Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 14, 2010

R. Gagliano
LACNIC
S. Krishnan
Ericsson
A. Kukec
University of Zagreb

November 10, 2009

SEND Name Type field Registry
draft-rgaglian-csi-send-name-type-registry-01

Abstract

SEcure Neighbor Discovery (SEND) defines the Name Type field in the Trust Anchor option. This document requesto to IANA the creation and management of a registry for this field. This document also specifies a new Name Type field based on a certificate Subject Key Identifier (SKI).

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 14, 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 [RFC3779] extension for IPv6 addresses to certify a router authority over an IPv6 prefix for NDP (Neighbor Discovery Protocol). The Trust Anchor Option in section 6.4.3 of RFC 3971 allows the identification of the Trust Anchor (TA) selected by the host. In that section, two name types were defined, the DER Encoded X.501 Name and a Fully Qualified Domain Name (FQDN). This document requesto to IANA the creation and management of a registry for this field.

In any Public Key Infrastructure, the subject name of a certificate is only unique within each CA. 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 the certificates are 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 a new Name Type field in the SEND TA option that allows to use of the SKI X.509 extension to identify TA X.509 certificates.

3. SEND SKI trust anchor Name Type field.

Name Type

3 SHA-1 Subject Key Identifier (SKI)

The Key Identifier used here is the 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 4.2.1.2 of [RFC5280].

3.1. Processing Rules for Router

As described in RFC 3971, a TA is identified by the SEND TA option. If the TA option is represented as a SHA-1 SKI, then the SKI must be equal to the SKI in the anchor's certificate calculated as described

in [draft-ietf-sidr-res-certs-17]. The router SHOULD include the TA option(s) in the advertisement for which the certification path was found.

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.

4. IANA Considerations

IANA will maintains the registry of Name Type field in the ICMP Trust Anchor option. The registry records Name Type fields for the ICMP Trust Anchor option (15) defined in the RFC 3971.

The following Name Type fields are defined:

1 DER Encoded X.501 Name (RFC 3971).

2 FQDN (RFC 3971)

3 SHA-1 Subject Key Identifier (SKI) (Section 3)

New assignments of Name Type field is through Standards Action.

5. Security Considerations

No security considerations.

6. Normative References

[I-D.ietf-csi-send-cert]
Krishnan, S., Kukec, A., and R. Gagliano, "Certificate profile and certificate management for SEND", draft-ietf-csi-send-cert-00 (work in progress), July 2009.

[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-17 (work in progress), September 2009.

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

[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.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

Authors' Addresses

Roque Gagliano
LACNIC
Rambla Rep Mexico 6125
Montevideo, 11400
Uruguay

Email: roque@lacnic.net

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