Network Working Group	R. Gagliano	
Internet-Draft	Cisco Systems	
Updates: 3971 (if approved)	S. Krishnan	
Intended status: Standards Track	Ericsson	
Expires: May 28, 2011	A. Kukec	
	University of Zagreb	
	November 24, 2010	

TOC

Certificate profile and certificate management for SEND
draft-ietf-csi-send-cert-10

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

Copyright Notice

described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

---

1. Requirements notation

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

---

2. Introduction

TOC

SEcure Neighbor Discovery [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) (SEND) utilizes X.509v3 certificates that include the [RFC3779] (Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers," June 2004.) 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 supersedes the profile for router certificates specified in [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.). 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] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.).

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 referred in Section 6.2 of [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.). Consequently, SEND will use the RPKI certificate profile and certificate validation detailed in [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.). 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] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.).

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 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.

---

3. Terminology

TOC

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.

ISP Internet Service Provider.

NIR National Internet Registry.

RIR
Regional Internet Registry.

RPKI Resource PKI established in accordance with [I-D.ietf-sidr-arch] (Lepinski, M. and S. Kent, “An Infrastructure to Support Secure Internet Routing,” September 2010.).

RPKI certificates Certificates defined in [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” October 2010.).

SEND certificates Certificates described in [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) and extended in this document. They are end-entity certificates that belong either to SEND routers, SEND hosts or SEND Proxies:

- Router Authorization Certificates defined in [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.).
- Owner Authorization Certificates defined in [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.).
- Secure Proxy ND Certificates defined in [I-D.ietf-csi-proxy-send] (Krishnan, S., Laganier, J., Bonola, M., and A. Garcia-Martinez, “Secure Proxy ND Support for SEND,” September 2010.).

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

---

4. SEND Certificate profile

TOC

SEND certificates MUST comply with the RPKI resource profile [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” October 2010.). 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] (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” October 2010.) 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] (Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP

Addresses and AS Identifiers," June 2004.). 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] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.). SEND certificates MUST NOT have more than one IP Resources extension.

4.1. Unconstrained Certified subnet prefixes

TOC

Section 7.3 of [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) 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] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.).
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

TOC

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] (Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses," October 2005.).
The public SEND deployment models represent those cases where SEND deployment is linked to RPKI deployment as described in

[I-D.ietf-sidr-arch] (Lepinski, M. and S. Kent, “An Infrastructure to Support Secure Internet Routing,” September 2010.). 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

TOC

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 and [I-D.ietf-csi-send-name-type-registry] (Gagliano, R., Krishnan, S., and A. Kukec, “Subject Key Identifier (SKI) SEND Name Type fields.,” June 2010.) list the trust anchor configuration options 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.

---

7. Extended Key Usage Values

TOC

The Internet PKI document [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,” May 2008.) 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 EKU extension is defined as optional in [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” October 2010.) 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 standard 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 RA and Redirect messages for any prefix(es) encompassed (as defined in Section 7.1 of [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.)) 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 proxied owner authorization value (id-kp-sendProxiedOwner) indicates that the certificate has been issued for allowing the proxy to perform proxying of NS, NA and RS messages for any address 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 certificate the node can assign the address to an interface, send/receive traffic from/to this address, and can send/respond NS, NA and RS messages about that address.

```
  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 [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.), 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 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] (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," May 2008.).

---

8. CRL profile and revocation

TOC

RPKI requires the use of CRLs [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.).The host will obtain the necessary CRLs and perform the certificate validation method described in [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.).

8.1. Online Certificate Status Protocol (OCSP) Considerations

TOC

A host MAY use OCSP [RFC2560] (Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," June 1999.) protocol to verify the revocation status of a certificate.
By adopting the [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates," October 2010.) as the 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 [I-D.ietf-sidr-cp] (Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate Policy (CP) for the Resource PKI (RPKI," October 2010.).

---

9. Certificate validation

TOC

This section updates section 6.3.1 of [RFC3971] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.) by introducing new validations without introducing any conflict.
The host MUST perform the certificate validation method described in [I-D.ietf-sidr-res-certs] (Huston, G., Michaelson, G., and R. Loomans, “A Profile for X.509 PKIX Resource Certificates,” October 2010.). The validation of certificates that uses the "inherit" element is describe in RFC 3779 where the existence of a parent prefix or range is required.
The host MUST verify that the Key PurposedId value corresponding to the Neighbor Discovery message type is present as described in Section 7.

---

10. IANA Considerations

TOC

This document makes use of object identifiers to identify EKUs and the ASN.1 (Abstract Syntax Notation One) module found in Appendix B (ASN.1 Module). 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

TOC

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.

TOC

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

TOC

13.1. Normative References

TOC

[I-D.ietf-csi-send-name-type-registry]	Gagliano, R., Krishnan, S., and A. Kukec, “Subject Key Identifier (SKI) SEND Name Type fields.,” draft-ietf-csi-send-name-type-registry-06 (work in progress), June 2010 (TXT).
[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-15 (work in progress), October 2010 (TXT).
[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-19 (work in progress), October 2010 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[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 (TXT).
[RFC3779]	Lynn, C., Kent, S., and K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers,” RFC 3779, June 2004 (TXT).
[RFC3971]	Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” RFC 3971, March 2005 (TXT).
[RFC4193]	Hinden, R. and B. Haberman, “Unique Local IPv6 Unicast Addresses,” RFC 4193, October 2005 (TXT).
[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 (TXT).

13.2. Informative References

TOC

[I-D.ietf-csi-proxy-send]	Krishnan, S., Laganier, J., Bonola, M., and A. Garcia-Martinez, "Secure Proxy ND Support for SEND," draft-ietf-csi-proxy-send-05 (work in progress), September 2010 (TXT).
[I-D.ietf-sidr-arch]	Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing," draft-ietf-sidr-arch-11 (work in progress), September 2010 (TXT).

TOC

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
```

TOC

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

TOC

	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