Secure Inter-Domain Routing Working Group
Internet-Draft
Updates: 7935 (if approved)
Intended status: Standards Track
Expires: May 18, 2017

S. Turner
sn3rd

November 14, 2016

BGPsec Algorithms, Key Formats, & Signature Formats
draft-ietf-sidr-bgpsec-algs-16

Abstract

This document specifies the algorithms, algorithm parameters, asymmetric key formats, asymmetric key size and signature format used in BGPsec (Border Gateway Protocol Security). This document updates the Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RFC 7935).

Table of Contents

1. Introduction

This document specifies:

- the digital signature algorithm and parameters;
- the hash algorithm and parameters;
- the public and private key formats; and,
- the signature format

used by Resource Public Key Infrastructure (RPKI) Certification Authorities (CA), and BGPsec (Border Gateway Protocol Security) speakers (i.e., routers). CAs use these algorithms when processing requests for BGPsec Router Certificates [ID.sidr-bgpsec-pki-profiles]. Examples when BGPsec routers use these algorithms include requesting BGPsec certificates [ID.sidr-bgpsec-pki-profiles], signing BGPsec Update messages [ID.sidr-bgpsec-protocol], and verifying BGPsec Update messages [ID.sidr-bgpsec-protocol].

This document updates [RFC7935] to add support for a) a different algorithm for BGPsec certificate requests, which are issued only by BGPsec speakers; b) a different Subject Public Key Info format for BGPsec certificates, which is needed for the specified BGPsec signature algorithm; and, c) a different signature format for BGPsec signatures, which is needed for the specified BGPsec signature algorithm. The BGPsec certificate are differentiated from other RPKI certificates by the use of the BGPsec Extended Key Usage defined in [ID.sidr-bgpsec-pki-profiles].

1.1. Terminology

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. Algorithms

The algorithms used to compute signatures on CA certificates, BGPsec Router Certificates, and CRLs are as specified in Section 2 of [RFC7935]. This section addresses BGPsec algorithms, for example these algorithms are used by BGPsec routers to request BGPsec certificates, by RPKI CAs to verify BGPsec certification requests, by BGPsec routers to generate BGPsec Update messages, and by BGPsec routers to verify BGPsec Update message:

- The signature algorithm used MUST be the Elliptic Curve Digital Signature Algorithm (ECDSA) with curve P-256 [RFC6090][DSS].

- The hash algorithm used MUST be SHA-256 [SHS].

Hash algorithms are not identified by themselves in certificates or BGPsec Update messages. They are represented by an OID that combines the hash algorithm with the digital signature algorithm as follows:

- The ecdsa-with-SHA256 OID [RFC5480] MUST appear in the PKCS #10 signatureAlgorithm field [RFC2986] or in Certificate Request Message Format (CRMF) POPOSigningKey algorithm field [RFC4211], which location depends on the certificate request format generated.

- In BGPsec Update messages, the ECDSA with SHA-256 Algorithm Suite Identifier value 0x1 (see Section 7) is included in the Signature-Block List's Algorithm Suite Identifier field.

3. Asymmetric Key Pair Formats

The key formats used to compute signatures on CA certificates, BGPsec Router Certificates, and CRLs are as specified in Section 3 of [RFC7935]. This section addresses key formats found in the BGPsec router certificate requests and in BGPsec Router Certificates.

The ECDSA private keys used to compute signatures for certificate requests and BGPsec Update messages MUST come from the P-256 curve [RFC5480]. The public key pair MUST use the uncompressed form.

3.1. Public Key Format

The Subject's public key is included in subjectPublicKeyInfo [RFC5280]. It has two sub-fields: algorithm and subjectPublicKey. The values for the structures and their sub-structures follow:

- algorithm (an AlgorithmIdentifier type): The id-ecPublicKey OID MUST be used in the algorithm field, as specified in Section 2.1.1 of [RFC5480]. The value for the associated parameters MUST be secp256r1, as specified in Section 2.1.1.1 of [RFC5480].

- subjectPublicKey: ECPoint MUST be used to encode the certificate's subjectPublicKey field, as specified in Section 2.2 of [RFC5480].

3.2. Private Key Format

Local Policy determines private key format.

4. Signature Format

The structure for the certificate's and CRL's signature field MUST be as specified in Section 4 of [RFC7935], which is the same format used by other RPKI certificates. The structure for the certification request's and BGPsec Update message's signature field MUST be as specified in Section 2.2.3 of [RFC3279].

5. Additional Requirements

It is anticipated that BGPsec will require the adoption of updated key sizes and a different set of signature and hash algorithms over time, in order to maintain an acceptable level of cryptographic security. This profile should be updated to specify such future requirements, when appropriate.

The recommended procedures to implement such a transition of key sizes and algorithms is specified in [RFC6916].

6. Security Considerations

The Security Considerations of [RFC3279], [RFC5480], [RFC6090], [RFC7935], and [ID.sidr-bgpsec-pki-profiles] apply to certificates. The security considerations of [RFC3279], [RFC6090], [RFC7935], [ID.sidr-bgpsec-pki-profiles] apply to certification requests. The security considerations of [RFC3279], [ID.sidr-bgpsec-protocol], and [RFC6090] apply to BGPsec Update messages. No new security considerations are introduced as a result of this specification.

7. IANA Considerations

The Internet Assigned Numbers Authority (IANA) is requested to define the "BGPsec Algorithm Suite Registry" in the Resource Public Key Infrastructure (RPKI) group. The one-octet BGPsec Algorithm Suite Registry identifiers assigned by IANA identifies the digest algorithm and a signature algorithm used in the BGPsec Signature-Block List's Algorithm Suite Identifier field.

IANA is kindly requested to also register a single algorithm suite identifier, for the digest algorithm SHA-256 [SHS] and the signature algorithm ECDSA on the P-256 curve [RFC6090][DSS].

BGPsec Algorithm Suites Registry

Algorithm Suite Identifier	Digest Algorithm	Signature Algorithm	Specification Pointer
0x0	Reserved	Reserved	This draft
0x1	SHA-256	ECDSA P-256	[SHS][DSS][RFC6090]
0x2-0xE	Unassigned	Unassigned	This draft
0xF	Reserved	Reserved	This draft

Future assignments are to be made using the Standards Action process defined in [RFC5226]. Assignments consist of the one-octet algorithm suite identifier value and the associated digest algorithm name and signature algorithm name.

8. Acknowledgements

The author wishes to thank Geoff Huston and George Michaelson for producing [RFC7935], which this document is entirely based on. I'd also like to thank Roque Gagliano, David Mandelberg, Tom Petch, Sam Weiller, and Stephen Kent 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>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <http://www.rfc-editor.org/info/rfc2986>.

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, DOI 10.17487/RFC3279, April 2002, <http://www.rfc-editor.org/info/rfc3279>.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, DOI 10.17487/RFC4211, September 2005, <http://www.rfc-editor.org/info/rfc4211>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[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>.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, DOI 10.17487/RFC5480, March 2009, <http://www.rfc-editor.org/info/rfc5480>.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, DOI 10.17487/RFC6090, February 2011, <http://www.rfc-editor.org/info/rfc6090>.

[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>.

[RFC7935] Huston, G. and G. Michaelson, Ed., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure", RFC 7935, DOI 10.17487/RFC7935, August 2016, <http://www.rfc-editor.org/info/rfc7935>.

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

[ID.sidr-bgpsec-pki-profiles] Reynolds, M. and S. Turner, "A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests", draft-ietf-sidr-bgpsec-pki-profiles, work-in-progress.

[DSS] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, "Digital Signature Standard", FIPS Publication 186-4, July 2013.

[SHS] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, "Secure Hash Standard", FIPS Publication 180-4, August 2015.

9.2. Informative References

None.

Authors' Addresses

Sean Turner
sn3rd

EMail: sean@sn3rd.com