            A Profile for BGPsec Router Certificates,
      Certificate Revocation Lists, and Certification Requests
               draft-ietf-sidr-bgpsec-pki-profiles-18

Abstract

   This document defines a standard profile for X.509 certificates used
   to enable validation of Autonomous System (AS) paths in the Border
   Gateway Protocol (BGP), as part of an extension to that protocol
   known as BGPsec. BGP is the standard for inter-domain routing in the
   Internet; it is the "glue" that holds the Internet together. BGPsec
   is being developed as one component of a solution that addresses the
   requirement to provide security for BGP. The goal of BGPsec is to
   provide full AS path validation based on the use of strong
   cryptographic primitives. The end-entity (EE) certificates specified
   by this profile are issued (to routers within an Autonomous System).
   Each of these certificates is issued under a Resource Public Key
   Infrastructure (RPKI) Certification Authority (CA) certificate.
   These CA certificates and EE certificates both contain the AS
   Identifier Delegation extension. An EE certificate of this type
   asserts that the router(s) holding the corresponding private key are
   authorized to emit secure route advertisements on behalf of the
   AS(es) specified in the certificate. This document also profiles the
   format of certification requests, and specifies Relying Party (RP)
   certificate path validation procedures for these EE certificates.
   This document extends the RPKI; therefore, this documents updates the
   RPKI Resource Certificates Profile (RFC 6487).

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."

Copyright Notice

Table of Contents

1. Introduction

This document defines a profile for X.509 end-entity (EE)
certificates [RFC5280] for use in the context of certification of
Autonomous System (AS) paths in the Border Gateway Protocol Security
protocol (BGPsec). Such certificates are termed "BGPsec Router
Certificates". The holder of the private key associated with a
BGPsec Router Certificate is authorized to send secure route
advertisements (BGPsec UPDATEs) on behalf of the AS(es) named in the
certificate. A router holding the private key is authorized to send
route advertisements (to its peers) that contain one or more of the
specified AS number as the last item in the AS PATH attribute. A key
property provided by BGPsec is that every AS along the AS PATH can
verify that the other ASes along the path have authorized the
advertisement of the given route (to the next AS along the AS PATH).

This document is a profile of [RFC6487], which is a profile of
[RFC5280]; thus this document updates [RFC6487]. It establishes
requirements imposed on a Resource Certificate that is used as a
BGPsec Router Certificate, i.e., it defines constraints for
certificate fields and extensions for the certificate to be valid in
this context. This document also profiles the certification requests
used to acquire BGPsec Router Certificates. Finally, this document
specifies the Relying Party (RP) certificate path validation
procedures for these certificates.

1.1. Terminology

It is assumed that the reader is familiar with the terms and concepts
described in "A Profile for X.509 PKIX Resource Certificates"
[RFC6487], "BGPsec Protocol Specification" [ID.sidr-bgpsec-protocol],
"A Border Gateway Protocol 4 (BGP-4)" [RFC4271], "BGP Security
Vulnerabilities Analysis" [RFC4272], "Considerations in Validating
the Path in BGP" [RFC5123], and "Capability Advertisement with BGP-4"
[RFC5492].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
[RFC2119].

2. Describing Resources in Certificates

Figure 1 depicts some of the entities in the RPKI and some of the
products generated by RPKI entities. IANA issues a Certification
Authority (CA) certificate to each Regional Internet Registry (RIR).
The RIR, in turn, issues a CA certificate to an Internet Service
Providers (ISP). The ISP in turn issues EE Certificates to itself to

enable verification of signatures on RPKI signed objects. The CA also
generate. The CA also generates Certificate Revocation Lists (CRLs).
 These CA and EE certificates are referred to as "Resource
Certificates", and are profiled in [RFC6487]. The [RFC6480]
envisioned using Resource Certificates to enable verification of
Manifests [RFC6486] and Route Origin Authorizations (ROAs) [RFC6482].
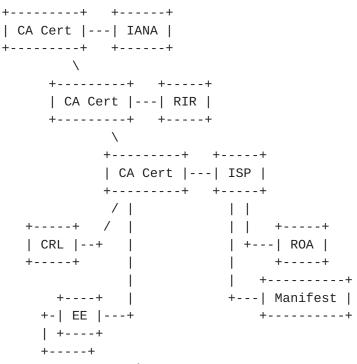 ROAs and Manifests include the Resource Certificates used to verify
them.

```
                +---------+   +------+
                | CA Cert |---| IANA |
                +---------+   +------+
                     \
                  +---------+   +-----+
                  | CA Cert |---| RIR |
                  +---------+   +-----+
                       \
                     +---------+   +-----+
                     | CA Cert |---| ISP |
                     +---------+   +-----+
                      / |              | |
              +-----+  / |             | |   +-----+
              | CRL |--+  |            | +---| ROA |
              +-----+     |            |     +-----+
                          |            |   +----------+
                +----+    |            +---| Manifest |
              +-| EE |---+                 +----------+
              | +----+
              +-----+
                          Figure 1
```

This document defines another type of Resource Certificate, which is
referred to as a "BGPsec Router Certificate". The purpose of this
certificate is explained in Section 1 and falls within the scope of
appropriate uses defined within [RFC6484]. The issuance of BGPsec
Router Certificates has minimal impact on RPKI CAs because the RPKI
CA certificate and CRL profile remain unchanged (i.e., they are as
specified in [RFC6487]). Further, the algorithms used to generate
RPKI CA certificates that issue the BGPsec Router Certificates and
the CRLs necessary to check the validity of the BGPsec Router
Certificates remain unchanged (i.e., they are as specified in
[ID.sidr-rfc6485bis]). The only impact is that RPKI CAs will need to
be able to process a profiled certificate request (see Section 5)
signed with algorithms found in [ID.sidr-bgpsec-algs]. The use of
BGPsec Router Certificates in no way affects RPKI RPs that process
Manifests and ROAs because the public key found in the BGPsec Router
Certificate is used only to verify the signature on the BGPsec

certificate request (only CAs process these) and the signature on a
BGPsec Update Message [ID.sidr-bgpsec-protocol] (only BGPsec routers
process these).

This document enumerates only the differences between this profile
and the profile in [RFC6487]. Note that BGPsec Router Certificates
are EE certificates and as such there is no impact on process
described in [RFC6916].

3. Updates to [RFC6487]

3.1 BGPsec Router Certificate Fields

A BGPsec Router Certificate is a valid X.509 public key certificate,
consistent with the PKIX profile [RFC5280], containing the fields
listed in this section. This profile is also based on [RFC6487] and
only the differences between this profile and the profile in
[RFC6487] are specified below.

3.1.1.1. Subject

This field identifies the router to which the certificate has been
issued. Consistent with [RFC6487], only two attributes are allowed
in the Subject field: common name and serial number. Moreover, the
only common name encoding options that are supported are
printableString and UTF8String. For BGPsec Router Certificates, it
is RECOMMENDED that the common name attribute contain the literal
string "ROUTER-" followed by the 32-bit AS Number [RFC3779] encoded
as eight hexadecimal digits and that the serial number attribute
contain the 32-bit BGP Identifier [RFC4271] (i.e., the router ID)
encoded as eight hexadecimal digits. If there is more than one AS
number, the choice of which to include in the common name is at the
discretion of the Issuer. If the same certificate is issued to more
than one router (hence the private key is shared among these
routers), the choice of the router ID used in this name is at the
discretion of the Issuer. Note that router IDs are not guaranteed to
be unique across the Internet, and thus the Subject name in a BGPsec
Router Certificate issued using this convention also is not
guaranteed to be unique across different issuers. However, each
certificate issued by an individual CA MUST contain a Subject name
that is unique within that context.

3.1.2. Subject Public Key Info

Refer to section 3.1 of [ID.sidr-bgpsec-algs].

3.1.3. BGPsec Router Certificate Version 3 Extension Fields

3.1.3.1. Basic Constraints

   BGPsec speakers are EEs; therefore, the Basic Constraints extension
   must not be present, as per [RFC6487].

3.1.3.2. Extended Key Usage

   BGPsec Router Certificates MUST include the Extended Key Usage (EKU)
   extension. As specified in [RFC6487] this extension MUST be marked
   as non-critical. This document defines one EKU for BGPsec Router
   Certificates:

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

   id-kp-bgpsec-router OBJECT IDENTIFIER ::= { id-kp 30 }
```

   A BGPsec router MUST require the extended key usage extension to be
   present in a BGPsec Router Certificate it receives. If multiple
   KeyPurposeId values are included, the BGPsec routers need not
   recognize all of them, as long as the required KeyPurposeId value is
   present. BGPsec routers MUST reject certificates that do not contain
   the BGPsec Router EKU even if they include the anyExtendedKeyUsage
   OID defined in [RFC5280].

3.1.3.3. Subject Information Access

   This extension is not used in BGPsec Router Certificates. It MUST be
   omitted.

3.1.3.4. IP Resources

   This extension is not used in BGPsec Router Certificates. It MUST be
   omitted.

3.1.3.5. AS Resources

   Each BGPsec Router Certificate MUST include the AS Resource
   Identifier Delegation extension, as specified in section 4.8.11 of
   [RFC6487]. The AS Resource Identifier Delegation extension MUST
   include one or more AS numbers, and the "inherit" element MUST NOT be
   specified.

3.2. BGPsec Router Certificate Request Profile

Refer to section 6 of [RFC6487]. The only differences between this
profile and the profile in [RFC6487] are:

  o The Basic Constraints extension:

    If included, the CA MUST NOT honor the cA boolean if set to TRUE.

  o The Extended Key Usage extension:

    If included, id-kp-bgpsec-router MUST be present (see Section
    3.1). If included, the CA MUST honor the request for id-kp-
    bgpsec-router.

  o The Subject Information Access extension:

    If included, the CA MUST NOT honor the request to include the
    extension.

  o The SubjectPublicKeyInfo and PublicKey fields are specified in
    [ID.sidr-bgpsec-algs].

  o The request is signed with the algorithms specified in [ID.sidr-
    bgpsec-algs].

3.3. BGPsec Router Certificate Validation

   The validation procedure used for BGPsec Router Certificates is
   identical to the validation procedure described in Section 7 of
   [RFC6487] (and any RFC that updates this procedure), but using the
   constraints applied come from this specification. For example, in
   step 3: "the certificate contains all the field that must be present"
   - refers to the fields that are required by this specification.

   The differences are as follows:

  o BGPsec Router Certificates MUST include the BGPsec Router EKU
    defined in Section 3.1.3.2.

  o BGPsec Router Certificates MUST NOT include the SIA extension.

  o BGPsec Router Certificates MUST NOT include the IP Resource
    extension.

  o BGPsec Router Certificates MUST include the AS Resource Identifier
    Delegation extension.

  o BGPsec Router Certificate MUST include the "Subject Public Key
    Info" described in [ID.sidr-bgpsec-algs] as it updates [ID.sidr-

   rfc6485bis].

   NOTE: The cryptographic algorithms used by BGPsec routers are found
   in [ID.sidr-bgpsec-algs]. Currently, the algorithms specified in
   [ID.sidr-bgpsec-algs] and [ID.sidr-rfc6485bis] are different. BGPsec
   RPs will need to support algorithms that are used to validate BGPsec
   signatures as well as the algorithms that are needed to validate
   signatures on BGPsec certificates, RPKI CA certificates, and RPKI
   CRLs.

3.4. Router Certificates and Signing Functions in the RPKI

   As described in Section 1, the primary function of BGPsec route
   certificates in the RPKI is for use in the context of certification
   of Autonomous System (AS) paths in the Border Gateway Protocol
   Security protocol (BGPsec).

   The private key associated with a router EE certificate may be used
   multiple times in generating signatures in multiple instances of the
   BGPsec_Path Attribute Signature Segments [ID.sidr-bgpsec-protocol].
   I.e., the BGPsec router certificate is used to validate multiple
   signatures.

   BGPsec router certificates are stored in the issuing CA's repository,
   where a repository following RFC6481 MUST use a .cer filename
   extension for the certificate file.

4. Design Notes

   The BGPsec Router Certificate profile is based on the Resource
   Certificate profile as specified in [ID.sidr-rfc6485bis]. As a
   result, many of the design choices herein are a reflection of the
   design choices that were taken in that prior work. The reader is
   referred to [RFC6484] for a fuller discussion of those choices.

   CAs are required by the Certificate Policy (CP) [RFC6484] to issue
   properly formed BGPsec Router Certificates regardless of what is
   present in the certification request so there is some flexibility
   permitted in the certificate requests:

    o BGPsec Router Certificates are always EE certificates; therefore,
      requests to issue a CA certificate result in EE certificates;

    o BGPsec Router Certificates are always EE certificates; therefore,
      requests for Key Usage extension values keyCertSign and cRLSign
      result in certificates with neither of these values;

    o BGPsec Router Certificates always include the BGPsec Rouer EKU

value; therefore, request without the value result in certificates
with the value; and,

o BGPsec Router Certificates never include the Subject Information
Access extension; therefore, request with this extension result in
certificates without the extension.

Note that this behavior is similar to the CA including the AS
Resource Identifier Delegation extension in issued BGPsec Router
Certificates despite the fact it is not present in the request.

5. Implementation Considerations

This document permits the operator to include a list of ASNs in a
BGPsec Router Certificate. In that case, the router certificate would
become invalid if any one of the ASNs is removed from any superior CA
certificate along the path to a trust anchor. Operators could choose
to avoid this possibility by issuing a separate BGPsec Router
Certificate for each distinct ASN, so that the router certificates
for ASNs that are retained in the superior CA certificate would
remain valid.

6. Security Considerations

The Security Considerations of [RFC6487] apply.

A BGPsec Router Certificate will fail RPKI validation, as defined in
[RFC6487], because the algorithm suite is different. Consequently, a
RP needs to identify the EKU to determine the appropriate Validation
constraint.

A BGPsec Router Certificate is an extension of the RPKI [RFC6480] to
encompass routers. It is a building block BGPsec and is used to
validate signatures on BGPsec Signature-Segment origination of
Signed-Path segments [ID.sidr-bgpsec-protocol]. Thus its essential
security function is the secure binding of one or more AS numbers to
a public key, consistent with the RPKI allocation/assignment
hierarchy.

Hash functions [ID.sidr-bgpsec-algs] are used when generating the two
key identifiers extension included in BGPsec certificates. However
as noted in [RFC6818], collision resistance is not a required
property of one-way hash functions when used to generate key
identifiers. Regardless, hash collisions are possible and if
detected an operator should be alerted.

7. IANA Considerations

This document makes use of two object identifiers in the SMI Registry
for PKIX. One is for the ASN.1 module in Appendix A and it comes
from the SMI Security for PKIX Module Identifier IANA registry (id-
mod-bgpsec-eku). The other is for the BGPsec router EKU defined in
Section 3.1.3.2 and Appendix A and it comes from the SMI Security for
PKIX Extended Key Purpose IANA registry. These OIDs were assigned
before management of the PKIX Arc was handed to IANA. No IANA
allocations are request of IANA, but please update the references in
those registries when this document is published by the RFC editor.

8. Acknowledgements

We would like to thank Geoff Huston, George Michaelson, and Robert
Loomans for their work on [RFC6487], which this work is based on. In
addition, the efforts of Steve Kent and Matt Lepinski were
instrumental in preparing this work. Additionally, we'd like to
thank Rob Austein, Roque Gagliano, Richard Hansen, Geoff Huston,
David Mandelberg, Sandra Murphy, and Sam Weiller for their reviews
and comments.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI
           10.17487/RFC2119, March 1997, <http://www.rfc-
           editor.org/info/rfc2119>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP
           Addresses and AS Identifiers", RFC 3779, DOI
           10.17487/RFC3779, June 2004, <http://www.rfc-
           editor.org/info/rfc3779>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border
           Gateway Protocol 4 (BGP-4)", RFC 4271, DOI
           10.17487/RFC4271, January 2006, <http://www.rfc-
           editor.org/info/rfc4271>.

[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, DOI 10.17487/RFC5280, May 2008,
           <http://www.rfc-editor.org/info/rfc5280>.

[RFC6487] Huston, G., Michaelson, G., and R. Loomans, "A Profile for
           X.509 PKIX Resource Certificates", RFC 6487, DOI
           10.17487/RFC6487, February 2012, <http://www.rfc-

          editor.org/info/rfc6487>.

   [RFC6818] Yee, P., "Updates to the Internet X.509 Public Key
             Infrastructure Certificate and Certificate Revocation List
             (CRL) Profile", RFC 6818, DOI 10.17487/RFC6818, January
             2013, <http://www.rfc-editor.org/info/rfc6818>.

   [ID.sidr-rfc6485bis] G. Huston and G. Michaelson, "The Profile for
             Algorithms and Key Sizes for use in the Resource Public Key
             Infrastructure", draft-ietf-sidr-rfc6485bis, work-in-
             progress.

   [ID.sidr-bgpsec-algs] S. Turner, "BGP Algorithms, Key Formats, &
             Signature Formats", draft-ietf-sidr-bgpsec-algs, work-in-
             progress.

9.2. Informative References

   [RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis",
             RFC 4272, DOI 10.17487/RFC4272, January 2006,
             <http://www.rfc-editor.org/info/rfc4272>.

   [RFC5123] White, R. and B. Akyol, "Considerations in Validating the
             Path in BGP", RFC 5123, DOI 10.17487/RFC5123, February
             2008, <http://www.rfc-editor.org/info/rfc5123>.

   [RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement
             with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009,
             <http://www.rfc-editor.org/info/rfc5492>.

   [RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support
             Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480,
             February 2012, <http://www.rfc-editor.org/info/rfc6480>.

   [RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route
             Origin Authorizations (ROAs)", RFC 6482, DOI
             10.17487/RFC6482, February 2012, <http://www.rfc-
             editor.org/info/rfc6482>.

   [RFC6484] Kent, S., Kong, D., Seo, K., and R. Watro, "Certificate
             Policy (CP) for the Resource Public Key Infrastructure
             (RPKI)", BCP 173, RFC 6484, DOI 10.17487/RFC6484, February
             2012, <http://www.rfc-editor.org/info/rfc6484>.

   [RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski,
             "Manifests for the Resource Public Key Infrastructure
             (RPKI)", RFC 6486, DOI 10.17487/RFC6486, February 2012,
             <http://www.rfc-editor.org/info/rfc6486>.

   [RFC6916] Gagliano, R., Kent, S., and S. Turner, "Algorithm Agility
             Procedure for the Resource Public Key Infrastructure
             (RPKI)", BCP 182, RFC 6916, DOI 10.17487/RFC6916, April
             2013, <http://www.rfc-editor.org/info/rfc6916>.

   [ID.sidr-bgpsec-protocol] Lepinksi, M., "BGPsec Protocol
             Specification", draft-ietf-sidr-bgpsec-protocol, work-in-
             progress.

Appendix A. ASN.1 Module

```
   BGPSECEKU { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-bgpsec-eku(84) }

     DEFINITIONS EXPLICIT TAGS ::=

     BEGIN

     -- EXPORTS ALL --

     -- IMPORTS NOTHING --

     -- OID Arc --

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

     -- BGPsec Router Extended Key Usage --

     id-kp-bgpsec-router OBJECT IDENTIFIER ::= { id-kp 30 }

     END
```

Authors' Addresses

   Mark Reynolds
   Island Peak Software
   328 Virginia Road
   Concord, MA 01742

   Email: mcr@islandpeaksoftware.com

   Sean Turner
   sn3rd

   EMail: sean@sn3rd.com

Stephen Kent
Raytheon BBN Technologies
10 Moulton St.
Cambridge, MA 02138

Email: kent@bbn.com