Host Identity Protocol Certificates

Abstract

The Certificate (CERT) parameter is a container for digital 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 (HITs) in X.509 version 3 (v3).

The concrete use cases of certificates, including how certificates are obtained and 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 is left to the documents that use the CERT parameter.

This document updates RFC 7401 and obsoletes RFC 6253.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8002.
1. Introduction

Digital certificates bind pieces 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) [RFC7401] 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 [RFC7401] and thus updates [RFC7401].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "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 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. Hence, the use of the CERT parameter will be defined in the documents that use the CERT parameter.

The CERT parameter is covered and protected, 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 first Initiator (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, each carrying one certificate. 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). Ungrouped certificates exhibit a unique CERT group field and set the CERT count to 1. CERT parameters with the same group number in the CERT 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.

<table>
<thead>
<tr>
<th>Type</th>
<th>CERT group</th>
<th>CERT count</th>
<th>CERT ID</th>
<th>CERT type</th>
<th>Certificate</th>
<th>Padding (variable length)</th>
</tr>
</thead>
</table>

- **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. Any added padding bytes MUST be zeroed by the sender, and their values SHOULD NOT be checked by the receiver.

The certificates MUST use the algorithms defined in [RFC7401] as the signature and hash algorithms.
The following certificate types are defined:

<table>
<thead>
<tr>
<th>CERT format</th>
<th>Type number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0</td>
</tr>
<tr>
<td>X.509 v3</td>
<td>1</td>
</tr>
<tr>
<td>Obsoleted</td>
<td>2</td>
</tr>
<tr>
<td>Hash and URL of X.509 v3</td>
<td>3</td>
</tr>
<tr>
<td>Obsoleted</td>
<td>4</td>
</tr>
<tr>
<td>LDAP URL of X.509 v3</td>
<td>5</td>
</tr>
<tr>
<td>Obsoleted</td>
<td>6</td>
</tr>
<tr>
<td>Distinguished Name of X.509 v3</td>
<td>7</td>
</tr>
<tr>
<td>Obsoleted</td>
<td>8</td>
</tr>
</tbody>
</table>

The next sections outline the use of HITs in X.509 v3. X.509 v3 certificates and the handling procedures are defined in [RFC5280]. The wire format for X.509 v3 is the Distinguished Encoding Rules format as defined in [X.690].

Hash and Uniform Resource Locator (URL) encoding (3) is used as defined in Section 3.6 of [RFC7296]. Using hash and URL encodings result in smaller HIP control packets than by including the certificate(s) but requires the receiver to resolve the URL or check a local cache against the hash.

Lightweight Directory Access Protocol (LDAP) URL encoding (5) is used as defined in [RFC4516]. 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) encoding (7) is represented by the string representation of the certificate’s subject DN as defined in [RFC4514]. 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

If needed, HITs can represent an issuer, a subject, or both in X.509 v3. HITs are represented as IPv6 addresses as defined in [RFC7343]. When the Host Identifier (HI) is used to sign the certificate, the respective HIT SHOULD be placed into the Issuer Alternative Name (IAN) extension using the GeneralName form iPAddress as defined in [RFC5280]. When the certificate is issued for a HIP host, identified by a HIT and an HI, the respective HIT SHOULD be placed into the...
Subject Alternative Name (SAN) extension using the GeneralName form iPAddress, and the full HI is presented as the subject’s public key info as defined in [RFC5280].

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

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:
  X509v3 Subject Alternative Name:
    IP Address:2001:2c:5a14:26de:a07c:385b:de35:60e3

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

As another example, consider a managed Public Key Infrastructure (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 Certification 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.

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 SHOULD 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. Revocation of Certificates

Revocation of X.509 v3 certificates is handled as defined in Section 5 of [RFC5280] with two exceptions. First, any HIP certificate serial number that appears on the Certificate Revocation List (CRL) is treated as invalid regardless of the reason code. Second, the certificateHold is not supported.
5. Error Signaling

If the Initiator does not send all the certificates 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_REQUIRED.

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.

<table>
<thead>
<tr>
<th>NOTIFICATION PARAMETER - ERROR TYPES</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREDENTIALS_REQUIRED</td>
<td>48</td>
</tr>
<tr>
<td>INVALID_CERTIFICATE</td>
<td>50</td>
</tr>
</tbody>
</table>

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

Sent in response to a failed verification of a certificate. Notification Data MAY contain a CERT group and CERT ID octet (in this order) of the CERT parameter that caused the failure.

6. IANA Considerations

This document defines the CERT parameter for HIP [RFC7401]. The CERT parameter type number (768) is defined in [RFC7401].

The CERT parameter has an 8-bit unsigned integer field for different certificate types, for which IANA has created and maintains a subregistry entitled "HIP Certificate Types" under "Host Identity Protocol (HIP) Parameters". Values for the "HIP Certificate Types" registry are given in Section 2. New values for the Certificate types from the unassigned space are assigned through IETF Review.

In Section 5, this document defines two types for the "NOTIFY Message Types" subregistry under "Host Identity Protocol (HIP) Parameters".

As this document obsoletes [RFC6253], references to [RFC6253] in IANA registries have been replaced by references to this document. This document changes the "HIP Certificate Types" registry in Section 2.
The following updates to the "HIP Certificate Types" registry have been made.

The references have been updated from [RFC6253] to this document.

This document obsoleted the type numbers "2", "4", "6", and "8" for the Simple Public Key Infrastructure (SPKI) certificates.

7. 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, the sending of fragments in the 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.

Although the CERT parameter is allowed in the I1 packet, it is NOT RECOMMENDED because it can increase the processing times of I1s, which can be problematic when processing storms of I1s. Furthermore, the Initiator has to take into consideration that the Responder can drop the CERT parameter in I1 without processing the parameter.

Checking of the URL and LDAP entries might allow denial-of-service (DoS) attacks, where the target host may be subjected to bogus work.

Security considerations for X.509 v3 are discussed in [RFC5280].

8. Differences from RFC 6253

This section summarizes the technical changes made from [RFC6253]. This section is informational and is intended to help implementors of the previous protocol version. If any text in this section contradicts text in other portions of this specification, the text found outside of this section should be considered normative.

The following change has been made.

o Support for SPKI certificates has been removed.
9. References

9.1. Normative References


9.2. Informative References

Appendix A. X.509 v3 Certificate Example

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

Certificate:

Datata:
Version: 3 (0x2)
Serial Number: 12705268244493893545 (0xb0522e729b12cb9)
Signature Algorithm: sha256WithRSAEncryption
Issuer: DC=Example, DC=com, CN=Example issuing host
Validity
Not After : Feb 24 11:28:29 2017 GMT
Subject: DC=Example, DC=com, CN=Example issuing host

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
e2:40:e4:7b:98:33:2f:bf:03:
Exponent: 65537 (0x10001)

X509v3 extensions:
X509v3 Subject Alternative Name:

X509v3 Issuer Alternative Name:
Signature Algorithm: sha256WithRSAEncryption
54:6e:66:cc:ee:7e:c6:bb:56:61:30:cb:be:7f:00:0e:50:0f:8:
1f:ae:07:30:6b:9c:6e:12:93:72:e2:10:c9:8e:2c:00:8b:d6:
f0:05:3c:ff:9f:91:24:69:6d:5b:5a:0c:40:28:01:ff:5b:45:bb:
55:cl:8c:fa

-----BEGIN CERTIFICATE-----
MIIDWTCCAkGgAwIBAgIJALBSLicpGyy5MA0GCSqGSIb3DQEBCwUAMEMoFzAVBgoJ
ka1ajk/IzSAEZFdFegFtcGxlMRMWQYKZClm12PyLGQBRGRYD29tMR0wGwYDVQQD
ExRFcGcGx1IlGlzc3VpmbmcgG9zdDAeFw0xNjAyMjUxMTI4MjlaFw0xNzA2MjQX
MTI4MjlaME0xFzAVBgoJka1ajk/IzSAEZFdFegFtcGxlMRMWQYKZClm12PyLGQ
BRGRYD29tMR0wGwYDVQQDExRFcGtcGxlIlGlzc3VpmbmcgG9zdDCASIIwQY
K0JkOJi
hvcNAQEBQADggEPADCCAQoCggEBAKBBQADgEAMc53cqlsOhxjvdMUvN4xuX28v
Kb21Gfasyuv3iNHEUVEBNWlH2Njiz27O1EIg7pppA1A7+7G35OeP0e5gK9LA
7E826Bckiywfg95/kqvinNAQ9QfFIMqZbRfRc8H21pN5cfteG+E+K0hpvg8gVPi4
av7z7T0kaXB+JuzDmmL2e613hsFHCbMAYPf35pt39Ub0AIVGouraJVxGoqQFWIBT
H8XLEaDa2PKt1pUzUl1zAVWxlLT71ldmlte3LTVuj3RrK1g+lmUQpG8EeCvV
yol445lhcwAJKVM2qqZmNjnpXq1lizG2LTmvbcrCOB/jTLLBMJcCAW000IONMow
GwYDV0RBBQSwocQ1A5AEJ9z8DLJ4hdJ/TmN1tzAbBqMVHRIFEDAShxAgAQ7h
HkWfjlxaiWwkJMA0CGSgSISb3DQEBCwUAA4IBAQ8t5gmmMMrPsP5Ht52UT6kLWN
u0G/0wxmEn4tNS1BNvYyqP7OoEEaAHJRWB5sICN5jYvCyWc2phoPufbfqA+fdppom
xGjziz1lu7U7M8777V8xXY7PL5/AVAUP13xTwa3nTQqoPIFSWxv76kf68K3ggJHDhMd
KjsamdmvEPwIk1/YOBDWuQyGz0u7PRLNXkBACT1ofrgcwa/XmEqNv4hDJJiA19bw
Bcp/kSRpbVt5aDEA0AfJbRbibrp5s6d2D41XXrrWxygagyMDedYL250KH1YeLXmN1a
XCFWPgJ+82+13kB1cpFbAFeYsfdmqNQxNSpkWGeTxjd39hqD4FIRVwYz6
-----END CERTIFICATE-----
Acknowledgments

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.

Authors’ Addresses

Tobias Heer
Albstadt-Sigmaringen University
Poststr. 6
72458 Albstadt
Germany

Email: heer@hs-albsig.de

Samu Varjonen
University of Helsinki
Gustaf Haellstroemin katu 2b
00560 Helsinki
Finland

Email: samu.varjonen@helsinki.fi