Internet Engineering Task Force (IETF)
Request for Comments: 6495
Updates: 3971
Category: Standards Track
ISSN: 2070-1721

R. Gagliano
Cisco Systems
S. Krishnan
Ericsson
A. Kukec
Enterprise Architects

February 2012

# Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields

## 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 (SKIs).

## 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 5741.

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/rfc6495.

## Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents



## 1. Introduction

SEcure Neighbor Discovery (SEND) [RFC3971] 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 Certification Authority (CA). Consequently, a new option to identify TAs across CAs is needed.

In [RFC6494], the certificate profile described in [RFC6487] 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 [RFC3971] by changing the "Trust Anchor option (Type 15) Name Type field" registration procedures from Standards Action to Standards Action or IESG Approval [RFC5226].

## 2. 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].

## 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 4.8.2 of [RFC6487]. 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-384, and SHA-512 SKI name types.

Name Type fields 253 and 254 are marked as experimental, per guidance in [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 the specification defined in [RFC3971], 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 has updated the "Trust Anchor option (Type 15) Name Type field" registry to include 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 has also modified the registration procedures for the "Trust Anchor option (Type 15) Name Type field" registry to Standards 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 a 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

[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., Ed., 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.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[RFC6494] Gagliano, R., Krishnan, S., and A. Kukec, "Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)", RFC 6494, February 2012.

## 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
Enterprise Architects
46/525 Collins St
Melbourne, VIC 3000
Australia

EMail: ana.kukec@enterprisearchitects.com