Internet Engineering Task Force J. Pellikka
Internet-Draft Centre for Wireless
Intended status: Experimental Communications, University of Oulu
Expires: May 16, 2011 November 12, 2010

HIP Certificate Requests
draft-pellikka-hiprg-certreq-00

Abstract

This memorandum describes how the HIP control packets can be used to send requests for preferred certificates to the correspondent hosts. This document specifies a new CERTREQ parameter and describes its use in requesting an issuance of certificates from accepted Certification Authorities (CAs). This document focuses on the means as to how to request for a certificate, and how to signal an error in case of the desired certificate is not available. The syntax of certificates and certificate requests is out of scope of this document.

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].

Status of this Memo

Copyright Notice

1. Introduction

Certificate requests are authorized requests for an authority to issue a certificate, which binds the identity and other relevant information on the requestor to its public key. These requests typically contain the public key of the requestor along with registration information to be associated with the certificate by a trusted Certification Authority (CA).

Host Identity Protocol (HIP) [RFC5201] is a mobility and multihoming protocol, which separates the end-point-identifier and locator roles of IP address. The protocol introduces a new cryptographic namespace based on the public/private key cryptography. As HIP-capable hosts are effectively identified by public keys and they are able to sign information with their private key, their identity along with other host related information can be verified by a trusted 3rd party.

This memorandum describes how HIP control packets can be harnessed to transmit requests for desired type of certificates of an authority accepted by the requestor. The document specifies a new CERTREQ parameter to convey the certificate requests and describes its combined use with the CERT parameter, a placeholder for the certificate and certificate request related data. How to use the CERT parameter to convey digital certificates is specified in [I-D.ietf-hip-cert].

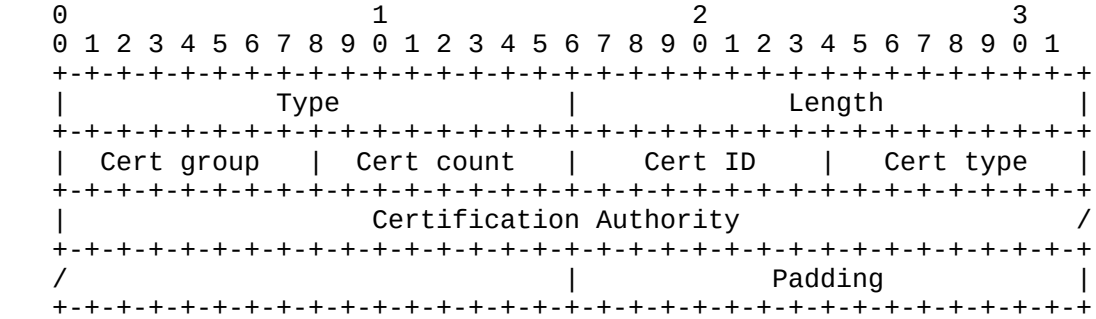
2. CERTREQ Parameter

The CERTREQ parameter provides HIP hosts with a means to request preferred certificates via the HIP control packets. The CERTREQ parameter MAY be included in the HIP Base Exchange (BEX) packets (i.e. I1, R1, I2, R2) or other HIP control packets transmitted after the communicating hosts have successfully authenticated one another. It is, however, NOT RECOMMENDED to include a CERTREQ parameter in the

I1 packet, nor it is NOT RECOMMENDED to process the parameter if present in the I1 packet.

A bit confusingly, the CERTREQ parameter is not to hold the actual certificate request, but instead carries the type of the requested certificate and a list of accepted CAs for it. The request for the desired certificate values is conveyed inside the CERT parameter. The syntax of this request is certificate type specific and thus is not described in this document. The CERTREQ parameter is included in HIP SIGNATURE, when present in the HIP packet.

The CERTREQ parameter is defined below. The fields Cert group, Cert count, Cert ID, and Cert type has been previously defined in [I-D.ietf-hip-cert] and their use conforms to what has been described in that document. The use case described by this document, however, maps the CERT and CERTREQ parameters in the same logical group by sharing the same value in the Cert group field.



Type	770
Length	Size in octets, excluding Type, Length, and Padding
Cert group	Group ID grouping multiple related CERTREQ parameters
Cert count	Total number of CERTREQ parameters in one request
Cert ID	Sequence number for this CERTREQ parameter
Cert type	Indicates the type for the requested certificate
Padding	To make the TLV a multiple of 8 bytes (if needed)

As CERT and CERTREQ parameters are related, the Cert group field provides a means to define the two parameters as belonging to the same request. The value in the Cert ID field uniquely identifies a CERTREQ parameter in the group, while the Cert count indicates the total number of CERTREQ field belonging to the certificate request. In other words, the namespace of Cert IDs are separate between the CERT and CERTREQ parameters. In order to transmit a successful request, at least one CERTREQ and one CERT parameter sharing the same value in their Cert group fields MUST be transmitted. The Cert count field is set to indicate the total count of CERTREQ parameters

belonging to the request. The values of the Cert ID and Cert group fields MUST start from 1 and their namespaces are locally managed by the host transmitting certificate requests in the HIP control packets.

The Certificate Type field has the same values as those defined in [I-D.ietf-hip-cert]. The Certificate Authority field contains an indicator of trusted CAs for the certificate type. The field contains a concatenation of all accepted CAs by order of preference, listing the most preferred CA first. The encoding of each CA indication is a SHA1 hash over the public key indicated in the certificate of the CA in question. The hashes are appended without any delimiters or other formatting. If the certificate type does not explicitly allow a concatenated list as a payload, each accepted CA MAY be included in separate CERTREQ parameters carried by the same or sequential HIP control packets. Also in this case, the CAs are listed by order of preference using the Cert ID field as an identifier.

3. Error Signaling

If the requestee is prevented from delivering the desired kind of certificate to the requestor, it MAY signal this by transmitting a HIP NOTIFY packet with the error type of the NOTIFICATION parameter set to CERTIFICATE_NOT_AVAILABLE. The CERTIFICATE_NOT_AVAILABLE error type can be carried in the NOTIFICATION parameter of other HIP packets as well. The CERTIFICATE_NOT_AVAILABLE error type is defined as follows.

NOTIFICATION PARAMETER - ERROR TYPES	Value
CERTIFICATE_NOT_AVAILABLE	52

Transmitted if the requestee is not able to deliver a certificate of the requested type or a certificate issued by any of the CAs accepted by the requestor. Notification Data contains an octet, i.e. Cert group to identify the request that the requestee was not able not fulfil.

The CERTREQ parameter should not be considered as a mandate for a certain type of certificate, but merely as a suggestion from the requestor. Therefore, if the requestee is unable to deliver the desired kind of certificate, this SHOULD NOT necessarily be considered as error and the operation of the HIP protocol SHOULD proceed as normal. In some cases where, e.g. a HIP host is

configured to require a certificate for a successful authentication and authorization, it MAY, however, be required to terminate the BEX or ongoing HIP session with the correspondent host if desired credentials cannot be obtained.

4. IANA Considerations

This memorandum specifies the CERTREQ parameter for Host Identity Protocol (HIP) [RFC5201]. The parameter is defined in Section 2 of this document and identified by type 770. The assigned type number needs to be confirmed and included to the "Host Identity Protocol (HIP) Parameters" registry by IANA.

The CERTREQ parameter contains a 8-bit unsigned integer field for a certificate type. The certificate types are maintained in a sub-registry referred to as "HIP certificate types" under the "Host Identity Protocol (HIP) Parameters" by IANA. This document conforms with the certificate type values defined by [I-D.ietf-hip-cert] and does not specify any additional values. It is assumed that the values for certificate types are maintained in that particular document.

Finally, in Section 3, this memorandum specifies a new type CERTIFICATE_NOT_AVAILABLE for the "NOTIFY message types" sub-registry under "Host Identity Protocol (HIP) Parameters". Its value is specified as 52.

5. Security Considerations

The CERTREQ parameter SHOULD NOT be attached to the I1 packet of BEX. If the Responder was to receive an I1 packet with a CERTREQ parameter, it SHOULD ignore it and proceed with the BEX as normal. The handling of CERTREQ parameter requires the Responder to utilize CPU and memory, and therefore handling the parameter before the correspondent host is authenticated would allow a Denial of Service (DoS) attack toward the Responder.

6. Acknowledgements

The authors would like to thank A. Gurtov for fruitful conversations on the subject of this document.

7. Normative References

[I-D.ietf-hip-cert]
Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", draft-ietf-hip-cert-05 (work in progress), November 2010.

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

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

Author's Address

Jani Pellikka
Centre for Wireless Communications, University of Oulu
P.O. Box 4500, FI-90014
Oulu,
Finland

Phone: +358 8 553 2965
Email: jani.pellikka@ee.oulu.fi
URI: http://www.cwc.oulu.fi