Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 3, 2010

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

July 2, 2009

Certificate profile and certificate management for SEND draft-ietf-csi-send-cert-00

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.

Since the IP addresses extension does not mention what functions the node 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, it is necessary to utilize 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.

The SEND specification also does not describe a revocation mechanism for SEND certificates. This document describes different possible solutions for the certificate management, as well as certificate profile for certificates that a SEND capable node needs to support in addition to what has been defined in [RFC5280].

3. Terminology

End entity certificates issued in support of SeND MUST comply with the RPKI resource profile [res-certificate-profile]. 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-certificate-profile] 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.

4. Terminology

SEND certificates	Certificates described in [RFC3971] and extended in this document. They belong either to SEND routers or Secure Proxy ND nodes: * Router Authorization Certificate and parent certificates in the Authorization Delegation chain. There is no difference in the profile of the Router Authorization Certificate and other (parent) certificates in the Authorization Delegation process. * Secure Proxy ND certificates for ND Proxy, Mobile IPv6 Home Agent or Proxy Mobile Access Gateway [draft-ietf-csi-proxy-send-00].
SIDR RPKI certificates	Certificates defined in [draft-ietf-sidr-res-certs-16].
RPKI	SIDR PKI hierarchy established in accordance with [draft-ietf-sidr-arch-00] whose Trust Anchors are entities which provide administrative control of the IP address space (IANA, RIRs).
SEND PKI	PKI hierarchy used by SEND.
SEND RPKI	SEND PKI established as part of the bigger SIDR RPKI.

5. Certificate Management

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 (certific ate issuance and revocation). The only two routines described in SEND specification are the Certificate path validation and IP address extension verification.

This document explains two possible solutions for the SEND Public Key Infrastructure (SEND PKI). The certificate management and certificate profile will depend on the type of SEND PKI:

- Per-ISP (ISP-centric) PKI model (with CRL based revocation),
- SEND PKI being a part of the bigger RPKI (with OCSP based revocation).

5.1. Per-ISP SEND model

The Per-ISP PKI model is a model with isolated ISP-centric PKI islands. It does not have any prerequisites on certificate revocation or certificate profile, contrary to RPKI model which uses only CRLs (not even delta CRLs) and has defined certificate profile [draft-ietf-sidr-res-certs-11]. Per-ISP PKI model could use in-band revocation and OCSP. Two main advantages of OCSP over CRL in the SEND context are:

- The size of the CRL is potentially large and unbounded, and would be too big to carry in a CPA message.
- The relying party (SEND host) at the instant of receiving of CPA message does not have an access to Internet. The SEND router receives an OCSP response from OCSP responder and forwards it to the SEND non-router node. With CRLs, the relying part would have to accept certificates from the CPA message, consider them as provisional and perform revocation out-of-band later when it gains the Internet access.

The disadvantage of this model is that it represents a local PKI where the mobile users would be ill-served, not knowing the the Trust Anchors in the visited local PKI.

5.1.1. Support for OCSP in SEND

This section suggests the solution for the support of OCSP in SEND. It defines new options in the Certification Path Solicitation message, as well as in the Certification Path Advertisement message.

The Certification Path Solicitation message would then have the following options.

- Trust Anchor: Trust Anchors, as defined in Section 6.4.3 of [RFC3971], which the client is willing to accept

- OCSP Responder: The hash of a trusted OCSP responder's public key or a concatenated list of hashes of more OCSP Responders' public keys.

The client (non-router SEND node) sends multiple OCSP responder hashes in one CPS message, rather than one OCSP Responder per CPS message. Matching of certificate waiting for validation with the corresponding OCSP response can be achieved by matching the target certificate identifier from the OCSP response to the corresponding certificate.

The modified Certification Path Advertisement message contains the following new, optional fields:

- Certificate

- Trust Anchor: to help the client to find out which advertisement is useful

- OCSP response: One or more OCSP response messages, each containing the response for a certificate from the request, as specified in Section 2.2 of [RFC2560].

- OCSP responder: the hash of the trusted OCSP responder's public key that is used to help the client to find the advertisement which corresponds to the defined OCSP responder's public key.

The problem for the client is that when it is in the process of forming a CPS message, it does not have certificates for which it is sending the OCSP request. Thus, it can not form the OCSP request as described in [RFC2560]. However, the client can work around this problem using the hashes of OCSP responders. This problem is also described in Section 5.1 of [RFC4806].

5.2. RPKI SEND model

This solution suggests for the SEND PKI to be the part of the bigger RPKI [draft-ietf-sidr-arch-03]. The main advantages of this model are:

- It is a global model suitable for mobile users. The RPKI has a 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 5 RIRs and IANA. SEND could simply adopt well-known and already accepted RPKI mechanisms.

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:

- It defines its own IP prefix validation routine and it is not suitable for the use with CRLs, while the RPKI suports only CRLs.

- It requires different certificate profile, with the certificate extensions described in the Section 6.

The solution would be to amend RPKI certificate profile to develop a separate profile for SEND RPKI certificates, support for OCSP and inclusion of SEND specific extensions (e.g. EKU extension) on the lower (local) tiers of the RPKI. On the RIR and NIR tier of the RPKI, CRL is not expected to grow to large sizes, but on the lower tiers (SEND level), the link topology is expected to be more dynamic and the CRL might grow to larger sizes. Thus, the use of OCSP is more suitable than the use of the CRLs.

6. Certificate profile

The SEND certificate profile is similar to the RPKI certificate profile, but differs in the certificate extensions. In case of the per-ISP SEND PKI model, the certificate profile described in this section could be fully adopted. In case of the SEND RPKI model, the described certificate extensions are not compliant with the current SIDR documents [draft-ietf-sidr-res-certs-11]. In case of the SEND RPKI model, such certificate profile requires the RPKI certificate profile to be amended, to support OCSP and SEND RPKI certificates on the lower tiers of the RPKI hierarchy.

The subjectAltName extension MAY appear in the SEND RPKI certificates, and the Extended Key Usage MUST appear in the SEND RPKI certificates, while they do not appear in the SIDR RPKI certificates. CRL Distribution Points, Subject Information Access, Subject Key Identifier and Authority Key Identifier, and the extension for AS Resources which appear in SIDR RPKI certificates, MUST NOT appear in SEND RPKI certificates.

The Trust Anchor option in CPS and CPA messages can be specified as DER encoded X.501 Name or FQDN. The values of the Trust Anchor option field is tied to the values of certificate fields. In the first case (X.501 Name), the Trust Anchor option MUST be equal to the Subject field from the certificate. The Subject field MUST be used in accordance with both Resource Certificate Profile [draft-ietf-sidr-res-certs-11] and SEND specification [RFC3971]. In the case of FQDN, Trust Anchor option MUST be equal to the subjectAltName of type FQDN in the certificate. If Subject Name is empty, subjectAltName extension MUST be marked as critical [RFC5280].

The Key Usage extension defines the basic purposes for which the key pair may be used. The Router Authorization Certificate MUST have the digitalSignature bit set, since its key pair is used for the CGA generation and Router Advertisement signing. Other certificates in the Authorization Delegation chain MUST have the keyCertSign bit set. Certificates MUST NOT have a CRLSign bit set. This extension MUST be marked as critical and MUST be processed independently of the Extended Key Usage extension. The certificate purpose must be consistent with both the Extended Key Usage extension and the Key Usage extension.

The Extended Key Usage extension is described in the section 5.1. It MUST be marked as critical.

Certificate policy extension MAY be used in the SEND RPKI certificates, as well as the Name Constraints and Policy Constraints, in order to provide possibility for the future TA management

[draft-ietf-pkix-ta-mgmt-reqs-00], but they MUST NOT be marked as critical.

The Authority Information Access extension specifies how to retrieve additional CA information, e.g. the information about the OCSP responder. It MUST be marked as non-critical, since the host can learn the OCSP responder from its configuration file.

The extension for IP addresses MUST be used as described in [[draft-ietf-sidr-res-certs-11]], but applications have to take into account that IP addresses in the IP address extension might have a larger scope than the IP addresses in SIDR-defined RPKI certificates (e.g. null prefix).

All other extensions MUST be used in accordance with Resource Certificate Profile [draft-ietf-sidr-res-certs-11].

6.1. 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.

7. 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.

8. Normative References

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

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[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.

[RFC4806] Myers, M. and H. Tschofenig, "Online Certificate Status Protocol (OCSP) Extensions to IKEv2", RFC 4806, February 2007.

[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

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

Roque Gagliano
LACNIC

Email: roque@lacnic.net