Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 9, 2010

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

October 6, 2009

Subject Key Identifier (SKI) name type for SEND TA option
draft-rgaglian-csi-send-ski-ta-nametype-00

Status of this Memo

Copyright Notice

Abstract

SEcure Neighbor Discovery (SEND) Utilizes X.509v3 certificates for performing router authorization. This document specifies a SEND name type to identify trust anchor X.509v3 certificates based on its Subject Key Identifier.

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 Tust Anchor Option in section 6.4.3 of RFC 3971 allows the identification of the trust anchor 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).

In any Public Key Infraestructure, the subject name of a certificate is only unique for each CA. A new option to identify trust anchors accross CAs is needed.

In [draft-ietf-csi-send-cert-01] the certificate profile described in [draft-ietf-sidr-res-certs-17] is selected 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 option for SEND that allows to use of the SKI X.509 extension to identify trust anchor material as described in section X.X of RFC 3971.

3. SEND SKI trust anchor identifier option

Name Type

TBD 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, The anchor is identified by the Trust Anchor option. If the Trust Anchor 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 Trust Anchor 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 certificates. In this case, the router SHOULD include the Trust Anchor options that were solicited.

4. IANA Considerations

This document defines a new Name Type for Neighbor Discovery Protocol Trust Anchor option (15).

5. Security Considerations

TBD.

6. Normative References

[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
UY

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