HIP-CERT & HIP-SERVICE

Samu Varjonen
Helsinki Institute for Information Technology
IETF 76
Hiroshima, Japan
9.11.2009
Agenda

- HIP Certificates
- Changes to it
- HIP Service
- Open questions
HIP CERT parameter

- Unified way to transport certificates in HIP
- Unified way to use HITs as in certificates
- R1, I2, R2, UPDATE and NOTIFY
- Covered by HIP_SIGNATURE
- Non-critical
- Multiple CERTs in one packet
# HIP CERT Param

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

+---------------------------+---------------------------+
| Type                      | Length                    |
+---------------------------+---------------------------+
| Cert group | Cert count | Cert ID | Cert type |
+---------------------------+---------------------------+
| Certificate               | Padding                   |
+---------------------------+---------------------------+
CERT & Grouping

- Group ID
- Cert Count
- Cert ID
- Groups can be divided over multiple sequential packets
- Cert ID in a group must start from 1
Certificate Types

- X.509v3
- SPKI
- Hash and URL encoding
- Distinguished Name
- LDAP URL
HITs as Identifiers

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

- X.509v3:
  

- X509v3 extensions:
  
  X509v3 Issuer Alternative Name:
  X509v3 Subject Alternative Name:
Changes from 01 to 02

- Loosened the requirements on HIT usage
- Added new certificate types
- Restructuring
- Signaling additions
Service Identifiers for HIP

draft-heer-hip-service-00
(Tobias Heer, Samu Varjonen, Hanno Wirtz)
Services

- Services: static, dynamic
- Description: static, dynamic
- Offered services can even depend on requester
- Offered by end-hosts and middleboxes
- Some services require additional credentials (certs, ACL)
REG_INFO

• Quite simple (just a number)
• Always in signed part of the packet
SERVICE_OFFER

- Service properties: classification (understood by everyone)
- Service ID: identifier for a service
- Service description: service-specific details
- 2 flavors – signed and unsigned

0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5  6  7  8  9  0  1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type         |   Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SP (SERVICE_PROPERTIES) (32 bit) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SID (SERVICE_ID) (32 bit)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  SD (SERVICE_DESCRIPTION (variable length) / |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Padding       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
SERVICE_OFFER (cont’d)

- Transmifed in R1, I2, R2, UPDATE
- Signed: for end-hosts
- Unsigned: for end hosts and middleboxes
  - End hosts? -> R1 pre-creation and dynamic services
  - Middleboxes: adding offers to HIP packets
SERVICE_ACK

- Acknowledges a subset of the set of offered services
- Echoes the hashed service offer as service contract
- In signed part of the packet (contract)
Service Properties

- Bit-field with general information about a service
- Classification
Service Properties Field

- 0 REQ - Required
- 1 COM - Commercial
- 2 FOR - Forwarding
- 3 TER - Terminal
- 4 INI - Initial
- 5 ACI - ACL Initiator
- 6 ACR - ACL Responder
- 7 CEI - Cert Initiator
- 8 CER - Cert Responder
Open Questions

• Should signaling be defined specifically for hip-cert?
• Should the hip-cert be just a about the parameter and leave the signaling to other documents?
• Should hip-service be adopted as WG item and handled in bundle with hip-cert?
• Hip-cert to experimental RFC?
• Something to think about before Anaheim?