BGPsec Algorithms, Key Formats, & Signature Formats
draft-ietf-sidr-bgpsec-algs-12

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 (draft-ietf-sidr-rfc6485bis).

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."

Copyright Notice

Table of Contents

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.sidr-bgpsec-pki-profiles] and CRLs
   [RFC6487]. BGPsec routers use these when requesting BGPsec
   certificates [ID.sidr-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.sidr-
   bgpsec-protocol] and the profile for BGPsec Router Certificates and
   Certification Requests [ID.sidr-bgpsec-pki-profiles]. Familiarity
   with these documents is assumed. Implementers are reminded, however,
   that, as noted in Section 2 of [ID.sidr-bgpsec-pki-profiles], the
   algorithms used to sign CA Certificates, BGPsec Router Certificates,
   and CRLs are found in [ID.sidr-rfc6485bis].

   This document updates [ID.sidr-rfc6485bis] 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.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

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 [ID.sidr-rfc6485bis].

   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 [ID.sidr-rfc6485bis].

   o The hashing algorithm used 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 [RFC6487].

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
     [ID.sidr-rfc6485bis].

   o In certification request, an OID is used. 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].

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
[ID.sidr-rfc6485bis]. 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 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].

  o 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 [ID.sidr-rfc6485bis]. 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 are not specified in this
   document, see Section 6 in [ID.sidr-bgpsec-protocol] for more
   information.

6. Security Considerations

   The Security Considerations of [RFC3279], [RFC5480], [RFC6090],
   [ID.sidr-rfc6485bis], and [ID.sidr-bgpsec-pki-profiles] apply to
   certificates. The security considerations of [RFC3279], [RFC6090],
   [ID.sidr-rfc6485bis], [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" 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   Signature   Algorithm   Specification
      Algorithm   Algorithm   Suite   Pointer
                                   Identifier

     +---+
     | Reserved | Reserved | 0x0 | This draft |
     +---+
     | SHA-256 | ECDSA P-256 | TBD | RFC 5480 |
     +---+

```
        | Unassigned | Unassigned  | TBD..0xF   | This draft   |
        +-----------------------------------------------------+
        | Reserved   | Reserved    | 0xF        | This draft   |
        +-----------------------------------------------------+
```

Future assignments are to be made using either the Standards Action
process defined in [RFC5226], or the Early IANA Allocation process
defined in [RFC7120]. Assignments consist of a digest algorithm
name, signature algorithm name, and the algorithm suite identifier
value.

8. Acknowledgements

The author wishes to thank Geoff Huston for producing [ID.sidr-
rfc6485bis], which this document is heavily based on. I'd also like
to thank Roque Gagliano, David Mandelberg, and Sam Weiller for their
review 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, 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.

[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.

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

[RFC7120] Cotton, M., "Early IANA Allocation of Standards Track Code
           Points", BCP 100, RFC 7120, January 2014.

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

[ID.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, work-in-
           progress.

[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.

## 9.2.  Informative References

   None.

Authors' Addresses

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

   EMail: turners@ieca.com