SIDR Working Group
Internet-Draft
Updates: 6487 (if approved)
Intended status: Standards Track
Expires: February 14, 2015

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

August 13, 2014

A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests

draft-ietf-sidr-bgpsec-pki-profiles-08

Abstract

This document defines a standard profile for X.509 certificates for the purposes of supporting 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 a critical component for the proper operation of the Internet as a whole. The BGPSEC protocol is under development as a component to address the requirement to provide security for the BGP protocol. The goal of BGPSEC is to design a protocol for full AS path validation based on the use of strong cryptographic primitives. The End-Entity (EE) certificates specified by this profile are issued under Resource Public Key Infrastructure (RPKI) Certification Authority (CA) certificates, containing the AS Identifier Delegation extension, to routers within the Autonomous System (AS). The certificate asserts that the router(s) holding the private key are authorized to send out secure route advertisements on behalf of the specified AS. This document also profiles the Certificate Revocation List (CRL), profiles the format of certification requests, and specifies Relying Party certificate path validation procedures. The 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."

This Internet-Draft will expire on February 14, 2015.

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 (BGPSEC) protocol. 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 named in the certificate. That is, a router holding the private key may send to its BGP peers, route advertisements that contain the specified AS number as the last item in the AS PATH attribute. A key property that BGPSEC will provide 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], and it 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 Certificate Revocation List (CRL) and certification requests. Finally, this document specifies the Relying Party (RP) certificate path validation procedures.

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" [I-D.ietf-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) to a Regional Internet Registries (RIR). The RIR, in turn, issues a CA certificate to an Internet Service Provider (ISP). The ISP in turn issues End-Entity (EE) Certificates to itself as well as CRLs. These certificates are referred to as "Resource Certificates", and are profiled in [RFC6487]. The [RFC6480] envisioned using Resource Certificates to generate Manifests [RFC6486] and Route Origin Authorizations (ROAs) [RFC6482]. ROAs and Manifests also include the Resource Certificates used to sign them.

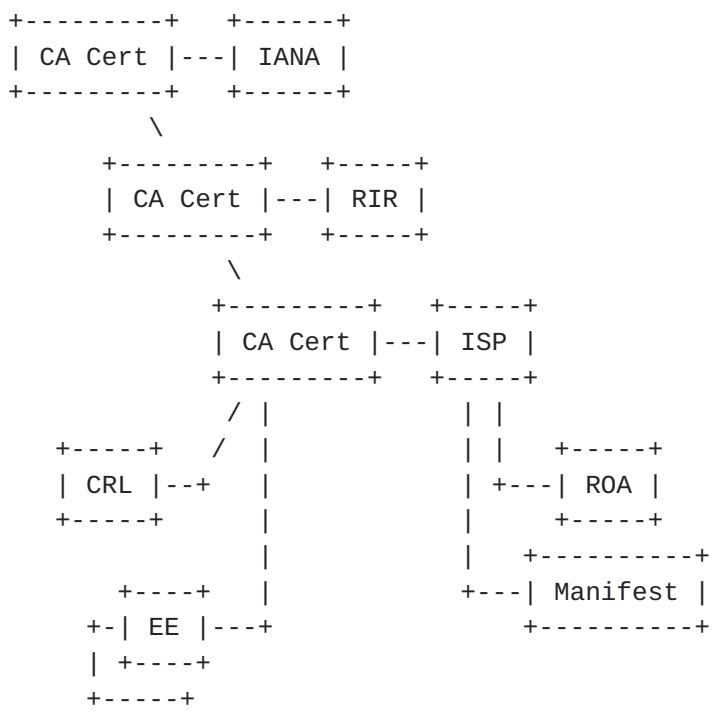

Figure 1: RPKI and BGPsec Hierarchies

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 [I-D.ietf-sidr-rfc6485bis]). The only impact is that the RPKI CAs will need to be able to process a profiled certificate request (see Section 5) signed with algorithms found in [I-D.ietf-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 only ever used to verify the signature on the BGPSEC certificate request (only CAs process these) and the signature on a BGPSEC Update Message [I-D.ietf-sidr-bgpsec-protocol] (only BGPSEC routers process these).

Only the differences between this profile and the profile in [RFC6487] are listed. Note that BGPSEC Router Certificates are EE certificates and as such there is no impact on process described in [RFC6916].

3. Updates to RFC 6487

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 listed.

3.1.1. 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 more than one certificate for an AS is issued (i.e., more than one router gets a certificate for the AS and hence the private key is shared among more than one router), the choice of the router ID used in Subject 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 [I-D.ietf-sidr-bgpsec-algs].

3.1.3. BGPSEC Router Certificate Version 3 Extension Fields

The following X.509 V3 extensions MUST be present (or MUST be absent, if so stated) in a conforming BGPSEC Router Certificate, except where explicitly noted otherwise. No other extensions are allowed in a conforming BGPSEC Router Certificate.

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 }
```

Relying Parties MUST require the extended key usage extension be present in a BGPSEC Router Certificate. If multiple KeyPurposeId values are included, the relying parties need not recognize all of them, as long as the required KeyPurposeId value is present. BGPSEC RPs 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 absent.

3.1.3.4. IP Resources

This extension is not used in BGPSEC Router Certificates. It MUST be absent.

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 only one AS number, 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 [I-D.ietf-sidr-bgpsec-algs]; and,

- The attributes field contains the ASN extension with exactly one ASN.

- The request is signed with the algorithms specified in [I-D.ietf-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]. The exception is that the constraints applied come from this specification (e.g., in step 3: the certificate contains all the field that must be present - refers to the fields that are required by this specification).

{spt: should the algorithm fail if there's more than one in the cert?}

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 and only one AS number.

- BGPSEC Router Certificate MUST include the "Subject Public Key Info" described in [I-D.ietf-sidr-bgpsec-algs] as it updates [I-D.ietf-sidr-rfc6485bis].

NOTE: The cryptographic algorithms used by BGPSEC routers are found in [I-D.ietf-sidr-bgpsec-algs]. Currently, the algorithms specified in [I-D.ietf-sidr-bgpsec-algs] and [I-D.ietf-sidr-rfc6485bis] are different. BGPSEC RPs will need to support algorithms that are needed 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 [I-D.ietf-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.

One design choice made by this document is to include one AS number per certificate. Simplicty is the driving rationale. If a router supports more than one AS, the router can simply be issued another certificate though the impact on the router is that additional secure storage may be needed for additional private keys.

5. Security Considerations

The Security Considerations of [RFC6487] apply.

A BGPSEC certificate will fail RPKI validation, as defined in [RFC6487], because the algorithm suite is different. Consequently, a RP needs to identify the EKU before applying the correspondent validation.

A BGPSEC Router Certificate is an extension of the RPKI [RFC6480] to encompass routers. It is a building block of the larger BGPSEC security protocol used to validate signatures on BGPSEC Signature-Segment origination of Signed-Path segments [I-D.ietf-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.

6. IANA Considerations

None.

7. Acknowledgements

We would like to thanks 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, Randy Bush, and Rob Austein for their reviews and comments. Finally, we'd like to thank Russ Housley for assigning us an OID for the ASN.1 module.

8. References

8.1. Normative References

[I-D.ietf-sidr-bgpsec-algs]
Turner, S., "BGP Algorithms, Key Formats, & Signature Formats", draft-ietf-sidr-bgpsec-algs-08 (work in progress), July 2014.

[I-D.ietf-sidr-rfc6485bis]
Huston, G. and G. Michaelson, "The Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure", draft-ietf-sidr-rfc6485bis-01 (work in progress), March 2014.

[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., Li, T., and S. Hares, "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.

8.2. Informative References

[I-D.ietf-sidr-bgpsec-protocol]
Lepinski, M., "BGPSEC Protocol Specification", draft-ietf-sidr-bgpsec-protocol-09 (work in progress), July 2014.

[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.

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. Example BGPSEC Router Certificate

Appendix C. Example BGPSEC Router Certificate Request

Appendix D. Change Log

Please delete this section prior to publication.

D.1. Changes from sidr-bgpsec-pki-profiles-07 to sidr-bgpsec-pki-profiles-08

Changed references to RFC 6485 to [I-D.ietf-sidr-rfc6485bis] and added OIDs for ASN.1 module. Certificate and certification request restricted to contain one ASN.

D.2. 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.

D.3. Changes from sidr-bgpsec-pki-profiles-05 to sidr-bgpsec-pki-profiles-06

Keep alive version.

D.4. Changes from sidr-bgpsec-pki-profiles-04 to sidr-bgpsec-pki-profiles-05

Keep alive version.

D.5. 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.

D.6. 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).

D.7. Changes from sidr-bgpsec-pki-profiles-01 to sidr-bgpsec-pki-profiles-02

Updated references.

D.8. 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.

D.9. 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 [I-D.ietf-sidr-bgpsec-algs] for BGPSEC and the algorithms in [RFC6487] for certificates and CRLs.

Changed the name of AS Resource extension to AS Resource Identifier Delegation to match what's in [RFC3779].

D.10. 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.

D.11. 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 [I-D.ietf-sidr-bgpsec-protocol].

Authors' Addresses

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

Email: mcr@islandpeaksoftware.com

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

Phone: +1-703-628-3180
Email: turners@ieca.com

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

Email: kent@bbn.com