Network Working Group
Internet-Draft
Updates: 3971 (if approved)
Intended status: Standards Track
Expires: December 30, 2010

R. Gagliano
Cisco Systems
S. Krishnan
Ericsson
A. Kukec
University of Zagreb

June 28, 2010

Certificate profile and certificate management for SEND draft-ietf-csi-send-cert-05

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.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 30, 2010.

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 the [RFC3779] extension for IPv6 addresses to certify a router's authorization to advertise IPv6 prefix for the Neighbor Discovery (ND) Protocol. The SEND specification defines a basic certificate profile for SEND. The certificate profile defined in this document supercedes the profile for router certificates specified in [RFC3971]. That is, certificates used in SEND (by routers, proxies, or address owners) MUST conform to this certificate profile and MAY conform to the original profile in [RFC3971].

The Resource Public Key Infrastructure (RPKI) is the global PKI that attests to allocation of IP address space. The RPKI represents the centralized model referred in Section 6.2 of [RFC3971]. Consequently, SEND will use the RPKI certificate profile and certificate validation detailed in [I-D.ietf-sidr-res-certs]. A consequence of the use of RPKI certificate profile, the certificate validation method described in RFC3971 is updated with the certificate validation method in [I-D.ietf-sidr-res-certs].

Since the RFC 3779 IPv6 addresses extension does not mention what functions the node can perform for the certified IPv6 space, 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 (optional in RPKI Certificates) of the X.509 certificate to mention the purpose why 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.

In RFC 3971 two deployment models were described: centralized and decentralized. This document describes the different deployment models that can be used with the SEND certificates defined here.

3. Terminology

Certified IPv6 address space	IPv6 address space included in an X.509v3 certificate using RFC 3779 extension for IPv6 addresses.
End Entity (EE)	An entity in the PKI that is not a CA.
ETA	External Trust Anchor as defined in [I-D.ietf-sidr-ta].
ISP	Internet Service Provider.
NIR	National Internet Registry.
RIR	Regional Internet Registry.
RPKI	Resource PKI established in accordance with [I-D.ietf-sidr-arch].
RPKI certificates	Certificates defined in [I-D.ietf-sidr-res-certs].
RTA	RPKI Trust Anchor as defined in [I-D.ietf-sidr-ta].
SEND certificates	Certificates described in [RFC3971] and extended in this document. They are end-entity certificates that belong either to SEND routers or Secure Proxy ND nodes: * Router Authorization Certificates. * Secure Proxy ND certificates for ND Proxy, Mobile IPv6 Home Agent or Proxy Mobile Access Gateway [I-D.ietf-csi-proxy-send].

4. SEND Certificate profile

SEND certificates MUST comply with the RPKI resource profile [I-D.ietf-sidr-res-certs]. A Router Authorization Certificate example is included in the Appendix A.

In sections 2, 4.9.10 and 4.9.11 [I-D.ietf-sidr-res-certs] it is stated that RFC 3779 resource extensions MUST be critical and MUST be present in all Resource Certificates. SEND certificates MUST include the IP Resources extension [RFC3779]. This extension MUST include at least one address block for the IPv6 Address Family (AFI=0002), as described in Section 4.9.10 of [I-D.ietf-sidr-res-certs]. SEND certificates MUST NOT have more than one IP Resources extension.

4.1. Unconstrained Certified subnet prefixes

Section 7.3 of [RFC3971] defines the Unconstrained Certified subnet prefixes category by using certificates containing either the null prefix or no prefix extension at all.

When using RPKI certificate profile, prefix extensions are mandatory and the null prefix MUST be validated. However, a certificate may inherit its parent's prefix or range by using the "inherit" element for IPv6 AFI as defined in RFC3779. The use of the "inherit" element is permited in [I-D.ietf-sidr-res-certs].

Consequently, this document updates section 7.3 of RFC 3971 adding the following text under Unconstrained:

Network operators that do not want to constrain routers to route particular subnet prefixes but rather inherit them from its parent certificate, should configure routers with certificates containing the "inherit" element for IPv6 AFI.

5. Deployment Models

RFC 3971 describes two deployment models:centralized and decentralized. These models were differentiated by having one or many trust anchor. In this document we introduce two new deployment models, not based on the number of trust anchors but on the localization of the SEND deployment.

The local SEND deployment model represent those cases where SEND deployment is confined to an administrative domain. In this scenario, the deployment of SEND MAY be done independently of the existence of deployment in the upper RPKI hierarchy (i.e. an end user could perform local SEND deployment without the need of RPKI deployment in its ISP). This model requires the use of local trust anchors and configuring islands of trust. This model MAY include Unique Local Addresses(ULAs) [RFC4193].

The public SEND deployment models represent those cases where SEND deployment is linked to RPKI deployment as described in [I-D.ietf-sidr-arch]. Trust anchor material MAY be part of a different administrative domain (i.e. RIR, NIR or ISPs). It is a global model suitable for mobile users.

These two models are not mutually exclusive. It is entirely possible to have a hybrid model that incorporates features from both these models. In one such hybrid deployment model most IP address resources (e.g. global unicast addresses) would be certified under the global RPKI, while some others (e.g., ULAs) are certified under local TAs.

6. Trust Anchor Material

Relying parties (e.g., end hosts that implement SEND and process these router certificates) MUST be configured with one or more trust anchors to enable validation of the routers' certificates. Section 6.5 of RFC 3971 lists the trust anchor configurations for end hosts using SEND.

In the local SEND deployment model, it is possible to use as trust anchor a certificate that includes in its RFC 3779 address extension the prefix ::/0. In this case no new trust anchor material would be needed when renumbering. However, if trying to move from the local deployment model to the public deployment model, new trust anchor material will have to be distributed to relying parties.

[I-D.ietf-sidr-ta] describes a scenario where relying parties use as trust anchor material ETA (External Trust Anchor) certificates, which do not list any address space. This configuration allows network renumbering without the need for distributing new trust anchor material in both the local and the public model.

This document updates Section 6.5 of RFC3971, where the following paragraph should be added:

An end host MAY use as trust anchor material ETA certificates as described in [I-D.ietf-sidr-ta]. In this case, the end host MUST obtain the correspondent RTA (RPKI Trust Anchor) certificates from the ETA repository in order to complete the Name Type Field of the ICMP Trust Anchor Option, which MUST always refer to a trust anchor certificate that validates Section 9.

7. 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 is defined as optional in [I-D.ietf-sidr-res-certs] for end entity certificates but MUST be present when issuing end entity certificates for SEND.

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]. For an address in such certificate the host can assign the address, send/receive traffic from this address, and can respond to NSes about that address. For a prefix in such certificate the node can perform all the above mentioned operations for any address in that prefix. Also, when a prefix is present in the certificate with the owner authorization value, the node cannot advertise the prefix in an RA.

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) pkix(7) kp(3) }

id-kp-sendRouter OBJECT IDENTIFIER ::= { id-kp 23 }

id-kp-sendProxy OBJECT IDENTIFIER ::= { id-kp 24 }

id-kp-sendOwner OBJECT IDENTIFIER ::= { id-kp 25 }
```

As described in [I-D.ietf-sidr-res-certs], the extended key usage extension, if present, MUST be non-critical.

Relying Parties MUST 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 relying parties need not recognize all of them, as long as the required KeyPurposeId value is present.Relying parties MUST reject certificates that do not contain one of the three KeyPurposeIds defined above even if they include the anyExtendedKeyUsage OID defined in [RFC5280].

8. CRL profile and revocation

RPKI requires the use of CRLs [I-D.ietf-sidr-res-certs].The host will obtain the necessary CRLs and perform the certificate validation method described in [I-D.ietf-sidr-res-certs].

8.1. OCSP Considerations

By adopting the [I-D.ietf-sidr-res-certs] as the certificate profile for SEND, the use of the OCSP protocol is not allowed by the RPKI Certicate Policies [I-D.ietf-sidr-cp]. As CRLs are expected to be small, the fetching of the required CRLs are not expected to demand important bandwidth.

9. Certificate validation

This section updates section 6.3.1 of [RFC3971] by introducing new validations without introducing any conflict.

The host MUST perform the certificate validation method described in [I-D.ietf-sidr-res-certs].

The validation of certificates that uses the "inherit" element is describe in RFC 3779 where the existance of a parent prefix or range is required.

10. IANA Considerations

This document makes use of object identifiers to identify Extended Key Usages (EKUs) and the ASN.1 module found in Appendix B. The EKUs and ASN.1 module OID are registered in an arc delegated by IANA to the PKIX Working Group. No further action by IANA is necessary for this document.

11. 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. In particular, since a SEND certificate attests that its subject is authorized to play a given role in the SEND protocol, certificates that contain incorrect EKU values can enable some of the same attacks that SEND was meant to prevent. For example, if a malicious host can obtain a certificate that authorizes it to act as a router for a given prefix, then it can masquerade as a router for that prefix, e.g., in order to attract traffic from local nodes.

12. Acknowledgements

The authors would like to thank Stephen Kent, Sean Turner, Roni Even, Richard Barnes, Alexey Melnikov, Jari Arkko, David Harrington and Tim Polk for their reviews and suggestions on the earlier versions of this document.

13. References

13.1. Normative References

[I-D.ietf-csi-proxy-send]
Krishnan, S., Laganier, J., and M. Bonola, "Secure Proxy ND Support for SEND", draft-ietf-csi-proxy-send-01 (work in progress), July 2009.

[I-D.ietf-sidr-cp]
Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource PKI (RPKI)", draft-ietf-sidr-cp-08 (work in progress), January 2010.

[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-18 (work in progress), May 2010.

[I-D.ietf-sidr-ta]
Michaelson, G., Kent, S., and G. Huston, "A Profile for Trust Anchor Material for the Resource Certificate PKI", draft-ietf-sidr-ta-04 (work in progress), May 2010.

[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.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 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.

13.2. Informative References

[I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-09 (work in progress), October 2009.

[RFC5781] Weiler, S., Ward, D., and R. Housley, "The rsync URI Scheme", RFC 5781, February 2010.

Appendix A. Router Authorization Certificate example

```
    Certificate:
      Data:
          Version: 3 (0x2)
          Serial Number: 29 (0x1d)
          Signature Algorithm: sha256WithRSAEncryption
          Issuer: CN=EXAMPLE-CA-2342342652346
          Validity
              Not Before: Feb  15 23:06:53 2010 GMT
              Not After : Feb  15 23:06:53 2011 GMT
          Subject: CN=SEND-EXAMPLE-123432
          Subject Public Key Info:
              Public Key Algorithm: rsaEncryption
              RSA Public Key: (2048 bit)
                  Modulus (2048 bit):
                      00:bf:64:da:82:fb:b6:fd:a6:2d:c4:3a:10:d7:2c:
                      7b:8c:22:0a:30:b7:45:b1:7d:ae:c0:fd:f1:06:04:
                      5b:4a:6c:21:e7:de:15:cb:9a:07:c8:c4:80:6f:55:
                      cd:71:33:01:04:9f:87:57:db:d5:b3:c7:91:c5:81:
                      28:7f:a8:eb:b1:53:80:3a:01:8a:7c:97:d2:d3:41:
                      92:f4:68:db:3b:86:64:12:24:1e:e1:84:f8:33:5c:
                      0f:fa:ae:8a:a0:1f:e7:b7:4e:5a:ad:0a:a0:a1:2d:
                      42:5a:54:10:37:e2:13:84:88:ed:70:e4:76:6c:d6:
                      75:ab:8a:5c:c9:42:39:60:55:49:c2:66:ee:e7:64:
                      a1:67:fa:69:27:de:f6:2f:55:4d:09:89:29:75:c0:
                      61:02:41:7e:99:4f:81:1d:78:5a:45:8b:1c:9c:85:
                      87:76:51:a3:24:3b:0e:63:72:e8:b9:c5:81:32:91:
                      46:bb:87:81:82:5d:14:48:60:4a:ae:79:4f:f4:7e:
                      bd:ce:cf:01:de:19:e0:34:1a:12:fe:10:9d:1e:a6:
                      91:8b:28:ca:d6:83:71:8a:f3:39:fa:7a:49:c6:36:
                      b5:66:39:3a:a3:f8:02:70:a1:7a:8c:92:55:bd:b6:
                      84:cf:18:02:78:82:4f:2f:8e:f1:08:db:54:02:e0:
                      c5:e9
                  Exponent: 65537 (0x10001)
          X509v3 extensions:
              X509v3 Certificate Policies: critical
                  Policy: 1.3.6.1.5.5.7.14.2

              X509v3 Authority Key Identifier:
              keyid:F7:EB:16:AB:D2:43:E3:72:16:41:
              E0:B7:99:CA:1F:A4:37:C3:74:FB

              Authority Information Access:
                  CA Issuers - URI:rsync://rsync.example.exampledomain/
                  EXAMPLE-CA-2342342652346/EXAMPLE-CA.cer

              X509v3 CRL Distribution Points:
```

```
                URI:rsync://rsync.example.exampledomain/
                EXAMPLE-CA-2342342652346/EXAMPLE-CA.crl

            X509v3 Subject Key Identifier:
            5F:AB:EC:98:8A:E1:47:41:55:4F:67:57:98:
            22:CE:99:85:8F:2A:85
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                1.3.6.1.5.5.7.3.23
            sbgp-ipAddrBlock: critical
                IPv6:
                  2001:db8:CAFE:BEBE::/64

    Signature Algorithm: sha256WithRSAEncryption
        6f:ec:08:b2:5f:2c:84:6b:99:4c:fe:7d:00:db:fa:c1:90:a2:
        de:34:0a:31:b0:f6:f1:95:d9:4a:ef:09:79:90:51:84:a9:5a:
        a1:5a:a2:cd:09:69:e2:cb:ff:da:f1:34:32:bd:cc:b5:c8:7e:
        b1:fa:46:78:93:a5:cc:d5:1b:03:30:42:c4:ab:55:d7:e5:0d:
        74:de:e8:f3:00:6b:68:df:0d:64:ba:58:49:d0:0b:5d:a5:7c:
        82:ec:5c:95:18:fe:67:f5:25:21:9c:07:8e:ba:81:80:c8:c2:
        95:e6:0a:ea:bd:4b:a2:fc:10:53:cf:c9:16:83:83:88:7c:06:
        39:04:dd:49:4e:75:b5:4b:6b:8d:4c:9f:d7:59:33:c3:95:c4:
        7f:48:f5:83:da:37:e0:c1:a5:5d:09:7d:65:78:b6:77:a7:f9:
        49:59:f8:83:3e:14:dd:e0:86:e1:5e:fa:6d:42:ee:dd:eb:c0:
        f6:4b:0a:31:f1:37:1b:77:12:79:99:1b:2f:d5:e7:7f:2f:a2:
        6e:54:71:17:17:0d:a4:7b:7d:5a:6e:40:02:1d:5c:6a:06:ab:
        5d:33:ea:b6:8a:1b:f6:85:16:ef:d4:00:db:54:e8:ac:53:b8:
        0f:39:d8:a4:3e:9b:87:41:f3:f5:05:d6:a0:44:cc:82:bc:b9:
        fd:72:40:ff
```

Appendix B. ASN.1 Module

```
SENDCertExtns { iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-send-cert-extns(TBD) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- OID Arc

id-kp  OBJECT IDENTIFIER  ::=
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) kp(3) }

-- Extended Key Usage Values

id-kp-sendRouter OBJECT IDENTIFIER ::= { id-kp 23 }
id-kp-sendProxy OBJECT IDENTIFIER ::= { id-kp 24 }
id-kp-sendOwner OBJECT IDENTIFIER ::= { id-kp 25 }

END
```

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
University of Zagreb
Unska 3
Zagreb
Croatia

Email: ana.kukec@fer.hr