Internet Engineering Task Force (IETF)
Request for Comments: 6494
Updates: 3971
Category: Standards Track
ISSN: 2070-1721

R. Gagliano
Cisco Systems
S. Krishnan
Ericsson
A. Kukec
Enterprise Architects

February 2012

Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)

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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6494.

Table of Contents

1. Introduction

SEcure Neighbor Discovery (SEND) [RFC3971] utilizes X.509v3 certificates that include the [RFC3779] extension for IPv6 addresses to certify a router's authorization to advertise the 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 supersedes the profile for Router Authorization 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 the allocation of IP address space. The RPKI represents the centralized model discussed in Section 6.2 of [RFC3971]. Consequently, SEND will use the RPKI Certificate Profile and certificate validation detailed in [RFC6487]. Consequently, the certificate validation method described in [RFC3971] is updated with the certificate validation method in [RFC6487].

Since the [RFC3779] IPv6 address 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 why the certificate was issued. This document specifies four extended key usage values -- one for routers, two 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.

2. 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].

3. Terminology

Certified IPv6 address space	IPv6 address space included in an X.509v3 certificate using the extension for IPv6 addresses [RFC3779].
End-entity (EE)	An entity in the PKI that is not a Certification Authority (CA).
ISP	Internet Service Provider.
NIR	National Internet Registry.
RIR	Regional Internet Registry.
RPKI	Resource PKI established in accordance with [RFC6480].
RPKI certificates	Certificates as defined in [RFC6487].
SEND certificates	Certificates as described in [RFC3971] and extended in this document. They are end-entity certificates that belong either to SEND routers, SEND hosts, or SEND proxies: * Router Authorization Certificates as defined in [RFC3971]. * Owner Authorization Certificates as defined in [RFC3971].

* Secure Proxy ND Certificates as defined in [RFC6496].

SEND KeyPurposeId	An Extended Key Usage (EKU) value for SEND, such as the four introduced in this document.

4. SEND Certificate Profile

SEND certificates MUST comply with the RPKI resource profile described in [RFC6487]. A Router Authorization Certificate example is included in Appendix A.

In Sections 2, 4.9.10, and 4.9.11 of [RFC6487], it is stated that RFC 3779 resource extensions MUST be marked as critical and MUST be present in all resource certificates. SEND certificates MUST include the IP Address Delegation 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 [RFC6487]. SEND certificates MUST NOT have more than one IP Address Delegation 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 the 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 the IPv6 Address Family Identifier (AFI) as defined in [RFC3779]. The use of the "inherit" element is permitted in [RFC6487].

Consequently, this document updates Section 7.3 of [RFC3971], adding the following text under Unconstrained:

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

5. Deployment Models

RFC 3971 describes two deployment models: centralized and decentralized. These models were differentiated by having one trust anchor or many trust anchors. 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 represents 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 for 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 [RFC6480]. Trust anchor material MAY be part of a different administrative domain (i.e., RIRs, NIRs, 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 of 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 trust anchors.

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. [RFC6495] and Section 6.5 of [RFC3971] list the trust anchor configuration options for end hosts using SEND.

In the local SEND deployment model, it is possible to use as a 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.

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 the key usage extension, which indicates the intended purpose of the certified public key. The EKU extension is defined as optional in [RFC6487] 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 four KeyPurposeId values: one for authorizing routers (Router Authorization Certificates), two for authorizing proxies (Secure Proxy ND Certificates), and one for address owners (Owner Authorization Certificates). Additional KeyPurposeId values may be specified in Standards Track documents.

The inclusion of the router authorization value (id-kp-sendRouter) indicates that the certificate has been issued for allowing the router to generate Router Advertisement (RA) and Redirect messages for any prefix(es) encompassed (as defined in Section 7.1 of [RFC6487]) by the IP address space included in the X.509 extensions for IP addresses.

The inclusion of the proxied routing authorization value (id-kp-sendProxiedRouter) indicates that the certificate has been issued for allowing the proxy to perform proxying of RA and Redirect messages for any prefix(es) encompassed by the IP address space included in the X.509 extensions for IP addresses.

The inclusion of the owner authorization value (id-kp-sendOwner) indicates that the certificate has been issued for allowing the node to use any address(es) that is/are encompassed by the IP address space included in the X.509 extensions for IP addresses. For an address in such a certificate, the node can assign the address to an interface; send/receive traffic from/to this address; and send/respond to NS, NA, and RS messages related to that address.

The inclusion of the proxied owner authorization value (id-kp-sendProxiedOwner) indicates that the certificate has been issued for allowing the proxy to perform proxying of Neighbor

Solicitation (NS), Neighbor Advertisement (NA), and Router Solicitation (RS) messages for any address encompassed by the IP address space included in the X.509 extensions for IP addresses.

```
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-sendProxiedRouter OBJECT IDENTIFIER ::= { id-kp 24 }

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

id-kp-sendProxiedOwner OBJECT IDENTIFIER ::= { id-kp 26 }
```

As described in [RFC6487], 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-sendProxiedRouter) 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 at least one SEND KeyPurposeId, even if they include the anyExtendedKeyUsage OID defined in [RFC5280].

8. CRL Profile and Revocation

RPKI requires the use of Certificate Revocation Lists (CRLs) [RFC6487]. The host will obtain the necessary CRLs and perform the certificate validation method described in [RFC6487].

8.1. Online Certificate Status Protocol (OCSP) Considerations

A host MAY use OCSP [RFC2560] to verify the revocation status of a certificate.

As [RFC6487] is adopted as the base certificate profile for SEND, the host SHOULD NOT assume that certificates will include the URI of an OCSP server as part of its Authority Information Access (AIA) extension. This is particularly evident in the SEND public deployment model, as OCSP services are not required by [RFC6484].

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 [RFC6487]. The validation of certificates that use the "inherit" element where the existence of a parent prefix or range is required is described in [RFC3779].

The host MUST verify that the KeyPurposeId value corresponding to the Neighbor Discovery message type is present, as described in Section 7.

10. IANA Considerations

This document makes use of object identifiers to identify EKUs and the ASN.1 (Abstract Syntax Notation One) 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.

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 Alberto Garcia, 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

[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., Ed., 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.

[RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource Public Key Infrastructure (RPKI)", BCP 173, RFC 6484, February 2012.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", RFC 6487, February 2012.

[RFC6495] Gagliano, R., Krishnan, S., and A. Kukec, "Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields", RFC 6495, February 2012.

13.2. Informative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

[RFC6496] Krishnan, S., Laganier, J., Bonola, M., and A. Garcia-Martinez, "Secure Proxy ND Support for SEcure Neighbor Discovery (SEND)", RFC 6496, February 2012.

Appendix A. Router Authorization Certificate Example

```
   Certificate:
       Data:
           Version: 3 (0x2)
           Serial Number: 249 (0xf9)
           Signature Algorithm: sha256WithRSAEncryption
           Issuer: CN=EXAMPLE-CA-2342342652346
           Validity
               Not Before: Jul  2 10:06:32 2010 GMT
               Not After : Jul  2 10:06:32 2011 GMT
           Subject: CN=SEND-EXAMPLE-123432
           Subject Public Key Info:
               Public Key Algorithm: rsaEncryption
                   Public-Key: (2048 bit)
                   Modulus:
                       00:b7:06:0d:8e:f7:39:0a:41:52:93:59:a8:f5:63:
                       3f:2e:3d:24:17:9d:19:aa:09:ff:c0:2a:f3:c6:99:
                       d7:34:0d:bf:f1:e9:73:b5:8f:dc:d4:91:d6:5d:cb:
                       9c:b8:2b:41:63:c1:8f:f7:48:54:02:89:07:24:c3:
                       b0:6e:11:5a:7d:c0:38:88:4b:d9:3b:93:c7:ca:4d:
                       a4:00:a2:d3:6d:14:15:8f:15:08:4d:4e:b3:8a:cc:
                       de:2d:e0:7a:9b:c0:6e:14:f6:a7:ae:b9:e0:c5:18:
                       60:75:3d:d3:50:00:47:0d:86:5b:1c:a0:85:81:af:
                       2b:84:98:49:7d:60:a2:e8:4f:6d:40:ba:d5:fe:de:
                       de:41:53:c7:c4:f4:d3:1a:41:cd:dc:9f:08:43:33:
                       48:00:57:e4:56:93:7d:dd:19:12:e8:bf:26:b3:4b:
                       30:ac:b8:9c:b1:37:05:18:3c:7b:6b:26:d7:c9:15:
                       c9:4a:eb:1b:fa:92:38:46:27:44:96:8a:a1:12:c1:
                       09:77:4a:7b:a5:07:88:a6:36:30:98:70:79:b6:44:
                       7e:b1:c9:4c:5b:11:56:e8:14:50:f7:f8:e5:ed:f1:
                       ac:a4:31:46:36:77:05:c9:63:fe:c3:ab:54:e2:bd:
                       79:1d:14:d1:c2:80:36:d3:be:e6:c7:a2:47:59:1b:
                       75:9f
                   Exponent: 65537 (0x10001)

           X509v3 extensions:
               X509v3 Authority Key Identifier:
                   keyid:4C:5D:56:82:15:8A:67:A6:8C:69:67:68:88
                   :6F:15:E5:C9:96:58:EB

               X509v3 CRL Distribution Points:

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

```
            X509v3 Subject Key Identifier:
                B8:69:EB:36:23:F1:C4:21:65:DD:13:76:EE:90:AF
                :F7:CD:E3:61:CD
            X509v3 Key Usage: critical
                Digital Signature
            sbgp-ipAddrBlock: critical
                IPv6:
                  2001:db8:cafe:bebe::/64

            X509v3 Extended Key Usage:
                1.3.6.1.5.5.7.3.23
    Signature Algorithm: sha256WithRSAEncryption
        92:14:38:6e:45:83:1b:cb:7c:45:0d:bc:7f:6e:36:bf:82:cc:
        7e:00:91:ea:f4:24:43:cc:00:3c:3f:c2:99:0c:c6:b9:20:2e:
        ca:dc:df:94:0d:c9:a1:75:c4:5c:39:a1:cf:9f:e1:40:9c:aa:
        a9:80:76:d1:3a:91:d9:db:2f:cd:3c:05:50:52:eb:28:47:d0:
        ab:d3:fd:6f:30:17:16:7f:c6:0f:2b:25:bb:db:29:d7:bb:4e:
        f3:7c:2d:e1:04:b7:f0:bc:d5:8a:ba:8c:0d:39:22:48:02:d1:
        67:fb:35:5c:b6:83:03:63:7c:73:03:70:20:de:fb:d7:12:ed:
        6f:a1:ff:b2:a6:39:fb:55:9a:07:bd:68:40:0f:6f:d5:24:34:
        cf:e8:dd:76:33:2a:d0:b9:1b:ae:a8:68:86:17:f8:13:35:0e:
        f6:04:ec:2a:39:88:06:70:c6:e8:56:87:f7:35:54:2a:28:2c:
        92:47:a9:89:39:d7:72:24:21:9d:02:52:f9:7c:76:7f:e9:cd:
        09:6e:82:f4:da:6c:f9:72:b2:64:98:b5:0c:6a:38:8d:81:e5:
        fc:50:46:6f:38:40:56:06:92:5a:e0:86:5d:55:f5:7b:85:b2:
        68:4f:49:72:e0:fa:2c:bf:9e:7d:aa:28:17:ca:04:b8:ae:69:
        c9:04:28:12
```

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(71) }

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-sendProxiedRouter OBJECT IDENTIFIER ::= { id-kp 24 }
   id-kp-sendOwner OBJECT IDENTIFIER ::= { id-kp 25 }
   id-kp-sendProxiedOwner OBJECT IDENTIFIER ::= { id-kp 26 }

   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
Enterprise Architects
46/525 Collins St.
Melbourne, VIC 3000
Australia

EMail: ana.kukec@enterprisearchitects.com