# Certificate Requests to HIP

Jani Pellikka

80th IETF
Mar 27th – Apr 1st 2011
Prague, Czech Republic

# Certificate Requests (1/4)

- Currently there is no way to request certificates through HIP control packets
  - Two use cases for certificate requests:
    1) request the certificate of the peer host
    2) request for issuance (i.e. signing) of a certificate
- Certificate request mechanism to HIP
  - Provides a means to request a preferred certificate through HIP BEX and possibly UPDATE packets
  - Request included in a HIP packet to 1) obtain the certificate of the peer host, and 2) to request for issuance of a certificate for the host itself

# Certificate Requests (2/4)

- Two new HIP parameter types:
  - ***CERT_REQ*** and ***CERT_SIGN_REQ***

- The two parameters are of the TLV form and holds (in addition to length and value) the following fields:
  - ***Cert Group, CA Count, CA ID, CA Type***
  - ***Indication of a Certificate Authority (CA)***

# Certificate Requests (3/4)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Cert group   |   CA count    |     CA ID     |    CA type    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Certification Authority (HIT or SHA-1 hash)          /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                               |            Padding            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

| CA name format | Type number |
|---|---|
| Reserved | 0 |
| HIT | 1 |
| SHA-1 hash | 2 |

***Type***
Unique indentifier for the parameter

***Length***
The size of the parameter in octets excluding Type, Length, and Padding

***Cert Group***
Group ID grouping multiple related CERT and CERT_X_REQ parameters

***CA Count***
Total number of preferred CAs in the certificate request

***CA ID***
Sequence number of a preferred CA

***CA Type***
Defines the format of the indication of a CA (either HIT or SHA-1 hash)

***Certification Authority***
The indication of an accetable CA in a format defined by the ”CA Type” field

***Padding***
To make the TLV a multiple of 8 bytes

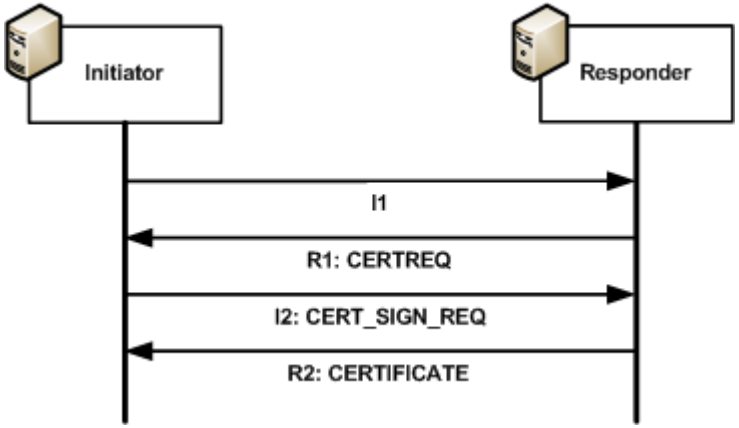
# Certificate Requests (4/4)

- *CERT_REQ* and *CERT_SIGN_REQ* parameters are basically lists of acceptable CAs
- CERT parameter is the placeholder for the actual certificate request mapped by a shared value in the ”Cert Group” field (i.e. the CERT and request field share the same namespace)
- CERT parameter can contain (for example):
  - Self-signed certificate (in case of sign request)
  - Certificate template with desired values and fields (in case of request for the certificate of the peer)

# Appendix A: Self-Signed Certificate

```
Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=Example Host
    Validity
        Not Before: Mar 21 10:47:24 2011 GMT
        Not After : Apr 20 10:47:24 2011 GMT
    Subject: CN=Example Host
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:eb:8e:59:16:90:06:44:e1:22:a3:d1:1f:71:36:
                1d:67:31:70:c7:28:7c:aa:db:6a:72:57:a7:c4:8a:
                97:b1:ad:e4:54:47:a1:09:89:47:a6:45:cd:64:92:
                5d:6c:9b:18:ae:e4:95:71:c6:f6:e8:0b:32:cc:42:
                aa:64:97:4e:ec:6e:29:b8:af:99:bc:98:95:58:37:
                15:05:00:27:36:7c:3c:c4:d6:72:e5:19:5c:30:15:
                24:54:49:e6:68:63:3f:3a:2b:2a:e6:73:75:65:f6:
                1d:ce:82:0e:c1:5d:a2:cf:8b:29:df:af:12:b1:97:
                1d:df:64:06:9f:6d:21:2d:93
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Issuer Alternative Name:
            IP Address: 2001:1015:5c0e:
  5a74:293f:be13:cbfa:f6bd
        X509v3 Subject Alternative Name:
            IP Address: 2001:1015:5c0e:
  5a74:293f:be13:cbfa:f6bd
Signature Algorithm: sha1WithRSAEncryption
    70:9f:78:a2:63:90:d3:1c:e8:c0:b2:03:b0:fa:52:b1:13:a7:
    0c:dd:f7:f4:42:86:06:68:0b:aa:1c:08:a3:bd:70:ad:47:f0:
    9f:a4:31:1b:53:e6:05:5c:cb:41:40:9e:f8:39:cc:6a:ce:c2:
    75:8a:e9:c0:8c:e3:03:b0:98:ed:6e:ac:0e:cb:82:96:fd:e4:
    13:18:b2:ad:bf:f0:aa:2f:6d:ac:71:09:24:ca:bd:da:c9:e1:
    63:fd:66:ad:e4:42:38:d5:68:3d:13:d4:ed:1c:49:e2:38:37:
    36:60:cc:63:43:ae:1d:b7:e2:31:d4:22:af:2e:5b:3f:ed:6a:
    72:ff
```

# Appendix B: Joint Use Case




- Initiator authenticates itself towards Responder, which requires certificate-based authentication
- Intitiator does not happen to have requested certificate; it requests Responder to obtain one for it
- Responder gets the certificate for Initiator, verifies required information on it, and forwards it to Initiator in R2