Secure Inter-Domain Routing Working Group
Internet-Draft
Updates: 6487 (if approved)
Intended status: Standard Track
Expires: May 7, 2016

M. Reynolds
IPSw
S. Turner
IECA
S. Kent
BBN

November 4, 2015

A Profile for BGPsec Router Certificates, Certificate Revocation Lists, and Certification Requests
draft-ietf-sidr-bgpsec-pki-profiles-14

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."

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 [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 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.

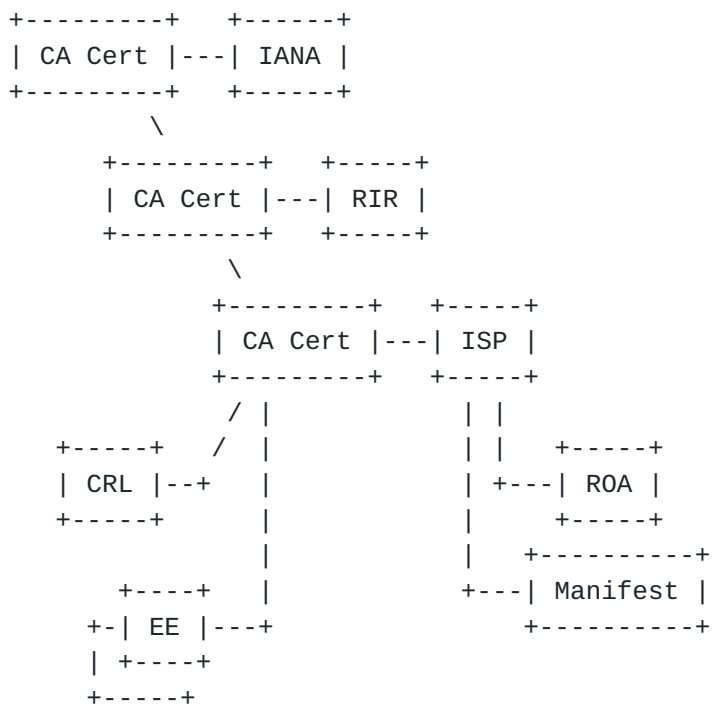

Figure 1

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:

- The ExtendedKeyUsage extension request MUST be included and the CA MUST honor the request;
- The SubjectPublicKeyInfo and PublicKey fields are specified in [ID.sidr-bgpsec-algs]; and,
- 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], 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:

- BGPsec Router Certificates MUST include the BGPsec EKU defined in Section 3.1.3.1.
- BGPsec Router Certificates MUST NOT include the SIA extension.
- BGPsec Router Certificates MUST NOT include the IP Resource extension.
- BGPsec Router Certificates MUST include the AS Resource Identifier Delegation extension.
- 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.

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.

5. 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.

6. 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.

7. 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 Roque Gagliano, Sandra Murphy, Geoff Huston, Richard Hansen, David Mandelberg, and Sam Weiller for their reviews and comments.

8. References

8.1. Normative References

[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.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[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.

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

[RFC6818] Yee, P., "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 6818, January 2013.

[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.

8.2. Informative References

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

[RFC5123] White, R. and B. Akyol, "Considerations in Validating the Path in BGP", RFC 5123, February 2008.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement

with BGP-4", RFC 5492, February 2009.

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

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, February 2012.

[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.

[RFC6486] Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Infrastructure (RPKI)", RFC 6486, February 2012.

[RFC6916] Gagliano, R., Kent, S., and S. Turner, "Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)", BCP 182, RFC 6916, April 2013.

[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
```

Appendix B. Change Log

Please delete this section prior to publication.

B.0 Changes from sidr-bgpsec-pki-profiles-12 to sidr-bgpsec-pki-profiles-13

Minor modifications to address WGLC comments.

B.1 Changes from sidr-bgpsec-pki-profiles-11 to sidr-bgpsec-pki-profiles-12

Added security consideration to address SKI collisions. Also updated the IANA considerations section.

B.2 Changes from sidr-bgpsec-pki-profiles-10 to sidr-bgpsec-pki-profiles-11

Removed text in s3.1.3. Consistently used BGPsec to refer to BGP Security. Fixed typos. Refer to RFC6485bis instead of RFC6485. Included OIDs.

B.3. Changes from sidr-bgpsec-pki-profiles-09 to sidr-bgpsec-pki-profiles-10

Updated dates.

B.4. Changes from sidr-bgpsec-pki-profiles-08 to sidr-bgpsec-pki-profiles-09

Editorial fixes for the sake of brevity.

B.5. Changes from sidr-bgpsec-pki-profiles-07 to sidr-bgpsec-pki-profiles-08

Fixed section numbering.

B.6. Changes from sidr-bgpsec-pki-profiles-06 to sidr-bgpsec-pki-profiles-07

Added text to multiple AS numbers in a single certificate. Updated reference to RFC 6916.

B.7. Changes from sidr-bgpsec-pki-profiles-05 to sidr-bgpsec-pki-profiles-06

Keep alive version.

B.8. Changes from sidr-bgpsec-pki-profiles-04 to sidr-bgpsec-pki-profiles-05

Keep alive version.

B.9. Changes from sidr-bgpsec-pki-profiles-03 to sidr-bgpsec-pki-profiles-04

In s2.1, removed the phrase "another BGPSEC Router Certificate (only BGPSEC routers process these)" because the BGPSEC certificates are only ever EE certificates and they're never used to verify another certificate only the PDUs that are signed.

Added new s3.1.3.1 to explicitly state that EE certificates are only ever EE certs.

B.10. Changes from sidr-bgpsec-pki-profiles-02 to sidr-bgpsec-pki-profiles-03

Updated s3.3 to clarify restrictions on path validation procedures are in this specification (1st para was reworded).

Updated s3.3 to point to s3.1.3.1 for BGPSEC EKU (thanks Tom).

B.11. Changes from sidr-bgpsec-pki-profiles-01 to sidr-bgpsec-pki-profiles-02

Updated references.

B.12. Changes from sidr-bgpsec-pki-profiles-00 to sidr-bgpsec-pki-profiles-01

Added an ASN.1 Module and corrected the id-kp OID in s3.1.3.1.

B.13. Changes from turner-bgpsec-pki-profiles-02 to sidr-bgpsec-pki-profiles-00

Added this change log.

Amplified that a BGPSEC RP will need to support both the algorithms in [ID.sidr-bgpsec-algs] for BGPSEC and the algorithms in [ID.sidr-rpki-algs] for certificates and CRLs.

Changed the name of AS Resource extension to AS Resource Identifier Delegation to match what's in RFC 3779.

B.14. Changes from turner-bgpsec-pki-profiles -01 to -02

Added text in Section 2 to indicate that there's no impact on the procedures defined in [RFC6916].

Added a security consideration to let implementers know the BGPSEC certificates will not pass RPKI validation [RFC6487] and that keying off the EKU will help tremendously.

B.15. Changes from turner-bgpsec-pki-profiles -00 to -01

Corrected Section 2 to indicate that CA certificates are also RPKI certificates.

Removed sections and text that was already in [RFC6487]. This will make it easier for reviewers to figure out what is different.

Modified Section 6 to use 2119-language.

Removed requirement from Section 6 to check that the AS # in the certificate is the last number in the AS path information of each BGP UPDATE message. Moved to [ID.sidr-bgpsec-protocol].

Authors' Addresses

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

Email: mcr@islandpeaksoftware.com

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com

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

Email: kent@bbn.com