Network Working Group
Internet-Draft
Updates: 3971 (if approved)
Intended status: Standards Track
Expires: December 5, 2010

R. Gagliano
Cisco Systems
S. Krishnan
Ericsson
A. Kukec
University of Zagreb

June 3, 2010

Subject Key Identifier (SKI) SEND Name Type fields. draft-ietf-csi-send-name-type-registry-06

Abstract

SEcure Neighbor Discovery (SEND) defines the Name Type field in the ICMPv6 Trust Anchor option. This document specifies new Name Type fields based on certificate Subject Key Identifiers (SKI).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 5, 2010.

Copyright Notice

Table of Contents

1. Requirements notation

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 [RFC2119] .

2. Introduction

SEcure Neighbor Discovery [RFC3971] (SEND) utilizes X.509v3 certificates that include the [RFC3779] extension for IPv6 addresses to certify a router's authority over an IPv6 prefix for the NDP (Neighbor Discovery Protocol). The Trust Anchor (TA) Option in section 6.4.3 of [RFC3971] allows the identification of the Trust Anchor selected by the host. In that same section, two name types were defined: the DER Encoded X.501 Name and a Fully Qualified Domain Name (FQDN).

In any Public Key Infrastructure, the subject name of a certificate is only unique within each CA. Consequently, a new option to identify TAs across CAs is needed.

In [I-D.ietf-csi-send-cert] the certificate profile described in [I-D.ietf-sidr-res-certs] is adopted for SEND. In these documents, the Subject field in the certificates is declared to be meaningless and the subjectAltName field is not allowed. On the other hand, the Subject Key Identifier (SKI) extension for the X.509 certificates is defined as mandatory and non-critical.

This document specifies new Name Type fields in the SEND TA option that allows the use of the SKI X.509 extension to identify TA X.509 certificates. This document also defines experimental and reserved Name Types values.

Finally, this document updates the [RFC3971] by changing the Name Type field in the ICMPv6 Trust Anchor option registration procedures from Standards Action to Standards Action or IESG Approval.

3. Name Type fields in the ICMPv6 TA option defined in this document

The following Name Type fields in the ICMPv6 TA option are defined:

Name Type	Description
0	Reserved
3	SHA-1 Subject Key Identifier (SKI).
4	SHA-224 Subject Key Identifier (SKI).
5	SHA-256 Subject Key Identifier (SKI).
6	SHA-384 Subject Key Identifier (SKI).
7	SHA-512 Subject Key Identifier (SKI).
253-254	Experimental
255	Reserved

Name Type field values 0 and 255 are marked as reserved. This means that they are not available for allocation.

When the Name Type field is set to 3, the Name Type field contains a 160-bit SHA-1 hash of the value of the DER-encoded ASN.1 bit string of the subject public key, as described in Section 3.9.2 of [I-D.ietf-sidr-res-certs]. Implementations MAY support SHA-1 SKI name type.

When the Name Type field is set to 4,5,6 or 7, the hash function will respectively be: SHA-224, SHA-256, SHA-384 or SHA-512. Implementations MAY support SHA-224, SHA-256, SHA-284 and SHA-512 SKI name types.

Name Type fields 253 and 254 are marked as experimental, following [RFC3692].

4. Processing Rules for Routers

As specified in [RFC3971], a TA is identified by the SEND TA option. If the TA option is represented as a SKI, then the SKI MUST be equal to the X.509 SKI extension in the trust anchor's certificate. The router SHOULD include the TA option(s) in the advertisement for which the certification path was found. Also, following [RFC3971] specification, if the router is unable to find a path to the requested anchor, it SHOULD send an advertisement without any certificate. In this case, the router SHOULD include the TA options that were solicited.

5. IANA Considerations

IANA is requested to update the Name Type field in the ICMPv6 Trust Anchor option registry by adding the following values:

Value	Description
0	Reserved (Section 3)
3	SHA-1 Subject Key Identifier (SKI) (Section 3)
4	SHA-224 Subject Key Identifier (SKI) (Section 3)
5	SHA-256 Subject Key Identifier (SKI) (Section 3)
6	SHA-384 Subject Key Identifier (SKI) (Section 3)
7	SHA-512 Subject Key Identifier (SKI) (Section 3)
253-254	Experimental use (Section 3)
255	Reserved (Section 3)

Table 1: New Name Type field values in the ICMPv6 TA option

IANA is also requested to modify the registration procedures for the Name Type field in the ICMPv6 Trust Anchor option registry to Standard Action or IESG Approval [RFC5226].

6. Security Considerations

The hash functions referenced in this document to calculate the SKI have reasonable random properties in order to provide reasonably unique identifiers. Two identical identifiers in the same validation path will cause the router to stop fetching certificates once the first certificate has been fetched. In the case that the upward certificate was configured as TA by a host, the router will send to this host an incomplete list of certificates, causing the SEND validation to fail.

For experimental values of the Name Type field, the guidance given in [RFC3692] about the use of experimental values needs to be followed.

7. Normative References

[I-D.ietf-csi-send-cert]
Gagliano, R., Krishnan, S., and A. Kukec, "Certificate profile and certificate management for SEND", draft-ietf-csi-send-cert-03 (work in progress), March 2010.

[I-D.ietf-sidr-res-certs]
Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-18 (work in progress), May 2010.

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

[RFC3692] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

Roque Gagliano
Cisco Systems
Avenue des Uttins 5
Rolle, 1180
Switzerland

Email: rogaglia@cisco.com

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

Ana Kukec
University of Zagreb
Unska 3
Zagreb
Croatia

Email: ana.kukec@fer.hr