A Certificate Request Mechanism for HIP?

IETF 79
Nov 7-12 2010, Beijing, China

Jani Pellikka, Andrei Gurtov
CWC, Oulu, Finland

Certificate Request (1/3)

- Currently, there is no way to request certificates via the HIP control packets
- Certificate request mechanism to HIP
  - Provides a means to request a preferred certificate via HIP Base Exchange (BEX) and UPDATE packets
  - A request to be included in a HIP packet to, e.g. obtain the certificate of the Responder or to apply for issuance of a certificate for the Initiator

Certificate Request (2/3)

- New HIP parameter type: *CERTREQ*
- *CERTREQ* parameter is of the TLV form and would hold (in addition to length and value):
  - ***Cert Group, Cert Count, Cert ID, Cert Type***
    - Usage as currently defined in draft-ietf-hip-cert-04
  - ***Certificate Authority (CA)***
    - Public key of acceptable trusted authority
- One CERTREQ parameter per CA
  - Usage similar to the CERT parameter,
    i.e. one CERT parameter per certificate

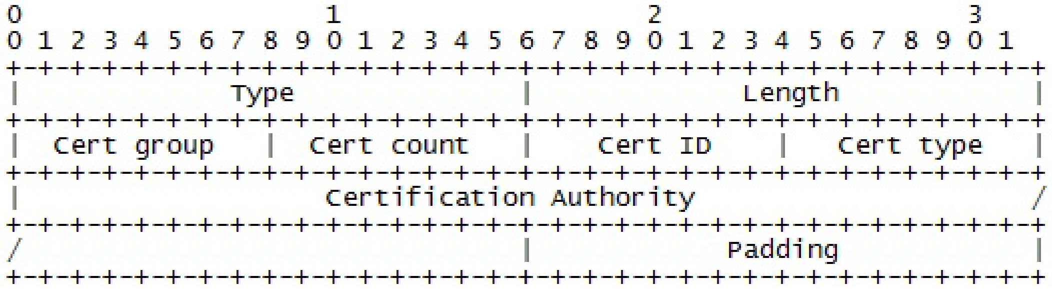
Certificate Request (3/3)

- CERTREQ holds only the public key of a CA
  - CERT parameter is the placeholder for the actual certificate request as specified by the respective certificate format (e.g. X.509 CertRequest)

  →CERT has a dual role: a placeholder for both

  (1) Certificate Requests, and (2) Certificates
- Multiple CERTREQ and CERT parameters are mapped/grouped by using the *Cert Group* and *Cert ID* fields defined in draft-ietf-hip-cert-04

Example of CERTREQ



```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Type             |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Cert group   |  Cert count   |    Cert ID    |   Cert type   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Certification Authority                     /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                               |           Padding             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 CERTREQ parameters

Cert Count
Total number of certificates and certificate requests in the group

Cert ID
The sequence number for this certificate request

Cert Type
Defines the desired format for the certificate being requested

Certification Authority
The public key of the accetable CA expressed in, e.g. a SHA-1 hash form

Padding
To make the TLV a multiple of 8 bytes