Algorithm	Elliptic Curve Group	Hash Function
ECDSA-256	256-bit random ECP group	SHA-256
ECDSA-384	384-bit random ECP group	SHA-384
ECDSA-521	521-bit random ECP group	SHA-512

   The elliptic curve groups, including their base points, are specified
   in [IKE-ECP].

5. Security Considerations

   Since this document proposes new digital signatures for use within
   IKE and IKEv2, many of the security considerations contained within
   [IKE] and [IKEv2] apply here as well. Implementers should ensure
   that appropriate security measures are in place when they deploy
   ECDSA within IKE or IKEv2.

ECDSA-256, ECDSA-384, and ECDSA-521 are designed to offer security
comparable with the AES-128, AES-192, and AES-256 respectively.

6. IANA Considerations

IANA updated its registry of IPsec authentication methods in
[IANA-IKE] and its registry of IKEv2 authentication methods in
[IANA-IKEv2] to include ECDSA-256, ECDSA-384, and ECDSA-521.

7. ECDSA Data Formats

When ECDSA-256, ECDSA-384, or ECDSA-521 is used as the digital
signature in IKE or IKEv2, the signature payload SHALL contain an
encoding of the computed signature consisting of the concatenation of
a pair of integers r and s. The definitions of r and s are given in
Section 8 of this document.

Digital Signature Algorithm	Bit Lengths of r and s	Bit Length of Signature
ECDSA-256	256	512
ECDSA-384	384	768
ECDSA-521	528	1056

The bit lengths of r and s are enforced, if necessary, by pre-pending
the value with zeros.

8. Test Vectors

The following are examples of the IKEv2 authentication payload for
each of the three signatures specified in this document.

The following notation is used. The Diffie-Hellman group is given by
the elliptic curve $y^2 = (x^3 - 3x + b)$ modulo p. If (x,y) is a
point on the curve (i.e., x and y satisfy the above equation), then
$(x,y)^n$ denotes the scalar multiple of the point (x,y) by the integer
n; it is another point on the curve. In the literature, the scalar
multiple is typically denoted $n(x,y)$; the notation $(x,y)^n$ is used to
conform to the notation used in [IKE], [IKEv2], and [IKE-ECP].

The group order for the curve group is denoted q. The generator is
denoted $g=(gx,gy)$. The hash of the message is denoted h. The
signer's static private key is denoted w; it is an integer between
zero and q. The signer's static public key is $g^w=(gwx,gwy)$. The
ephemeral private key is denoted k; it is an integer between zero and
q. The ephemeral public key is $g^k=(gkx,gky)$. The quantity kinv is
the integer between zero and q such that k*kinv = 1 modulo q. The

first signature component is denoted r; it is equal to gkx reduced
modulo q. The second signature component is denoted s; it is equal
to (h+r*w)*kinv reduced modulo q.

The test vectors below also include the data for verifying the ECDSA
signature. The verifier computes h and the quantity sinv, which is
the integer between zero and q such that s*sinv = 1 modulo q. The
verifier computes

         u = h*sinv modulo q
and
         v = r*sinv modulo q.

The verifier computes (gx,gy)^u = (gux,guy) and (gwx,gwy)^v =
(gwvx,gwvy). The verifier computes the sum

         (sumx,sumy) = (gux,guy) + (gwvx,gwvy)

where + denotes addition of points on the elliptic curve. The
signature is verified if

         sumx modulo q = r.

8.1. ECDSA-256

   IANA assigned the ID value 9 to ECDSA-256.

   The parameters for the group for this signature are

p:
 FFFFFFFF 00000001 00000000 00000000 00000000 FFFFFFFF FFFFFFFF FFFFFFFF

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

q:
 FFFFFFFF 00000000 FFFFFFFF FFFFFFFF BCE6FAAD A7179E84 F3B9CAC2 FC632551

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

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

   The static and ephemeral keys are given by

w:
 DC51D386 6A15BACD E33D96F9 92FCA99D A7E6EF09 34E70975 59C27F16 14C88A7F

gwx:
 2442A5CC 0ECD015F A3CA31DC 8E2BBC70 BF42D60C BCA20085 E0822CB0 4235E970

gwy:
 6FC98BD7 E50211A4 A27102FA 3549DF79 EBCB4BF2 46B80945 CDDFE7D5 09BBFD7D

k:
 9E56F509 196784D9 63D1C0A4 01510EE7 ADA3DCC5 DEE04B15 4BF61AF1 D5A6DECE

gkx:
 CB28E099 9B9C7715 FD0A80D8 E47A7707 9716CBBF 917DD72E 97566EA1 C066957C

gky:
 2B57C023 5FB74897 68D058FF 4911C20F DBE71E36 99D91339 AFBB903E E17255DC

   The SHA-256 hash of the message "abc" (hex 616263) is

h:
 BA7816BF 8F01CFEA 414140DE 5DAE2223 B00361A3 96177A9C B410FF61 F20015AD

   The signature of the message is (r,s) where

kinv:
 AFA27894 5AF74B1E 295008E0 3A8984E2 E1C69D9B BBC74AF1 4E3AC4E4 21ABFA61

r:
 CB28E099 9B9C7715 FD0A80D8 E47A7707 9716CBBF 917DD72E 97566EA1 C066957C

s:
 86FA3BB4 E26CAD5B F90B7F81 899256CE 7594BB1E A0C89212 748BFF3B 3D5B0315

   The quantities required for verification of the signature are

sinv:
 33BDC294 E90CFAD6 2A9F2FD1 F8741DA7 7C02A573 E1B53BA1 7A60BA90 4F491952

u:
 C3875E57 C85038A0 D60370A8 7505200D C8317C8C 534948BE A6559C7C 18E6D4CE

v:
 3B4E49C4 FDBFC006 FF993C81 A50EAE22 1149076D 6EC09DDD 9FB3B787 F85B6483

gux:
  4F749762 9362EFBB EE591206 D036568F 239789B2 34960635 C6607EC6 99062600

guy:
  8490E12D E4DBB68C BF941721 5D8C648E 57A8E0E4 4E176856 3CD58697 001A8D08

gwvx:
  726E5684 964DB8EA 341D8679 DFB70E04 EDA404E9 94BA730F A43F1E78 ED81211B

gwvy:
  0C10CBA8 DD2620C1 12A4F9BE 578E4BE1 E64DC0F7 D1D526CA 167749F9 CEC0DF08

sumx:
  CB28E099 9B9C7715 FD0A80D8 E47A7707 9716CBBF 917DD72E 97566EA1 C066957C

sumy:
  2B57C023 5FB74897 68D058FF 4911C20F DBE71E36 99D91339 AFBB903E E17255DC

   The signature is valid since sumx modulo q equals r.

   If the signature (r,s) were the one appearing in the authentication
   payload, then the payload would be as follows.

  00000048 00090000 CB28E099 9B9C7715 FD0A80D8 E47A7707 9716CBBF 917DD72E
  97566EA1 C066957C 86FA3BB4 E26CAD5B F90B7F81 899256CE 7594BB1E A0C89212
  748BFF3B 3D5B0315

8.2. ECDSA-384

   IANA assigned the ID value 10 to ECDSA-384.

   The parameters for the group for this signature are

p:
 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE
 FFFFFFFF 00000000 00000000 FFFFFFFF

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

q:
 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF C7634D81 F4372DDF
 581A0DB2 48B0A77A ECEC196A CCC52973

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

    The static and ephemeral keys are given by

w:
 0BEB6466 34BA8773 5D77AE48 09A0EBEA 865535DE 4C1E1DCB 692E8470 8E81A5AF
 62E528C3 8B2A81B3 5309668D 73524D9F

gwx:
 96281BF8 DD5E0525 CA049C04 8D345D30 82968D10 FEDF5C5A CA0C64E6 465A97EA
 5CE10C9D FEC21797 41571072 1F437922

gwy:
 447688BA 94708EB6 E2E4D59F 6AB6D7ED FF9301D2 49FE49C3 3096655F 5D502FAD
 3D383B91 C5E7EDAA 2B714CC9 9D5743CA

k:
 B4B74E44 D71A13D5 68003D74 89908D56 4C7761E2 29C58CBF A1895009 6EB7463B
 854D7FA9 92F934D9 27376285 E63414FA

gkx:
 FB017B91 4E291494 32D8BAC2 9A514640 B46F53DD AB2C6994 8084E293 0F1C8F7E
 08E07C9C 63F2D21A 07DCB56A 6AF56EB3

gky:
 2C735822 48686C41 8485E7B7 4E707625 A1832769 F7F56E81 7CF83B1E 4690E782
 65B7AD37 BC2F865F DC290DB6 15CDF17F

    The SHA-384 hash of the message "abc" (hex 616263) is

h:
 CB00753F 45A35E8B B5A03D69 9AC65007 272C32AB 0EDED163 1A8B605A 43FF5BED
 8086072B A1E7CC23 58BAECA1 34C825A7

    The signature of the message is (r,s) where

kinv:
 EB12876B F6191A29 1AA5780A 3887C3BF E7A5C7E3 21CCA674 886B1228 D9BB3D52
 918EF19F E5CE67E9 80BEDC1E 613D39C0

r:
  FB017B91 4E291494 32D8BAC2 9A514640 B46F53DD AB2C6994 8084E293 0F1C8F7E
  08E07C9C 63F2D21A 07DCB56A 6AF56EB3

s:
  B263A130 5E057F98 4D38726A 1B468741 09F417BC A112674C 528262A4 0A629AF1
  CBB9F516 CE0FA7D2 FF630863 A00E8B9F

    The quantities required for verification of the signature are

sinv:
  06EFACEE 8A657F77 584C5A03 9F7E2720 D61DF84C 8FAC6FA4 9A06F6C4 6E8CDA28
  6ADD7D3B 90E1CDA4 79BD899B EE14B99D

u:
  CA5E3714 B4B68BB8 5AF0BC69 E12B16C8 8FAFA26A A6598D7E 2D5C3C40 26F7A944
  7D731721 ABE62CC0 1165ABFD 847088E9

v:
  1342C935 5F1A4563 5435899A C24AEF06 3947CA47 951E89F6 83D73172 F964C359
  69E75EF9 06DA2396 2C747C04 A01137B8

gux:
  94B90657 77A3B5BE 399CEE66 A9DB4E64 8422E370 F19ED1A9 C699769E 01EC9A30
  E544EB10 7D35F7C9 3FA8FB11 8DCB91ED

guy:
  45882DC2 CF367F74 3FC02961 2D5B96FC F9A09E28 1C3C162D 0D189267 83841606
  87E9953A CC634CEF 2D9897B8 BEE32BC2

gwvx:
  6A142FF2 B0B8C552 9B7F78E2 1B014764 440ED8C0 339B2187 13DB9500 3D1A8BA5
  0811C3B8 41B34CA6 E1785BC8 DB9111F4

gwvy:
  98C2A76C 7E6EDB56 6B1DB657 ED3019F8 2FB94FBB F36124DE C23BB7DE 4B181357
  173F1ABF F3980DF1 F7EC4335 B185CEBF

sumx:
  FB017B91 4E291494 32D8BAC2 9A514640 B46F53DD AB2C6994 8084E293 0F1C8F7E
  08E07C9C 63F2D21A 07DCB56A 6AF56EB3

sumy:
  2C735822 48686C41 8485E7B7 4E707625 A1832769 F7F56E81 7CF83B1E 4690E782
  65B7AD37 BC2F865F DC290DB6 15CDF17F

   The signature is valid since sumx modulo q equals r.

   If the signature (r,s) were the one appearing in the authentication
   payload, then the payload would be as follows.

```
 00000068 000A0000 FB017B91 4E291494 32D8BAC2 9A514640 B46F53DD AB2C6994
 8084E293 0F1C8F7E 08E07C9C 63F2D21A 07DCB56A 6AF56EB3 B263A130 5E057F98
 4D38726A 1B468741 09F417BC A112674C 528262A4 0A629AF1 CBB9F516 CE0FA7D2
 FF630863 A00E8B9F
```

8.3. ECDSA-521

   IANA assigned the ID value 11 to ECDSA-521.

   The parameters for the group for this signature are

```
p:
 01FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
 FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
 FFFF

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

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

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
```

   The static and ephemeral keys are given by

```
w:
 0065FDA3 409451DC AB0A0EAD 45495112 A3D813C1 7BFD34BD F8C1209D 7DF58491
 20597779 060A7FF9 D704ADF7 8B570FFA D6F062E9 5C7E0C5D 5481C5B1 53B48B37
 5FA1
```

gwx:
 0151518F 1AF0F563 517EDD54 85190DF9 5A4BF57B 5CBA4CF2 A9A3F647 4725A35F
 7AFE0A6D DEB8BEDB CD6A197E 592D4018 8901CECD 650699C9 B5E456AE A5ADD190
 52A8

gwy:
 006F3B14 2EA1BFFF 7E2837AD 44C9E4FF 6D2D34C7 3184BBAD 90026DD5 E6E85317
 D9DF45CA D7803C6C 20035B2F 3FF63AFF 4E1BA64D 1C077577 DA3F4286 C58F0AEA
 E643

k:
 00C1C2B3 05419F5A 41344D7E 4359933D 734096F5 56197A9B 244342B8 B62F46F9
 373778F9 DE6B6497 B1EF825F F24F42F9 B4A4BD73 82CFC337 8A540B1B 7F0C1B95
 6C2F

gkx:
 0154FD38 36AF92D0 DCA57DD5 341D3053 988534FD E8318FC6 AAAAB68E 2E6F4339
 B19F2F28 1A7E0B22 C269D93C F8794A92 78880ED7 DBB8D936 2CAEACEE 54432055
 2251

gky:
 006D073D 72B272EA 86388D86 8EF64D4C 300A67AC 2981C0F8 E6710AEF A2FCF845
 8117B05E B91BA11C 68BCFC1B C24587E3 A1D0CA2A FE398CDB CFD79CB3 0B36B218
 B437

    The hash of the message "abc" (hex 616263) is

SHA-512(616263):
 DDAF35A1 93617ABA CC417349 AE204131 12E6FA4E 89A97EA2 0A9EEEE6 4B55D39A
 2192992A 274FC1A8 36BA3C23 A3FEEBBD 454D4423 643CE80E 2A9AC94F A54CA49F

    Therefore, the quantity h is

h:
 0000DDAF 35A19361 7ABACC41 7349AE20 413112E6 FA4E89A9 7EA20A9E EEE64B55
 D39A2192 992A274F C1A836BA 3C23A3FE EBBD454D 4423643C E80E2A9A C94FA54C
 A49F

    The signature of the message is (r,s) where

kinv:
 00E90EF3 CE52F8D1 E5A4EEBD 0905F425 2400B0AE 73B49E33 23BCE258 A55F507D
 7C45F3A2 DE3A3EA2 E51D9343 46D71593 A80C8C62 FE229DDF 5D2B64B7 AF4A0837
 0D32

r:
 0154FD38 36AF92D0 DCA57DD5 341D3053 988534FD E8318FC6 AAAAB68E 2E6F4339
 B19F2F28 1A7E0B22 C269D93C F8794A92 78880ED7 DBB8D936 2CAEACEE 54432055
 2251

s:
 017705A7 030290D1 CEB605A9 A1BB03FF 9CDD521E 87A696EC 926C8C10 C8362DF4
 97536710 1F67D1CF 9BCCBF2F 3D239534 FA509E70 AAC851AE 01AAC68D 62F86647
 2660

   The quantities required for verification of the signature are

sinv:
 00DDA6B8 83CB36BF CB21D5B0 B7D1F443 9D3C7797 B23A8D73 58032D5C C917142E
 3F6778BD 977D8460 867853AE 9C74EF5E 417CFA96 F7C937C1 418D9343 738A1BA8
 78E0

u:
 019E5FDB ECC2A88B 72679233 11B27868 427AE2B8 83ED0346 9CBABE65 ACD3F2F8
 D74FA657 8A23C85D 598D1DC6 C1DA074E 0AB83852 BDAAE2F1 857713D3 5BB9BDB7
 32D8

v:
 0069BB0C BA5A6FC8 8A08C0AD AA88F5A5 1EE60477 2D084D98 63DF86FD 958AD9B3
 006E62C4 30CE545E 9C918F04 D852DA13 47CC6A3E FA89BC2C 13B89124 25BA8D60
 BF03

gux:
 00921F3E CEAF579C FDDA6AF9 C1728E5B CA33F77B 57F5984C 624BFF10 F244B577
 144CA24E 20310DEF 2F777892 DA1ED5DE A9A6EF09 85D965AE 98BCF129 855C6C4F
 3311

guy:
 01812CBF E8D08BE9 0CD6AB5D 2ED107A0 123A41A9 C15ACB31 7D65E228 92D89AF8
 C29A4220 83E3495E D14726A0 9868AF1B 399CEF86 6DDDE6B1 0D709696 06525D15
 B4EB

gwvx:
 00AF23A7 7F50CC54 8CEBC506 58FE4A0B A26FF9DE 4E864DE2 7FD059B6 3AE14B5F
 87286BC7 7AAEBA32 4FF675A1 FF7035B6 89AF3835 95F8B5A8 67432FFE 8BF29CF6
 0688

gwvy:
 017A32C4 5A01DF60 3CA96FDF E83493BB 4CB5EE00 C32960A5 4FEB0B39 88841E2F
 9D52B745 C5A7FEC6 777BB899 B65730E9 32D1395D C0574D3C F1093C64 505804D0
 A5B3

sumx:
 0154FD38 36AF92D0 DCA57DD5 341D3053 988534FD E8318FC6 AAAAB68E 2E6F4339
 B19F2F28 1A7E0B22 C269D93C F8794A92 78880ED7 DBB8D936 2CAEACEE 54432055
 2251

sumy:
 006D073D 72B272EA 86388D86 8EF64D4C 300A67AC 2981C0F8 E6710AEF A2FCF845
 8117B05E B91BA11C 68BCFC1B C24587E3 A1D0CA2A FE398CDB CFD79CB3 0B36B218
 B437

   The signature is valid since sumx modulo q equals r.

   If the signature (r,s) were the one appearing in the authentication
   payload, then the payload would be as follows.

 0000008C 000B0000 0154FD38 36AF92D0 DCA57DD5 341D3053 988534FD E8318FC6
 AAAAB68E 2E6F4339 B19F2F28 1A7E0B22 C269D93C F8794A92 78880ED7 DBB8D936
 2CAEACEE 54432055 22510177 05A70302 90D1CEB6 05A9A1BB 03FF9CDD 521E87A6
 96EC926C 8C10C836 2DF49753 67101F67 D1CF9BCC BF2F3D23 9534FA50 9E70AAC8
 51AE01AA C68D62F8 66472660

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.

   [IKE-ECP]   Fu, D. and J. Solinas, "ECP Groups for IKE and IKEv2",
                 RFC 4753, January 2007.

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

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

    [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).

9.2. Informative References

    [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)

    [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)

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

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

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