Host Identity Protocol
Internet-Draft
Intended status: Experimental
Expires: May 23, 2011

Heer
Distributed Systems Group, RWTH
Aachen University
Varjonen
Helsinki Institute for Information
Technology
November 19, 2010

Host Identity Protocol Certificates
draft-ietf-hip-cert-06

Abstract

The CERT parameter is a container for X.509.v3 certificates and Simple Public Key Infrastructure (SPKI) certificates. It is used for carrying these certificates in Host Identity Protocol (HIP) control packets. This document specifies the certificate parameter and the error signaling in case of a failed verification. Additionally, this document specifies the representations of Host Identity Tags in X.509.v3 and SPKI certificates.

The concrete use of certificates including how certificates are obtained, requested, and which actions are taken upon successful or failed verification are specific to the scenario in which the certificates are used. Hence, the definition of these scenario-specific aspects are left to the documents that use the CERT parameter.

http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 23, 2011.

1. Introduction

Digital certificates bind a piece of information to a public key by means of a digital signature, and thus, enable the holder of a private key to generate cryptographically verifiable statements. The Host Identity Protocol (HIP) [RFC5201] defines a new cryptographic namespace based on asymmetric cryptography. The identity of each host is derived from a public key, allowing hosts to digitally sign data and issue certificates with their private key. This document specifies the CERT parameter, which is used to transmit digital certificates in HIP. It fills the placeholder specified in Section 5.2 of [RFC5201].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. CERT Parameter

The CERT parameter is a container for certain types of digital certificates. It MAY either carry SPKI certificates or X.509v3 certificates. It does not specify any certificate semantics.

However, it defines supplementary parameters that help HIP hosts to transmit semantically grouped CERT parameters in a more systematic way. The specific use of the CERT parameter for different use cases is intentionally not discussed in this document because it is specific to a concrete use case. Hence, the use of the CERT parameter will be defined in the documents that use the CERT parameter.

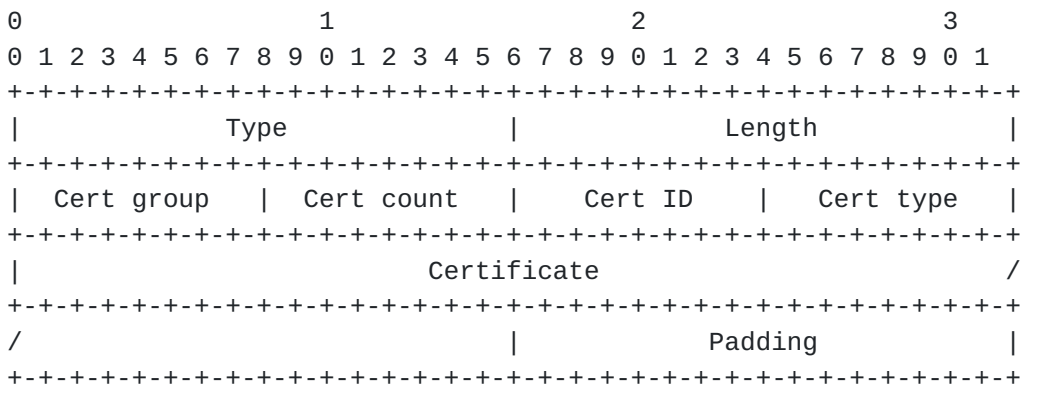
The CERT parameter is covered, when present, by the HIP SIGNATURE field and is a non-critical parameter.

The CERT parameter can be used in all HIP packets. However, using it in the I1 packet is not recommended because it can increase the processing times of I1s, which can be problematic when processing storms of I1s. Each HIP control packet MAY contain multiple CERT parameters. These parameters MAY be related or unrelated. Related certificates are managed in Cert groups. A Cert group specifies a group of related CERT parameters that SHOULD be interpreted in a certain order (e.g., for expressing certificate chains). For grouping CERT parameters, the Cert group and the Cert count field MUST be set. Ungrouped certificates exhibit a unique Cert group field and set the Cert count to 1. CERT parameters with the same Cert group number in the group field indicate a logical grouping. The Cert count field indicates the number of CERT parameters in the group.

CERT parameters that belong to the same Cert group MAY be contained in multiple sequential HIP control packets. This is indicated by a higher Cert count than the amount of CERT parameters with matching Cert group fields in a HIP control packet. The CERT parameters MUST be placed in ascending order, within a HIP control packet, according to their Cert group field. Cert groups MAY only span multiple packets if the Cert group does not fit the packet. A HIP packet MUST NOT contain more than one incomplete Cert group that continues in the next HIP control packet.

The Cert ID acts as a sequence number to identify the certificates in a Cert group. The numbers in the Cert ID field MUST start from 1 up to Cert count.

The Cert Group and Cert ID namespaces are managed locally by each host that sends CERT parameters in HIP control packets.



Type	768
Length	Length in octets, excluding Type, Length, and Padding
Cert group	Group ID grouping multiple related CERT parameters
Cert count	Total count of certificates that are sent, possibly in several consecutive HIP control packets.
Cert ID	The sequence number for this certificate
Cert Type	Indicates the type of the certificate
Padding	Any Padding, if necessary, to make the TLV a multiple of 8 bytes.

The following certificate types are defined:

Cert format	Type number
X.509.v3	1
SPKI	2
Hash and URL of X.509.v3	3
Hash and URL of SPKI	4
LDAP URL of X.509.v3	5
LDAP URL of SPKI	6
Distinguished Name of X.509.v3	7
Distinguished Name of SPKI	8

The next sections outline the use of HITs in X.509.v3 and in SPKI certificates. X.509.v3 certificates are defined in [RFC3280]. The wire format for X.509.v3 is Distinguished Encoding Rules format as defined in [X.690]. The SPKI and its formats are defined in [RFC2693].

Hash and URL encodings (3 and 4) are used as defined in [RFC4306] Section 3.6. Using hash and URL encodings results in smaller HIP control packets, but requires the receiver to resolve the URL or check a local cache against the hash.

LDAP URL encodings (5 and 6) are used as defined in [RFC2255]. Using LDAP URL encoding results in smaller HIP control packets but requires the receiver to retrieve the certificate or check a local cache against the URL.

Distinguished name (DN) encodings (7 and 8) are used as defined in [RFC1779]. Using the DN encoding results in smaller HIP control packets, but requires the receiver to retrieve the certificate or check a local cache against the DN.

3. X.509.v3 Certificate Object and Host Identities

When using X.509.v3 certificates to transmit information related to HIP hosts, HITs MAY be enclosed within the certificates. HITs can represent an issuer, a subject, or both. In X.509.v3 HITs are represented as issuer or subject alternative name extensions as defined in [RFC2459]. If only the HIT of the host is presented as either the issuer or the subject the respective HIT MUST be placed into the respective entity's DN's Common Name (CN) section in a colon delimited presentation format defined in [RFC5952]. Inclusion of CN is not necessary if DN contains any other naming information. It is RECOMMENDED to use the FQDN/NAI from the hosts HOST_ID parameter in the DN if one exists. The full HIs are presented in the public key entries of X.509.v3 certificates.

The following examples illustrate how HITs are presented as issuer and subject in the DN and in the X.509.v3 extension alternative names.

```
Format of DN:
    Issuer: CN=hit-of-issuer
    Subject: CN=hit-of-issuer

Example DN:
    Issuer: CN=2001:14:6cf:fae7:bb79:bf78:7d64:c056
    Subject: CN=2001:1c:5a14:26de:a07c:385b:de35:60e3

Format of X509v3 extensions:
    X509v3 Issuer Alternative Name:
        IP Address:hit-of-issuer
    X509v3 Subject Alternative Name:
        IP Address:hit-of-subject

Example X509v3 extensions:
    X509v3 Issuer Alternative Name:
        IP Address:2001:14:6cf:fae7:bb79:bf78:7d64:c056
    X509v3 Subject Alternative Name:
        IP Address:2001:1C:5a14:26de:a07C:385b:de35:60e3
```

Appendix B shows a full example X.509.v3 certificate with HIP content.

As another example, consider a managed PKI environment in which the peers have certificates that are anchored in (potentially different) managed trust chains. In this scenario, the certificates issued to HIP hosts are signed by intermediate Certificate Authorities (CAs) up to a root CA. In this example, the managed PKI environment is neither HIP aware, nor can it be configured to compute HITs and include them in the certificates.

In this scenario, it is RECOMMENDED that the HIP peers have and use some mechanism of defining trusted root CAs for the purpose of establishing HIP communications. Furthermore it is recommended that the HIP peers have and use some mechanism of checking peer certificate validity for revocation, signature, minimum cryptographic strength, etc., up to the trusted root CA.

When HIP communications are established, the HIP hosts not only need to send their identity certificates (or pointers to their certificates), but also the chain of intermediate CAs (or pointers to the CAs) up to the root CA, or to a CA that is trusted by the remote peer. This chain of certificates MUST be sent in a Cert group as specified in Section 2. The HIP peers validate each other's certificates and compute peer HITs based on the certificate public keys.

4. SPKI Cert Object and Host Identities

When using SPKI certificates to transmit information related to HIP hosts, HITs need to be enclosed within the certificates. HITs can represent an issuer, a subject, or both. In the following we define the representation of those identifiers for SPKI given as S-expressions. Note that the S-expressions are only the human-readable representation of SPKI certificates. Full HIs are presented in the public key sequences of SPKI certificates.

As an example the Host Identity Tag of a host is expressed as follows:

```
Format:  (hash hit hit-of-host)
Example: (hash hit 2001:13:724d:f3c0:6ff0:33c2:15d8:5f50)
```

Appendix A shows a full example SPKI certificate with HIP content.

5. Revocation of Certificates

Revocation of X.509.v3 certificates is handled as defined in Section 5 of [RFC2459]. Revocation of SPKI certificates is handled as defined in Section 5 of [RFC2693].

6. Error signaling

If the Initiator does not send the certificate that the Responder requires the Responder may take actions (e.g. reject the connection). The Responder MAY signal this to the Initiator by sending a HIP NOTIFY message with NOTIFICATION parameter error type CREDENTIALS_NEEDED.

If the verification of a certificate fails, a verifier MAY signal this to the provider of the certificate by sending a HIP NOTIFY message with NOTIFICATION parameter error type INVALID_CERTIFICATE.

NOTIFICATION PARAMETER - ERROR TYPES	Value
CREDENTIALS_REQUIRED	48

The Responder is unwilling to set up an association as the Initiator did not send the needed credentials.

INVALID_CERTIFICATE	50

Sent in response to a failed verification of a certificate. Notification Data MAY contain n groups of 2 octets (n calculated from the NOTIFICATION parameter length), in order Cert group and Cert ID of the certificate parameter that caused the failure.

7. IANA Considerations

This document defines the CERT parameter for the Host Identity Protocol [RFC5201]. This parameter is defined in Section 2 with type 768. The parameter type number is also defined in [RFC5201].

The CERT parameter has 8-bit unsigned integer field for different certificate types, for which IANA is to create and maintain a new sub-registry entitled "HIP certificate types" under the "Host Identity Protocol (HIP) Parameters". Initial values for the Certificate type registry are given in Section 2.

In Section 6 this document defines two new types for "NOTIFY message types" sub-registry under "Host Identity Protocol (HIP) Parameters".

8. Security Considerations

Certificate grouping allows the certificates to be sent in multiple consecutive packets. This might allow similar attacks as IP-layer fragmentation allows, for example sending of fragments in wrong order and skipping some fragments to delay or stall packet processing by the victim in order to use resources (e.g. CPU or memory). Hence, hosts SHOULD implement mechanisms to discard certificate groups with outstanding certificates if state space is scarce.

It is NOT RECOMMENDED to use grouping or hash and URL encodings when HIP aware middleboxes are anticipated to be present on the communication path between peers because fetching remote certificates require the middlebox to buffer the packets and to request remote data. This makes these devices prone to denial of service (DoS) attacks. Moreover, middleboxes and responders that request remote

certificates could be used as deflectors for distributed denial of service attacks.

9. Acknowledgements

The authors would like to thank A. Keranen, D. Mattes, M. Komu and T. Henderson for the fruitful conversations on the subject. D. Mattes most notably contributed the non-HIP aware use case in Section 3.

10. References

10.1. Normative References

[RFC1779] Kille, S., "A String Representation of Distinguished Names", RFC 1779, March 1995.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2255] Howes, T. and M. Smith, "The LDAP URL Format", RFC 2255, December 1997.

[RFC2459] Housley, R., Ford, W., Polk, T., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.

[RFC2693] Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., and T. Ylonen, "SPKI Certificate Theory", RFC 2693, September 1999.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

10.2. Informative References

[X.690] ITU-T, "Recommendation X.690 Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", July 2002, <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>.

Appendix A. SPKI certificate example

This section shows a SPKI certificate with encoded HITs. The example has been indented for readability.

```
(sequence
  (public_key
    (rsa-pkcs1-sha1
      (e #010001#)
      (n |uV7M1dl7OcJCPnlJrX8MvQ8SmE6wne5idnp7VfDMolestu
          JqvB69z3UwlVuSr3VVaQvDSA+15BUweYkis/1+UVnSDdcS
          XUTz6AUTH1tPifoebYPp4s+9XG/vAh7I25pImjW4uL6Jvq
          vI3WBE36wBt3Zmq12hpdA8jSIE1CRZYA8=|
      )
    )
  )
  (cert
    (issuer
      (hash hit 2001:001e:d709:1980:5c6a:bb0c:7650:a027)
    )
    (subject
      (hash hit 2001:001c:5a14:26de:a07c:385b:de35:60e3)
    )
    (not-before "2010-06-22_16:40:47")
    (not-after "2010-07-02_16:40:47")
  )
  (signature
    (hash sha1 |+UzjNn5+bXo3aMZQNGGtapKdlFAA|)
    |Fhioyxi0mpHa2aq2ofhotsauYyDuCa45mMAQ+yTEGOzcc1K+Prx
     +O6kFecKxl+Cwz9qXEI6a/zfAnZqLj18yvszM1D/tH+W3RKl2LW
     +lASsCDKXOi9ObNx+Dwzj3YlHABPxt4gGk0XVadEMXfCPDqiLF+
     zMR9fW5/OaJ+vRwhKs=|
  )
)
```

Appendix B. X.509.v3 certificate example

This section shows a X.509.v3 certificate with encoded HITs.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=2001:1e:d709:1980:5c6a:bb0c:7650:a027
        Validity
            Not Before: Jun 22 13:39:32 2010 GMT
            Not After : Jul  2 13:39:32 2010 GMT
        Subject: CN=2001:1c:5a14:26de:a07c:385b:de35:60e3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b9:5e:cc:d5:d9:7b:39:c2:42:3e:79:49:ad:7f:
                    0c:bd:0f:12:98:4e:b0:9d:ee:62:76:7a:7b:55:f0:
                    cc:a2:57:ac:b6:e2:6a:bc:1e:bd:cf:75:30:95:5b:
                    92:af:75:55:69:0b:c3:48:0f:b5:e4:15:30:79:89:
                    22:b3:fd:7e:51:59:d2:0d:d7:12:5d:44:f3:e8:05:
                    13:1f:5b:4f:89:fa:1e:6d:83:e9:e2:cf:bd:5c:6f:
                    ef:02:1e:c8:db:9a:48:9a:35:b8:b8:be:89:be:ab:
                    c8:dd:60:44:df:ac:01:b7:76:66:ab:5d:a1:a5:d0:
                    3c:8d:22:04:d4:24:59:60:0f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Issuer Alternative Name:
                IP Address:2001:1e:d709:1980:5c6a:bb0C:7650:a027
            X509v3 Subject Alternative Name:
                IP Address:2001:1c:5a14:26de:a07c:385b:de35:60e3
    Signature Algorithm: sha1WithRSAEncryption
        48:a1:25:fb:01:31:d9:80:76:1b:1a:2d:00:f1:26:22:3c:3b:
        20:a0:cb:b2:28:d2:0c:21:d3:9e:3b:4a:ab:3d:f6:ea:ad:46:
        f6:f5:c4:4f:71:ce:3e:7b:65:8d:58:75:2e:99:25:82:5f:73:
        10:c6:c2:f0:4b:35:ff:5c:65:ac:fc:a4:a7:76:50:ab:62:50:
        b8:86:21:e6:83:e1:c1:3d:20:c9:8e:13:ab:d7:4b:d4:ab:2d:
        72:9d:f0:9f:5f:e0:6f:95:fa:a1:95:64:3f:74:63:e5:a8:1d:
        f7:e6:48:98:33:53:7b:91:6d:b0:cb:af:32:15:8c:e0:01:a0:
        a0:b8
```

Appendix C. Change log

Changes from version 00 to 01:

- Revised text on DN usage.
- Revised text on Cert group usage.

Changes from version 01 to 02:

- Revised the type numbers.
- Added a section on signaling.

Changes from version 02 to 03:

- Revised text on CERT usage in control packets.

Changes from version 03 to 04:

- Added the non-HIP aware use case to the Section 3.
- Clarified that the HITs are not always required in the certificates.
- Rewrote the signaling section.
- LDAP URL to LDAP DN in Section 2 last paragraph.
- CERT is always covered by a signature as it's type number requires
- New example certificates
- Style and language clean-ups
- Changed IANA considerations
- Revised the type numbers
- RFC 2119 keywords
- Updated the IANA considerations section
- Rewrote the abstract

Changes from version 04 to 05:

- Clarified the examples in Section 3.
- Clarifications to Section Section 3.
- Modified the explanation of INVALID_CERTIFICATE to allow multiple certs.
- Added reference to the IPv6 colon delimited presentation format.
- Small editorial changes.

Changes from version 05 to 06:

- Editorial changes.
- Unified the example in Section 3.

Authors' Addresses

Tobias Heer
Distributed Systems Group, RWTH Aachen University
Ahornstrasse 55
Aachen
Germany

Phone: +49 241 80 214 36
Email: heer@cs.rwth-aachen.de
URI: http://ds.cs.rwth-aachen.de/members/heer

Samu Varjonen
Helsinki Institute for Information Technology
Gustaf Haellstroemin katu 2b
Helsinki
Finland

Email: samu.varjonen@hiit.fi
URI: http://www.hiit.fi