S. Kent
M. Lepinski
M. Reynolds
BBN

Internet-Draft
Intended status: Standards Track
Expires: December 4, 2011

June 2, 2011

# A Profile for BGPSEC Router Certificates
draft-reynolds-bgpsec-rtrcerts-00

## Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on December 4, 2011.

## Copyright and License Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must included Simplified BSD License text as described in Section 4.e of the Legal Trust Provisions and are provided without warranty as described in the BSD License.

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 PKI (RPKI) CA certificates, containing the RFC 3779 AS number extension, to routers within the autonomous system. The certificate asserts that the router(s) holding the public key are authorized to send out secure route advertisements on behalf of the specified autonomous system. Note that since these certificates extend the RPKI [ID.sidr-arch], this profile is based on the profile for RPKI resource certificates [ID.res-cert-prof].

Table of Contents

## 1. Introduction

This document defines a profile for X.509 end entity (EE) certificates [X.509] for use in the context of certification of AS paths in the 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 autonomous system 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 [ID.res-cert-prof], which is a profile of RFC 5280. 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. A relying party processing what purports to be a BGPSEC Router certificate MUST verify that the certificate conforms to this profile.

### 1.1 Terminology

It is assumed that the reader is familiar with the terms and concepts described in "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280], "X.509 Extensions for IP Addresses and AS Identifiers" [RFC3779],

"Capability Advertisement with BGP-4" [RFC 5492], "Considerations in Validating the Path in BGP" [RFC 5123], "BGP Security Vulnerabilities Analysis" [RFC 4272], and "A Border Gateway Protocol 4 (BGP-4)" [RFC 4271].

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 RFC 2119.





## 2. Describing Resources in Certificates

The framework for describing an association between the subject of a certificate and the AS resources currently under the subject's control is described in RFC 3779.

There are two aspects of this resource extension that are noted in this profile. First, RFC 3779 notes that a resource extension SHOULD be a CRITICAL extension to the X.509 certificate. This BGPSEC Router certificate profile further mandates that this certificate extension MUST appear in all BGPSEC Router certificates and MUST be marked as CRITICAL. Second, a test of the resource extension in the context of certificate validity includes the condition that the resources described in the immediate parent CA certificate in the PKI (the certificate where this certificate's issuer is the subject) has a resource set, hereinafter called the "issuer's resource set" that MUST encompass the resource set of the issued certificate. In this context "encompass" allows for the issuer's resource set to be the same as, or a strict superset of, a subject's resource set.

## 3. BGPSEC Router Certificate Fields

A BGPSEC Router Certificate is a valid X.509 public key certificate, consistent with the PKIX profile [RFC5380], containing the fields listed in this section. Unless specifically noted as being OPTIONAL, all the fields listed here MUST be present, and any other field MUST NOT appear in a conforming BGPSEC Router Certificate. If a field value is specified here, this value MUST be used in conforming BGPSEC Router certificates. For any BGPSEC Router certificate field that is the same as in the [ID.res-cert-prof] profile, this document will cite the corresponding section in that document.

### 3.1 Version

Refer to section 4.1 of [ID.res-cert-prof].

## 3.2 Serial Number

Refer to section 4.2 of [ID.res-cert-prof].

## 3.3 Signature Algorithm

Refer to section 4.3 of [ID.res-cert-prof].

## 3.4 Issuer

Refer to section 4.4 of [ID.res-cert-prof]. The value of this field is a distinguished name that adheres to the conventions imposed on Issuer (and Subject) names that appear in Resource Certificates, as described in [ID.sidr-arch].

## 3.5 Subject

This field identifies the router to which the certificate has been issued. Consistent with [ID.res-cert-prof], 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 router certificates, it is RECOMMENDED that the common name attribute contain the literal string "ROUTER-" followed by the 32-bit router ID encoded as eight hexadecimal digits. 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.

## 3.6 Valid From

Refer to section 4.6 of [ID.res-cert-prof].

## 3.7 Valid To

Refer to section 4.6 of [ID.res-cert-prof].

### 3.8 Subject Public Key Info

Refer to section 4.7 of [ID.res-cert-prof].

### 3.9 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.

#### 3.9.1 Basic Constraints

The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. Since a BGPSEC Router certificate is always an EE certificate, the basic constraints extension MUST NOT be present.

#### 3.9.2 Subject Key Identifier

The subject key identifier (SKI) extension MUST appear in every Resource Certificate, as per section 4.8.2 of [ID.res-cert-prof]. For a BGPSEC Router certificate, the SKI is used as a shorthand means of uniquely identifying an individual certificate. The SKI in a Resource certificate is generated from the public key in the certificate, using the SHA-1 algorithm, as described in section 4.2.1.2 of RFC 5280. This extension MUST appear in all BGPSEC Router certificates. This extension is non-critical.

#### 3.9.3 Authority Key Identifier

This is a non-critical extension and it MUST be present, as per section 4.8.3 of [ID.res-cert-prof].

#### 3.9.4 Key Usage

This is a critical extension, and it MUST be present. The





digitalSignature bit MUST be set to TRUE in all BGPSEC Router

certificates, and it MUST be the only bit set to TRUE.

### 3.9.5 Extended Key Usage

The EKU extension MUST NOT appear in a BGPSEC Router certificate.

### 3.9.6 CRL Distribution Points

The CRLDP extension is non-critical and MUST appear in every BGPSEC Router Certificate, as per section 4.8.6 of [ID.res-cert-prof].

### 3.9.7 Authority Information Access

The AIA extension is non-critical and MUST appear in every BGPSEC Router Certificate, as per section 4.8.7 of [ID.res-cert-prof].

### 3.9.8 Subject Information Access

This extension is not used in BGPSEC Router certificates. It MUST be omitted.

### 3.9.9 Certificate Policies

This critical extension MUST be present as per section 4.8.9 of [ID.res-cert-prof].

### 3.9.10 IP Resources

This extension is not used in BGPSEC Router certificates. It MUST be omitted.

### 3.9.11 AS Resources

This extension contains the list of AS numbers that the router is authorized to represent in BGP advertisements, encoded as specified in RFC 3779. The "inherit" element MUST NOT be specified. As specified in section 4.8.11 of [ID.res-cert-prof], RDI values MUST NOT be used. All BGPSEC Router certificates MUST include an AS resources extension, and the extension MUST contain exactly one AS number. This extension MUST be marked critical.

## 4. BGPSEC Router Certificate Revocation List Profile

BGPSEC Router certificates are just another type of EE certificate issued by an RPKI CA. Therefore, there are no distinguishing features for the CRLs on which they appear. Refer to section 5 of [ID.res-cert-prof] for a complete description of the profile for these CRLs.

## 5. BGPSEC Router Certificate Request Profile

Refer to section 6 of [ID.res-cert-prof].

## 6. BGPSEC Router Certificate Validation

The validation procedure used for BGPSEC Router certificates is identical to the validation procedure described in Section 7 of [ID.res-cert-prof], with two further restrictions. First, all IP address resources for a BGPSEC Router certificate will be empty. Second, the sole AS number resource in the BGPSEC Router certificate must match the last AS number in the AS path information of each BGP UPDATE message. While this second restriction is not part of validation per se, it is part of the operational validation of UPDATEs performed by the router.

## 7. Design Notes

The BGPSEC Router Certificate profile is based off the Resource Certificate profile as specified in [ID.res-cert-prof]. 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 [ID.res-cert-prof] for a fuller discussion of those choices.

## 8. Security Considerations

The Security Considerations of RFC5280 and RFC3779 apply to BGPSEC Router Certificates as defined by this profile, and their use. Additionally, the Security Considerations documented in the RPKI Architecture and Resource Certificate Profile [ID.res-cert-prof] apply.

A BGPSEC Router Certificate is an extension of the RPKI 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. Thus its essential security function is the secure binding of an AS number to a public key, consistent with the RPKI allocation/assignment hierarchy.

## 9. IANA Considerations

[Note to IANA, to be removed prior to publication: there are no IANA

considerations stated in this version of the document.]

# 10 References

## 10.1 Normative References


[ID.sidr-rpki-algs]
Huston, G., "A Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure" (work in progress); Internet Drafts draft-ietf-sidr-rpki-algs-05.txt, April 2011.

[RFC2050] Hubbard, K., Kosters, M., Conrad, D., Karrenburg, D., and J. Postel, "INTERNET REGISTRY IP ALLOCATION GUIDELINES", BCP 12, RFC 2050, November 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3513] Hinden, R., and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC4211] Schaad, J., and S. Deering, "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, June 2004.

[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.

[X.509] ITU-T, "Recommendation X.509: The Directory Authentication Format", 2000.

[I-D. sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-side-arch-13.txt (work in progress), May 2011.

[I-D. sidr-manifests]
Austein, R., Huston, G., Kent, S., and M. Lepinski, "Manifests for the Resource Public Key Intrastructure" (work in progress); Internet Draft draft-ietf-sidr-rpki-manifests-12.txt, May 2011.

[I-D. sidr-res-cert-prof]
Huston, G., Michaelson, G., and R. Loomans, "A Profile for X.509 PKIX Resource Certificates", draft-ietf-sidr-res-certs-22.txt; (work in progress), May 2011.

## 10.2 Informative References

[rsync] Tridgell, A., "rsync", April 2006, <http://samba.anu.edu.au/rsync/>

## Authors' Addresses

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

Email: kent@bbn.com

Matthew Lepinski
Raytheon BBN Technologies Corp.
10 Moulton St.
Cambridge, MA 02138

Email: mlepinsk@bbn.com

Mark Reynolds
Raytheon BBN Technologies Corp.





10 Moulton St.
Cambridge, MA 02138

Email: mreynold@bbn.com

## Appendix A: Example BGPSEC Router Certificate

TBD

## Appendix B: Example Certificate Revocation List

TBD