Draft-varjonen-hip-cert-01

Samu Varjonen
Helsinkin Institute for Information Technology

72nd IETF - Dublin, Ireland
July 27 - August 1, 2008

Agenda

- Introduction
- CERT Parameter Usage
- CERT Parameter
- CERT Parameter and Grouping
- Certificate Types
- Certificate Objects and HITs
- Hash and URL encodings and Revocation
- Changes from 00 to 01
- Open issues

Introduction

- We have a cryptographic namespace
- We use public-keys as idenfiers
- So why not use those keys to sign certificates
- There are already people using certificates with HIP
- For example:
  Registration extension (RFC5203) can use CERT parameter to carry credentials in I2s and in UPDATEs
- We do NOT specify any certificate semantics
- Instead we ...

CERT Parameter Usage

- We provide unified way to use HITs as identifiers In certificates
- We provide unified way to transport certificates in HIP control messages
- Type number for the parameter is 768 defined in RFC5201
- CERT parameter can be used in
  R1, I2, R2, UPDATE and NOTIFY messages
- CERT parameter is covered by HIP_SIGNATURE
- CERT parameter is non-critical
- Each HIP packet can contain multiple CERT parameters

CERT Parameter

-
  ```
  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   |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                          Certificate                          /
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  /                               |            Padding            |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  ```

- Type, Length, Padding … the usual stuff …

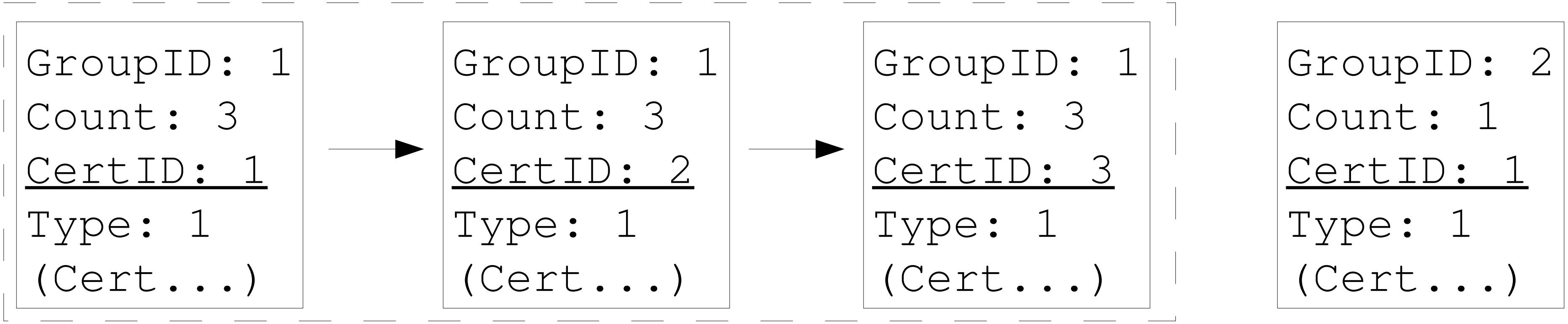
- Type of the certificate and the certificate … as expected …

CERT Parameter and Grouping

- What if I want to present my trust path to You?

- I would need a way to group multiple certificates together

  - Group ID: ID for groups of related CERT parameters
  - Cert count: Total count of certificates that belong to this group
  - Cert ID: The sequence number for the certificate



GroupID: 1
Count: 3
CertID: 1
Type: 1
(Cert...)

GroupID: 1
Count: 3
CertID: 2
Type: 1
(Cert...)

GroupID: 1
Count: 3
CertID: 3
Type: 1
(Cert...)

GroupID: 2
Count: 1
CertID: 1
Type: 1
(Cert...)

- Groups can be divided over multiple sequential packets

- Cert ID must start from one inside a group

Certificate Types

- SPKI
  - RFC2693
  - MUST be implemented (1)

- X.509.v3
  - RFC2459 (2)

- Hash and URL of SPKI
  - RFC4306 (3)

- Hash and URL of X.509.v3
  - RFC4306 (4)

- Others can be defined as needed

Certificate Objects and HITs

- SPKI:

```
(hash hit 2001:13:724d:f3c0:6ff0:33c2:15d8:5f50)
```

- X.509.v3

```
Issuer: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056
Subject: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056

X509v3 extensions:
    X509v3 Issuer Alternative Name:
        IP Address:2001:14:6CF:FAE7:BB79:BF78:7D64:C056
    X509v3 Subject Alternative Name:
        IP Address:2001:14:6CF:FAE7:BB79:BF78:7D64:C056
```

Hash and URL Encodings and revocation

- Hash and URL encodings as in IKEv2

- Using CERT parameter and Hash and URL encodings for certificates in R1 is NOT recommended

  - Middleboxes have to fetch the certificates
  - Middleboxes would need local caches for certificates
  - Middleboxes can be detected after R1 is sent by checking the presence of ECHO_REQUEST_M in control packets
  - If middleboxes on the way add them
  - draft-heer-hip-middle-auth-01

- Certificate revocation is done according to the RFCs defining the certificates (RFC2459 and RFC2693)

Changes from 00 to 01

- Added cert types to use with hash and URL.
- Added how HITs should be represented in X.509.v3 certificates.
- Added full examples of SPKI and X.509.v3 certificates with HIP content
- Added and updated references
- Added NOT recommendation of R1 usage with hash and URL encodings
- Added discussion about CRLs
- Removed the support for I1, because it may lead to DoS and middleboxes cannot be detected before R1

Open Issues

- Grouping can expose the recipient to similar attacks as IP-layer fragmentation. But we can always introduce timeouts instead of waiting forever
- Using HIT as the Common Name (CN) is not necessary if there is something else in the Distinguished Name (DN) part of the X.509.v3
- Size of the certificates can exceed maximum parameter segment size, IPv6 minimum MTU and IPv4 minimum MTU. This may be something to solve in completely separate draft for HIP control packet fragmentation

Thanks

Questions, Ideas, Suggestions?