Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2009

S. Krishnan
Ericsson
A. Kukec
University of Zagreb
K. Ahmed
Microsoft

March 9, 2009

Certificate profile and certificate management for SEND
draft-krishnan-cgaext-send-cert-eku-03

Status of this Memo

Copyright Notice

Abstract

Secure Neighbor Discovery (SEND) Utilizes X.509v3 certificates for performing router authorization. This document specifies a certificate profile for SEND based on Resource Certificates along with extended key usage values required for SEND.

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] Utilizes X.509v3 certificates for performing router authorization. It uses the X.509 extension for IP addresses to verify whether the router is authorized to advertise the mentioned IP addresses.

The SEND specification does not describe the set of extensions that need to be supported and the revocation mechanisms for SEND certificates. This document uses the Resource Certificates specified in [RES-CERTS] in order to provide this information.

Also, since the IP addresses extension does not mention what functions the subject of the certificate can perform for the IP addresses, it becomes impossible to know the reason for which the certificate was issued. In order to facilitate issuance of certificates for specific functions, this document utilizes the ExtKeyUsageSyntax field of the X.509 certificate to mention the purpose for which the certificate was issued. This document specifies three extended key usage values, one for routers, one for proxies, and one for address owners, for use with SEND.

3. Certificate Management in SEND

A certification path in SEND is transported in Certification Path Advertisement (CPA) message sent from a router to SEND host. CPA message is sent in reply to the Certification Path Solicitation message (CPS) message. The certification path sent in CPA message is a path between a router and SEND host's trust anchor and it might be potentially voluminous. Thus, CPA and CPS messages are kept separate from the rest of SEND messages.

SEND specification does not define any certificate management routines (certificate issuance and revocation). The only two routines described in SEND specification are the Certificate path validation and IP address extension verification.

3.1. Motivations for using RPKI

This draft recommends that the SEND PKI be made part of the bigger RPKI [SIDR-ARCH]. The main advantages of this model are:

- It is a global model suitable for mobile users. The RPKI has default trust anchors that are widely used and available for mobile users.

- The RPKI project (certificate management and certificate profile) has been adopted by all the RIRs and IANA. SEND could simply adopt well-known and already accepted RPKI mechanisms.

4. Certificate profile

End entity certificates issued in support of SeND MUST comply with the RPKI resource profile [RES-CERTS]. CA certificates used to verify these router (EE) certificates also MUST comply with this profile. This implies that these CA certificates MUST contain at an RFC 3779 address extension representing the address space allocations held by the service provider represented by the CA.

Relying parties (e.g., user devices that implement SeND and process these router certificates) MUST be configured with one or more trust anchors, to enable validation of the router certificates. These trust anchors MAY be the default trust anchors defined for the RPKI, or they MAY be self-signed (CA) certificates associated with the service providers operating the routers in question. In either case, it is RECOMMENDED that the RPKI trust anchor representation defined in [RES-CERTS] be employed.

Because of the flexibility afforded service through (local) trust anchor configuration, certificates used for SeND support can be issued prior to issuance of RPKI certificates under the global address allocation hierarchy. Note, however, that a CA certificate issued independently of the global RPKI will have to be reissued in order to integrate a local PKI with the global RPKI.

In addition to conforming to the Resource Certificate Profile as specified in [RES-CERTS] the SEND certificate MUST support the Extended Key Usage extension. The Extended Key Usage extension is described in section 5.1. It MUST be marked as critical.

4.1. Extended Key Usage Values

The Internet PKI document [RFC5280] specifies the extended key usage X.509 certificate extension. The extension indicates one or more purposes for which the certified public key may be used. The extended key usage extension can be used in conjunction with key usage extension, which indicates the intended purpose of the certified public key.

The extended key usage extension syntax is repeated here for convenience:

```
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER
```

This specification defines three KeyPurposeId values: one for authorizing routers, one for authorizing proxies, and one for address owners.

The inclusion of the router authorization value indicates that the certificate has been issued for allowing the router to advertise prefix(es) that are mentioned using the X.509 extensions for IP addresses and AS identifiers [RFC3779]

The inclusion of the proxy authorization value indicates that the certificate has been issued for allowing the proxy to perform proxying of neighbor discovery messages for the prefix(es) that are mentioned using the X.509 extensions for IP addresses and AS identifiers [RFC3779]

The inclusion of the owner authorization value indicates that the certificate has been issued for allowing the node to use the address(es) or prefix(es) that are mentioned using the X.509 extensions for IP addresses and AS identifiers [RFC3779]

Inclusion of multiple values indicates that the certified public key is appropriate for use by a node performing more than one of these functions.

```
send-kp OBJECT IDENTIFIER ::=
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) TBA1 }

id-kp-sendRouter OBJECT IDENTIFIER ::= { send-kp 1 }

id-kp-sendProxy OBJECT IDENTIFIER ::= { send-kp 2 }

id-kp-sendOwner OBJECT IDENTIFIER ::= { send-kp 3 }
```

The extended key usage extension MAY, at the option of the certificate issuer, be either critical or non-critical.

Certificate-using applications MAY require the extended key usage extension to be present in a certificate, and they MAY require a particular KeyPurposeId value to be present (such as id-kp-sendRouter or id-kp-sendProxy) within the extended key usage extension. If multiple KeyPurposeId values are included, the certificate-using application need not recognize all of them, as long as the required KeyPurposeId value is present.

5. Backward Compatibility

The disadvantages of this model are related to the fact that the SEND specification was developed before the standardization of the RPKI. Hence, SEND is not completely compliant with the RPKI specifications since it defines its own IP prefix validation routine and it is not suitable for the use with CRLs, while the RPKI suports only CRLs. This means that SEND implementations supporting this profile will not be able to interoperate with legacy SEND implementations.

6. Security Considerations

The certification authority needs to ensure that the correct values for the extended key usage are inserted in each certificate that is issued. Relying parties may accept or reject a particular certificate for an intended use based on the information provided in these extensions. Incorrect representation of the information in the extended key usage field can cause the relying party to reject an otherwise appropriate certificate or accept a certificate that ought to be rejected.

7. Acknowledgements

The authors would like to thank Steve Kent, Richard Barnes, Sandy Murphy, Marcelo Bagnulo, and Gabriel Montenegro for reviewing earlier versions of this document and suggesting text to make the document better.

8. Normative References

[RES-CERTS] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-16 (work in progress), February 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.

[SIDR-ARCH] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-04 (work in progress), November 2008.

Authors' Addresses

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

Khaja Ahmed
Microsoft

Email: khaja@windows.microsoft.com