BGP Algorithms, Key Formats, & Signature Formats
draft-ietf-sidr-bgpsec-algs-03

Abstract

   This document specifies the algorithms, algorithms' 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 6485).

Status of this Memo

Copyright Notice

1. Introduction

   This document specifies:
      o the digital signature algorithm and parameters;
      o the hash algorithm and parameters;
      o the public and private key formats; and,
      o 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 issuing
   BGPSEC Router Certificates [ID.bgpsec-pki-profiles] and CRLs
   [RFC6487]. BGPSEC routers use these when requesting BGPSEC
   certificates [ID.bgpsec-pki-profiles], generating BGPSEC Update
   messages [ID.sidr-bgpsec-protocol], and verifying BGPSEC Update
   messages [ID.sidr-bgpsec-protocol].

   This document is referenced by the BGPSEC specification [ID.bgpsec-
   protocol] and the profile for BGPSEC Router Certificates and
   Certification Requests [ID.bgpsec-pki-profiles]. Familiarity with
   these documents is assumed. Implementers are reminded, however,
   that, as noted in Section 2 of [ID.bgpsec-pki-profiles], the
   algorithms used to sign CA Certificates, BGPSEC Router Certificates,
   and CRLs are found in [RFC6485].

   This document updates [RFC6485] to add support for a) a different
   algorithm for BGPSEC certificate requests, which are only issued 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.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

   Four cryptographic algorithms are used to support BGPSEC:

     o The signature algorithm used when issuing BGPSEC certificates and
       CRLs, which would revoke BGPSEC certificates, MUST be as
       specified in [RFC6485].

o The signature algorithm used in certification requests and BGPSEC
  Update messages MUST be Elliptic Curve Digital Signature
  Algorithm (ECDSA) [RFC6090].

o The hashing algorithm used when issuing certificates and CRLs
  MUST be as specified in [RFC6485].

o The hashing algorithm use when generating certification requests
  and BGPSEC Update messages MUST be SHA-256 [SHS]. Hash
  algorithms are not identified by themselves in certificates, or
  BGPSEC Update messages instead they are combined with the digital
  signature algorithm (see below).

  NOTE: The exception to the above hashing algorithm is the use of
  SHA-1 [SHS] when CAs generate authority and subject key
  identifiers [ID.bgpsec-pki-profiles].

To support BGPSEC, the algorithms are identified as follows:

o In certificates and CRLs, an Object Identifier (OID) is used.
  The value and locations are as specified in section 2 of
  [RFC6485].

o In certification request, an OID is used. The ecdsa-with-SHA256
  OID [RFC5480] MUST appear in the PKCS #10 signatureAlgorithm
  field [RFC4211] or in Certificate Request Message Format (CRMF)
  POPOSigningKey signature field [RFC2986].

o In BGPSEC Update messages, the ECDSA with SHA-256 Algorithm Suite
  Identifier from Section 7 is included in the Signature-Block
  List's Algorithm Suite Identifier field.

3. Asymmetric Key Format

The RSA key pairs used to compute signatures on CA certificates,
BGPSEC Router Certificates, and CRLs are as specified in section 3 of
[RFC6485]. The remainder of this section addresses key formats found
in the BGPSEC router certificate requests and in BGPSEC Router
Certificates.

The ECDSA key pairs 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:

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

   o subjectPublicKey: ECPublicKey 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 [RFC6485]. 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 to protect the integrity of BGPSEC. This profile should be
   updated to specify such future requirements, when appropriate.

   CAs and RPs SHOULD be capable of supporting a transition to allow for
   the phased introduction of additional encryption algorithms and key
   specifications, and also accommodate the orderly deprecation of
   previously specified algorithms and keys. Accordingly, CAs and RPs
   SHOULD be capable of supporting multiple RPKI algorithm and key
   profiles simultaneously within the scope of such anticipated
   transitions. The recommended procedures to implement such a
   transition of key sizes and algorithms is not specified in this
   document.

6. Security Considerations

   The Security Considerations of [RFC3279], [RFC5480], [RFC6090],
   [RFC6485], and [ID.bgpsec-pki-profiles] apply to certificates. The
   security considerations of [RFC3279], [RFC6090], [RFC6485],
   [ID.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 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" described below.

An algorithm suite consists of a digest algorithm and a signature algorithm. This specification creates an IANA registry of one-octet BGPSEC algorithm suite identifiers. Additionally, this document registers a single algorithm suite which uses the digest algorithm SHA-256 and the signature algorithm ECDSA on the P-256 curve [RFC5480].

BGPSEC Algorithm Suites Registry

Digest Algorithm	Signature Algorithm	Algorithm Suite Identifier	Specification Pointer
SHA-256	ECDSA P-256	TBD	RFC 5480

Future assignments are to be made using either the Standards Action process defined in [RFC5226], or the Early IANA Allocation process defined in [RFC4020]. Assignments consist of a digest algorithm name, signature algorithm name, and the algorithm suite identifier value.

10. Acknowledgements

The author wishes to thank Geoff Huston for producing [RFC6485], which this document is heavily based on. I'd also like to thank Roque Gagliano for his review and comments.

11. References

11.1. Normative References

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

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, November 2000.

[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, April 2002.

[RFC4020] Kompella, K. and A. Zinin, "Early IANA Allocation of
          Standards Track Code Points", BCP 100, RFC 4020, February
          2005.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure
          Certificate Request Message Format (CRMF)", RFC 4211,
          September 2005.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
          IANA Considerations Section in RFCs", BCP 26, RFC 5226, May
          2008.

[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.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk,
          "Elliptic Curve Cryptography Subject Public Key
          Information", RFC 5480, March 2009.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic
          Curve Cryptography Algorithms", RFC 6090, February 2011.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for
          Use in the Resource Public Key Infrastructure (RPKI)",
          RFC 6485, February 2012.

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

[SHS] National Institute of Standards and Technology (NIST), "FIPS
          Publication 180-3: Secure Hash Standard", FIPS Publication
          180-3, October 2008.

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

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

11.1. Informative References

          None.

Authors' Addresses

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

    EMail: turners@ieca.com