Host Identity Protocol
Internet-Draft
Intended status: Informational
Expires: August 21, 2008

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

February 18, 2008

HIP Certificates
draft-varjonen-hip-cert-00

Status of this Memo

Copyright Notice

Abstract

This document specifies a certificate parameter called CERT for the Host Identity Protocol (HIP). The CERT parameter is a container for

Simple Public Key Infrastructure (SPKI) and X.509 certificates. It is used for carrying these certificates in HIP control messages. Additionally, this document specifies the representations of Host Identity Tags in SPKI certificates.

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].

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)[I-D.ietf-hip-base] defines a new cryptographic namespace based on asymmetric cryptography. Each host's identity is derived from a public key, allowing hosts to digitally sign data with their private key. This document specifies the CERT parameter that is used to transmit digital signatures in HIP. It corresponds to the placeholder specified in [I-D.ietf-hip-base].

2. CERT Parameter

The CERT parameter is a container for a certain types of digital certificates. It may either carry SPKI certificates or X.509.v3 certificates. It does not specify any certificate semantics. However, it defines organizational parameters that help HIP hosts to transmit semantically grouped parameters.

The CERT parameter may be covered by the HIP SIGNATURE field and is a non-critical parameter.

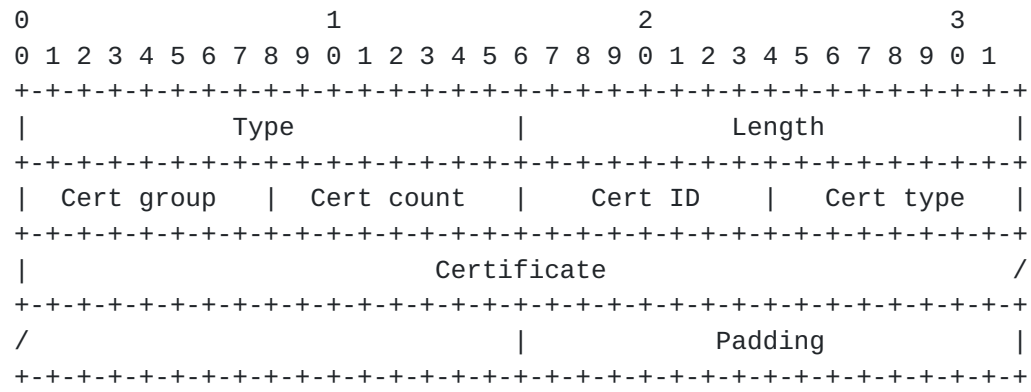
Each HIP packet may contain multiple CERT parameters. If these parameters are related in a way that requires several parameters to be handled in sequence, the Cert group and the Cert count field must be set. Ungrouped certificates exhibit a unique Cert group field and set the Cert count to 1. CERT parameters with the same Cert group number in the group field indicate a logical grouping. The Cert count field indicates the number of grouped CERT parameters.

CERT parameters that belong to the same CERT group may be contained in multiple sequential packets. This is indicated by a higher Cert count than the amount of CERT parameters with matching Cert group

fields in a packet. Within a HIP packet, CERT parameters must be placed in ascending order of their Cert group field. Cert groups may only span multiple packets if the cert group does not fit the packet. Only one Cert group may span two subsequent packets.

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 parameter can be used in I1, R1, I2, R2, and UPDATE messages.



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	Describes 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
SPKI	1
X.509.v3	2

All implementations MUST support SPKI. The next section outlines the use of HITs in SPKI. The wire formats for SPKI are defined in [SEXP].The encoding format for X.509.v3 certificate is defined

elsewhere [RFC3280].

3. SPKI cert object and Host Identities

When using SPKI certificates to transmit information relating to HIP hosts, HITs need to be enclosed within the certificates. In the following we define the representation of those identifiers for SPKI given as S-expressions. Note that S-expressions are only the human-readable representation of SPKI certificates.

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)
```

Below is a simple example of SPKI cert object with HIP content.

```
(cert
   (issuer (hash hit 2001:14:fd64:ca3b:9ef2:8374:ec80:4f20))
   (subject (hash hit 2001:13:724d:f3c0:6ff0:33c2:15d8:5f50))
   (tag <capability-name_1> (arg <arg_1>)
    ...
   (tag <capability-name_n> (arg <arg_n>)
   (propagate)
   (online crl http://www.issuersdomain.net/crl)
   (not before 1/1/2008)
   (not after 12/31/2008)
)
```

The certificate object has HITs encoded into issuer and subject fields. Otherwise it is as defined in [SPKI.structure] and [RFC2693]

4. IANA Considerations

This document defines the CERT parameter for the Host Identity Protocol [I-D.ietf-hip-base]. This parameter is defined in Section 2 with type 768. The parameter type number is also defined in [I-D.ietf-hip-base]. The Cert Group and Cert ID namespaces are managed locally by each peer that sends CERT parameters in HIP packets.

5. Security Considerations

Certificate grouping allows the certificates to be sent in multiple consecutive packets. This might allow similar attacks that fragmentation allows, i.e. sending of fragments in wrong order and skipping some fragments in order to leave the recipient waiting something that never comes. This problem can be alleviated by rate limiting HIP control packets

Using CERT parameter in I1 is not recommended, because it may lead to workload on the responder. This workload may lead to a denial-of-service attack.

6. Acknowledgements

The authors would like to thank M. Komu and T. Henderson of fruitful conversations on the subject.

7. Normative References

[I-D.ietf-hip-base]
Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", draft-ietf-hip-base-10 (work in progress), October 2007.

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

[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.

[SEXP] Rivest, R., "Code and description of S-expressions", <http://theory.lcs.mit.edu/~rivest/sexp.html>.

[SPKI.structure]
Ellison, C., "Simple Public Key Certificate", <draft-ietf-spki-cert-structure-06.txt>.

Authors' Addresses

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

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

Samu Varjonen
Helsinki Institute for Information Technology
Metsnneidonkuja 4
Helsinki
Finland

Fax: +35896949768
Email: samu.varjonen@hiit.fi
URI: http://www.hiit.fi

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).