

Topology:

AS(64496)----AS(65536)----AS(65537)

Prefix Announcements: AS(64496), 192.0.2.0/24, 2001:db8::/32

For this example, the ECDSA algorithm was provided with a static k to make the result deterministic.

The k used for all signature operations was taken from RFC 6979, chapter A.2.5 ?Signatures With SHA-256, message 'sample'?.

k = A6E3C57DD01ABE90086538398355DD4C3B17AA873382B0F24D6129493D8AAD60

Keys of AS64496:

=====

ski: AB4D910F55CAE71A215EF3CAFE3ACC45B5EEC154

private key:

x = D8AA4DFBE2478F86E88A7451BF075565709C575AC1C136D081C540254CA440B9

public key:

Ux = 7391BABB92A0CB3BE10E59B19EBFFB214E04A91E0CBA1B139A7D38D90F77E55A

Uy = A05B8E695678E0FA16904B55D9D4F5C0DFC58895EE50BC4F75D205A25BD36FF5

Router Key Certificate example using OpenSSL 1.0.1e-fips 11 Feb 2013

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 38655612 (0x24dd67c)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=ROUTER-0000FBF0

Validity

Not Before: Jan 1 05:00:00 2017 GMT

Not After : Jul 1 05:00:00 2018 GMT

Subject: CN=ROUTER-0000FBF0

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:73:91:ba:bb:92:a0:cb:3b:e1:0e:59:b1:9e:bf:

fb:21:4e:04:a9:1e:0c:ba:1b:13:9a:7d:38:d9:0f:

77:e5:5a:a0:5b:8e:69:56:78:e0:fa:16:90:4b:55:

d9:d4:f5:c0:df:c5:88:95:ee:50:bc:4f:75:d2:05:

a2:5b:d3:6f:f5

ASN1 OID: prime256v1

X509v3 extensions:

X509v3 Key Usage:

Digital Signature

X509v3 Subject Key Identifier:

AB:4D:91:0F:55:CA:E7:1A:21:5E:F3:CA:FE:3A:CC:45:B5:EE:C1:54

X509v3 Extended Key Usage:

1.3.6.1.5.5.7.3.30

sbgp-autonomousSysNum: critical

Autonomous System Numbers:

64496

Routing Domain Identifiers:

inherit

Signature Algorithm: ecdsa-with-SHA256

30:44:02:20:07:b7:b4:6a:5f:a4:f1:cc:68:36:39:03:a4:83:
ec:7c:80:02:d2:f6:08:9d:46:b2:ec:2a:7b:e6:92:b3:6f:b1:
02:20:00:91:05:4a:a1:f5:b0:18:9d:27:24:e8:b4:22:fd:d1:
1c:f0:3d:b1:38:24:5d:64:29:35:28:8d:ee:0c:38:29

-----BEGIN CERTIFICATE-----

```
MIIBiDCCAS+gAwIBAgIEAk3WfDAKBggqhkJOPQQDAjAaMRgwFgYDVQDDA9ST1VU
RVItMDAwMEZCRjAwHhcNMTcwMTAxMDUwMDAwWhcNMTgwNzAxMDUwMDAwWjAaMRgw
FgYDVQDDA9ST1VURVItdMDAwMEZCRjAwWTATBgcqhkJOPQIBBggqhkJOPQMBBwNC
AARzkbq7kqDL0+EOWbGev/shTgSpHgy6GxOaftjZD3f1WqBbjmLWeOD6FpBLVdnU
9cDfxYiV7lC8T3XSbaJb02/1o2MwYtALBgNVHQ8EBAMCB4AwHQYDVR0OBByEFKtN
kQ9VyucaIV7zyv46zEW17sFUMBGA1UdJQQMMAoGCCsGAQUFBwMeMB4GCCsGAQUF
BwEIAQH/BA8wDaAHMAUCAwD78KECBQAwCgYIKoZIZj0EAWIDRwAwRAIgb7e0a1+k
8cxoNjkDpIPsfiAC0vYInUay7Cp75pKzb7ECIACRBUqh9bAYnSck6LQi/dEc8D2x
OCrdZCk1KI3uDDgp
```

-----END CERTIFICATE-----

Keys of AS(65636):

=====

ski: 47F23BF1AB2F8A9D26864EBBD8DF2711C74406EC

private key:

x = 6CB2E931B112F24554BCDCAAFD9553A9519A9AF33C023B60846A21FC95583172

public key:

Ux = 28FC5FE9AFCF5F4CAB3F5F85CB212FC1E9D0E0DBEAE425BD2F0D3175AA0E989

Uy = EA9B603E38F35FB329DF495641F2BA040F1C3AC6138307F257CBA6B8B588F41F

Router Key Certificate example using OpenSSL 1.0.1e-fips 11 Feb 2013

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 3168189942 (0xbcdb6bdf6)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=ROUTER-0000FFFF

Validity

Not Before: Jan 1 05:00:00 2017 GMT

Not After : Jul 1 05:00:00 2018 GMT

Subject: CN=ROUTER-0000FFFF

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:28:fc:5f:e9:af:cf:5f:4c:ab:3f:5f:85:cb:21:

2f:c1:e9:d0:e0:db:ea:ee:42:5b:d2:f0:d3:17:5a:

a0:e9:89:ea:9b:60:3e:38:f3:5f:b3:29:df:49:56:

41:f2:ba:04:0f:1c:3a:c6:13:83:07:f2:57:cb:a6:

b8:b5:88:f4:1f

ASN1 OID: prime256v1

X509v3 extensions:

X509v3 Key Usage:

Digital Signature

X509v3 Subject Key Identifier:

47:F2:3B:F1:AB:2F:8A:9D:26:86:4E:BB:D8:DF:27:11:C7:44:06:EC

X509v3 Extended Key Usage:

1.3.6.1.5.5.7.3.30

sbgp-autonomousSysNum: critical

Autonomous System Numbers:

65535
Routing Domain Identifiers:
inherit

Signature Algorithm: ecdsa-with-SHA256

30:45:02:21:00:df:04:c5:17:04:d0:f2:b9:fa:f3:d9:6e:3f:
6f:a1:58:d8:fe:6c:18:e4:37:ca:19:7c:c8:75:40:57:6e:7e:
9d:02:20:12:45:e8:a8:58:6b:00:7b:e6:a9:0e:f2:b6:62:50:
4b:1c:01:6f:3b:41:11:69:88:30:73:9f:d7:02:9e:64:4f

-----BEGIN CERTIFICATE-----

```
MIIBijCCATCgAwIBAgIFALzWvfYwCgYIKoZIzj0EAwIwGjEYMBYGA1UEAwPuk9V
VEVSLTAwMDBGRkZGMB4XDTE3MDUwMjE4MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MBYGA1UEAwPuk9VVEVSLTAwMDBGRkZGMB4XDTE3MDUwMjE4MDAwMDAwMDAwMDAw
QgAEKPx6a/PX0yrP1+FyyEwenQ4Nvq7kJb0vDTF1qg6Ynqm2A+OPNfsynfSVZB
8roEDxw6xh0DB/JXy6a4tYj0H6NjMGEwCwYDVR0PBAQDAgeAMB0GA1UdDgQWBBRH
8jvxqy+KnSaGTrvY3ycRx0Q7DATBgNVHSUEDDAKBggrBgEFBQcDHjAeBggrBgEF
BQcBCAEB/wQPMA2gBzAFagMA//+hAgUAMaGCCCqGSM49BAMCA0gAMEUCIQDFBMUX
BNDyufRz2W4/b6FY2P5sGOQ3yh18yHVAV25+nQIEkXoqFhrAHvmaqQ7ytmJQSwB
bztBEWmIMHOf1wKeZ8=
```

-----END CERTIFICATE-----

BGPsec IPv4 Update from AS(65536) to AS(65537):

Binary Form of BGPsec Update (TCP-DUMP):

```
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
01 00 02 00 00 00 E9 40 01 01 02 80 04 04 00 00
00 00 80 0E 0D 00 01 01 04 C6 33 64 64 00 18 C0
00 02 90 21 00 CA 00 0E 01 00 00 01 00 00 01 00
00 00 FB F0 00 BC 01 47 F2 3B F1 AB 2F 8A 9D 26
86 4E BB D8 DF 27 11 C7 44 06 EC 00 46 30 44 02
20 72 14 BC 96 47 16 0B BD 39 FF 2F 80 53 3F 5D
C6 DD D7 0D DF 86 BB 81 56 61 E8 05 D5 D4 E6 F2
7C 02 20 2D DC 00 3C 64 BE 7B 29 C9 EB DB C8 A4
97 ED 66 28 5E E9 22 76 83 E6 C1 78 CE 8D E6 D3
59 5F 41 AB 4D 91 0F 55 CA E7 1A 21 5E F3 CA FE
3A CC 45 B5 EE C1 54 00 47 30 45 02 20 72 14 BC
96 47 16 0B BD 39 FF 2F 80 53 3F 5D C6 DD D7 0D
DF 86 BB 81 56 61 E8 05 D5 D4 E6 F2 7C 02 21 00
C6 17 19 34 07 43 06 3B 8A 5C CD 54 16 39 0B 31
21 1D 3C 52 48 07 95 87 D0 13 13 7B 41 CD 23 E2
```

Signature From AS(64496) to AS(65536):

```
-----
Digest: 21 33 E5 CA A0 26 BE 07 3D 9C 1B 4E FE B9 B9 77
          9F 20 F8 F5 DE 29 FA 98 40 00 9F 60
Signature: 30 45 02 20 72 14 BC 96 47 16 0B BD 39 FF 2F 80
           53 3F 5D C6 DD D7 0D DF 86 BB 81 56 61 E8 05 D5
           D4 E6 F2 7C 02 21 00 C6 17 19 34 07 43 06 3B 8A
           5C CD 54 16 39 0B 31 21 1D 3C 52 48 07 95 87 D0
           13 13 7B 41 CD 23 E2
```

Signature From AS(65536) to AS(65537):

```
-----
Digest: 46 4B 57 CE B1 2D 18 B0 FD 1A 1A 35 94 17 3A 4A
          09 88 E5 F4 ED ED 2F 3D 83 08 5A A8
Signature: 30 44 02 20 72 14 BC 96 47 16 0B BD 39 FF 2F 80
```

```
53 3F 5D C6 DD D7 0D DF 86 BB 81 56 61 E8 05 D5
D4 E6 F2 7C 02 20 2D DC 00 3C 64 BE 7B 29 C9 EB
DB C8 A4 97 ED 66 28 5E E9 22 76 83 E6 C1 78 CE
8D E6 D3 59 5F 41
```

The human readable output is produced using bgpsec-io, a bgpsec traffic generator that uses a wireshark like printout.

Send Update Message

```
++-marker: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
++-length: 256
++-type: 2 (UPDATE)
++-withdrawn_routes_length: 0
++-total_path_attr_length: 233
  +--ORIGIN: INCOMPLETE (4 bytes)
    | +--Flags: 0x40 (Well-Known, Transitive, Complete)
    | +--Type Code: ORIGIN (1)
    | +--Length: 1 byte
    | +--Origin: INCOMPLETE (1)
  +--MULTI_EXIT_DISC (7 bytes)
    | +--Flags: 0x80 (Optional, Complete)
    | +--Type Code: MULTI_EXIT_DISC (4)
    | +--Length: 4 bytes
    | +--data: 00 00 00 00
  +--MP_REACH_NLRI (16 bytes)
    | +--Flags: 0x80 (Optional, Complete)
    | +--Type Code: MP_REACH_NLRI (14)
    | +--Length: 13 bytes
    | +--Address family: IPv4 (1)
    | +--Subsequent address family identifier: Unicast (1)
    | +--Next hop network address: (4 bytes)
    | | +--Next hop: 198.51.100.100
    | +--Subnetwork points of attachment: 0
    | +--Network layer reachability information: (4 bytes)
    |   +--192.0.2.0/24
    |   +--MP Reach NLRI prefix length: 24
    |   +--MP Reach NLRI IPv4 prefix: 192.0.2.0
  +--BGPSEC Path Attribute (206 bytes)
    +--Flags: 0x90 (Optional, Complete, Extended Length)
    +--Type Code: BGPSEC Path Attribute (33)
    +--Length: 202 bytes
    +--Secure Path (14 bytes)
      | +--Length: 14 bytes
      | +--Secure Path Segment: (6 bytes)
      | | +--pCount: 1
      | | +--Flags: 0
      | | +--AS number: 65536 (1.0)
      | +--Secure Path Segment: (6 bytes)
      |   +--pCount: 1
      |   +--Flags: 0
      |   +--AS number: 64496 (0.64496)
    +--Signature Block (188 bytes)
      +--Length: 188 bytes
      +--Algo ID: 1
      +--Signature Segment: (92 bytes)
        | +--SKI: 47F23BF1AB2F8A9D26864EBBD8DF2711C74406EC
        | +--Length: 70 bytes
        | +--Signature: 30 44 02 20 72 14 BC 96 47 16 0B BD 39 FF 2F 80
        |   53 3F 5D C6 DD D7 0D DF 86 BB 81 56 61 E8 05 D5
        |   D4 E6 F2 7C 02 20 2D DC 00 3C 64 BE 7B 29 C9 EB
```

```

|          DB C8 A4 97 ED 66 28 5E   E9 22 76 83 E6 C1 78 CE
|          8D E6 D3 59 5F 41
+--Signature Segment: (93 bytes)
+--SKI: AB4D910F55CAE71A215EF3CAFE3ACC45B5EEC154
+--Length: 71 bytes
+--Signature: 30 45 02 20 72 14 BC 96   47 16 0B BD 39 FF 2F 80
              53 3F 5D C6 DD D7 0D DF   86 BB 81 56 61 E8 05 D5
              D4 E6 F2 7C 02 21 00 C6   17 19 34 07 43 06 3B 8A
              5C CD 54 16 39 0B 31 21   1D 3C 52 48 07 95 87 D0
              13 13 7B 41 CD 23 E2

```

BGPsec IPv6 Update from AS(65536) to AS(65537):

=====

Binary Form of BGPsec Update (TCP-DUMP):

```

FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
01 0C 02 00 00 00 F5 40 01 01 02 80 04 04 00 00
00 00 80 0E 1A 00 02 01 10 20 01 00 10 00 00 00
00 00 00 00 00 C6 33 64 64 00 20 20 01 0D B8 90
21 00 C9 00 0E 01 00 00 01 00 00 01 00 00 00 FB
F0 00 BB 01 47 F2 3B F1 AB 2F 8A 9D 26 86 4E BB
D8 DF 27 11 C7 44 06 EC 00 46 30 44 02 20 72 14
BC 96 47 16 0B BD 39 FF 2F 80 53 3F 5D C6 DD D7
0D DF 86 BB 81 56 61 E8 05 D5 D4 E6 F2 7C 02 20
0A 9A E7 5F 56 CE 42 9C D2 D2 20 38 6B 8D 24 73
E9 5C 8A 50 E5 58 DB 92 B7 88 3D 09 E8 42 4E E7
AB 4D 91 0F 55 CA E7 1A 21 5E F3 CA FE 3A CC 45
B5 EE C1 54 00 46 30 44 02 20 72 14 BC 96 47 16
0B BD 39 FF 2F 80 53 3F 5D C6 DD D7 0D DF 86 BB
81 56 61 E8 05 D5 D4 E6 F2 7C 02 20 6E 26 52 40
CF CA 0E F6 5C 8E A1 AF 6B 65 2A 19 13 D2 FC BD
B5 8E E9 53 60 9F 85 F0 D2 69 99 DF

```

Signature From AS(64496) to AS(65536):

```

-----
Digest:      8A 0C D3 E9 8E 55 10 45   82 1D 80 46 01 D6 55 FC
            52 11 89 DF 4D B0 28 7D   84 AC FC 77
Signature:   30 44 02 20 72 14 BC 96   47 16 0B BD 39 FF 2F 80
            53 3F 5D C6 DD D7 0D DF   86 BB 81 56 61 E8 05 D5
            D4 E6 F2 7C 02 20 6E 26   52 40 CF CA 0E F6 5C 8E
            A1 AF 6B 65 2A 19 13 D2   FC BD B5 8E E9 53 60 9F
            85 F0 D2 69 99 DF

```

Signature From AS(65536) to AS(65537):

```

-----
Digest:      BA BF F7 95 BF 3C BE 81   79 1F A9 90 06 FC 30 1B
            0D BC D5 49 39 5A 0A 71   C2 D5 B2 FA
Signature:   30 44 02 20 72 14 BC 96   47 16 0B BD 39 FF 2F 80
            53 3F 5D C6 DD D7 0D DF   86 BB 81 56 61 E8 05 D5
            D4 E6 F2 7C 02 20 0A 9A   E7 5F 56 CE 42 9C D2 D2
            20 38 6B 8D 24 73 E9 5C   8A 50 E5 58 DB 92 B7 88
            3D 09 E8 42 4E E7

```

The human readable output is produced using bgpsec-io, a bgpsec traffic generator that uses a wireshark like printout.

Send Update Message

```

+--marker: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
+--length: 268
+--type: 2 (UPDATE)
+--withdrawn_routes_length: 0
+--total_path_attr_length: 245
  +--ORIGIN: INCOMPLETE (4 bytes)
    | +--Flags: 0x40 (Well-Known, Transitive, Complete)
    | +--Type Code: ORIGIN (1)
    | +--Length: 1 byte
    | +--Origin: INCOMPLETE (1)
  +--MULTI_EXIT_DISC (7 bytes)
    | +--Flags: 0x80 (Optional, Complete)
    | +--Type Code: MULTI_EXIT_DISC (4)
    | +--Length: 4 bytes
    | +--data: 00 00 00 00
  +--MP_REACH_NLRI (29 bytes)
    | +--Flags: 0x80 (Optional, Complete)
    | +--Type Code: MP_REACH_NLRI (14)
    | +--Length: 26 bytes
    | +--Address family: IPv6 (2)
    | +--Subsequent address family identifier: Unicast (1)
    | +--Next hop network address: (16 bytes)
    | | +--Next hop: 2001:0010:0000:0000:0000:0000:c633:6464
    | +--Subnetwork points of attachment: 0
    | +--Network layer reachability information: (5 bytes)
    |   +--2001:db8::/32
    |   +--MP Reach NLRI prefix length: 32
    |   +--MP Reach NLRI IPv6 prefix: 2001:db8::
  +--BGPSEC Path Attribute (205 bytes)
    +--Flags: 0x90 (Optional, Complete, Extended Length)
    +--Type Code: BGPSEC Path Attribute (33)
    +--Length: 201 bytes
    +--Secure Path (14 bytes)
      | +--Length: 14 bytes
      | +--Secure Path Segment: (6 bytes)
      | | +--pCount: 1
      | | +--Flags: 0
      | | +--AS number: 65536 (1.0)
      | +--Secure Path Segment: (6 bytes)
      |   +--pCount: 1
      |   +--Flags: 0
      |   +--AS number: 64496 (0.64496)
    +--Signature Block (187 bytes)
      +--Length: 187 bytes
      +--Algo ID: 1
      +--Signature Segment: (92 bytes)
        | +--SKI: 47F23BF1AB2F8A9D26864EBBD8DF2711C74406EC
        | +--Length: 70 bytes
        | +--Signature: 30 44 02 20 72 14 BC 96 47 16 0B BD 39 FF 2F 80
        |                   53 3F 5D C6 DD D7 0D DF 86 BB 81 56 61 E8 05 D5
        |                   D4 E6 F2 7C 02 20 0A 9A E7 5F 56 CE 42 9C D2 D2
        |                   20 38 6B 8D 24 73 E9 5C 8A 50 E5 58 DB 92 B7 88
        |                   3D 09 E8 42 4E E7
      +--Signature Segment: (92 bytes)
        +--SKI: AB4D910F55CAE71A215EF3CAFE3ACC45B5EEC154
        +--Length: 70 bytes
        +--Signature: 30 44 02 20 72 14 BC 96 47 16 0B BD 39 FF 2F 80
        |                   53 3F 5D C6 DD D7 0D DF 86 BB 81 56 61 E8 05 D5
        |                   D4 E6 F2 7C 02 20 6E 26 52 40 CF CA 0E F6 5C 8E
        |                   A1 AF 6B 65 2A 19 13 D2 FC BD B5 8E E9 53 60 9F

```

85 F0 D2 69 99 DF