Stream: Independent Submission
RFC: 9558
Category: Informational
Published: April 2024
ISSN: 2070-1721
Authors: B. Makarenko
The Technical center of Internet, LLC
V. Dolmatov, Ed.
JSC "NPK Kryptonite"

RFC 9558
Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC

Abstract

This document describes how to produce digital signatures and hash functions using the GOST R 34.10-2012 and GOST R 34.11-2012 algorithms for DNSKEY, RRSIG, and DS resource records, for use in the Domain Name System Security Extensions (DNSSEC).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9558.

Copyright Notice

Table of Contents

1. Introduction

The Domain Name System (DNS) is the global, hierarchically distributed database for Internet Naming. The DNS has been extended to use cryptographic keys and digital signatures for the verification of the authenticity and integrity of its data. RFC 4033 [RFC4033], RFC 4034 [RFC4034], and RFC 4035 [RFC4035] describe these DNS Security Extensions, called DNSSEC.

RFC 4034 describes how to store DNSKEY and RRSIG resource records and specifies a list of cryptographic algorithms to use. This document extends that list with the signature and hash algorithms GOST R 34.10-2012 ([RFC7091]) and GOST R 34.11-2012 ([RFC6986]), and it specifies how to store DNSKEY data and how to produce RRSIG resource records with these algorithms.

GOST R 34.10-2012 and GOST R 34.11-2012 are Russian national standards. Their cryptographic properties haven't been independently verified.

Familiarity with DNSSEC and with GOST signature and hash algorithms is assumed in this document.

Caution:

This specification is not a standard and does not have IETF community consensus. It makes use of a cryptographic algorithm that is a national standard for Russia. Neither the IETF nor the IRTF has analyzed that algorithm for suitability for any given application, and it may contain either intended or unintended weaknesses.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. DNSKEY Resource Records

The format of the DNSKEY RR can be found in RFC 4034 [RFC4034].

GOST R 34.10-2012 public keys are stored with the algorithm number 23.

According to RFC 7091 [RFC7091], a GOST R 34.10-2012 public key is a point on the elliptic curve Q = (x, y). The wire representation of a public key **MUST** contain 64 octets, where the first 32 octets contain the little-endian representation of x and the second 32 octets contain the little-endian representation of y.

As RFC 6986 and RFC 7091 allow two variants of the length of the output hash and the signature and many variants of parameters of the digital signature, for the purpose of this document we use the 256-bit variant of the digital signature algorithm, corresponding with the 256-bit variant of the digest algorithm. We select the parameters for the digital signature algorithm to be id-tc26-gost-3410-2012-256-paramSetA as specified in RFC 7836 [RFC7836]; this document refers to it as "parameter set A".

2.1. Using a Public Key with Existing Cryptographic Libraries

At the time of this writing, existing GOST-aware cryptographic libraries are capable of reading GOST R 34.10-2012 public keys via a generic X.509 API if the key is encoded according to RFC 9215 [RFC9215], Section 4.

To make this encoding from the wire format of a GOST R 34.10-2012 public key with the parameters used in this document, prepend the 64 octets of key data with the following 30-byte sequence:

```
0x30 0x5c 0x30 0x17 0x06 0x08 0x2a 0x85
0x03 0x07 0x01 0x01 0x01 0x01 0x30 0x0b
0x06 0x09 0x2a 0x85 0x03 0x07 0x01 0x02
0x01 0x01 0x01 0x03 0x41 0x00
```

These bytes provide the following ASN.1 structure suitable for parsing by cryptographic toolkits:

```
  0  92: SEQUENCE {
  2  23:   SEQUENCE {
  4   8:     OBJECT IDENTIFIER '1 2 643 7 1 1 1 1'
 14  11:     SEQUENCE {
 16   9:       OBJECT IDENTIFIER '1 2 643 7 1 2 1 1 1'
        :       }
        :     }
 27  65:   BIT STRING
```

The OIDs in the structure above represent a GOST R 34.10-2012 public key with a 256-bit private key length and parameter set A. The structure itself represents SubjectPublicKeyInfo field of an X.509 certificate as defined in RFC 5280 [RFC5280], Section 4.1

2.2. GOST DNSKEY RR Example

Given a private key with the following value:

```
Private-key-format: v1.2
Algorithm: 23 (ECC-GOST12)
Gost12Asn1: MD4CAQAwFwYIKoUDBwEBAQEwCwYJKoUDBwECAQEBBCD/Mw9o6R5lQHJ13
            jz0W+C1tdsS4W7RJn04rk9MGJq3Hg==
```

The following DNSKEY RR stores a DNS zone key for example:

```
example.  600  IN  DNSKEY  256 3 23 (
            XGiiHlKUJd5fSeAK5O3L4tUNCPxs4pGqum6wKbqjdkqu
            IQ8nOXrilXZ9HcY8b2AETkWrtWHfwvJD4twPPJFQSA==
    ) ;{id = 47355 (zsk), size = 512b}
```

The private key here is presented in PrivateKeyInfo ASN.1 structure, as described in RFC 5958 [RFC5958], Section 2.

The public key can be calculated from the private key using algorithm described in RFC 7091 [RFC7091].

3. RRSIG Resource Records

The value of the signature field in the RRSIG RR follows RFC 7091 [RFC7091] and is calculated as follows. The values for the RDATA fields that precede the signature data are specified in RFC 4034 [RFC4034].

```
hash = GOSTR3411-2012(data)
```

where "data" is the wire format data of the resource record set that is signed, as specified in RFC 4034 [RFC4034].

The signature is calculated from the hash according to GOST R 34.10-2012, and its wire format is compatible with RFC 7091 [RFC7091].

3.1. RRSIG RR Example

Consider a given RRset consisting of one MX RR to be signed with the private key described in Section 2.2 of this document:

```
example.  600  IN  MX  10 mail.example.
```

Setting the inception date to 2022-10-06 12:32:30 UTC and the expiration date to 2022-11-03 12:32:30 UTC, the following signature RR will be valid:

```
example.  600 IN  RRSIG MX 23 1 600 20221103123230 (
                      20221006123230 47355 example.
                      EuLO0Qpn6zT1pzj9T2H5AWjcgzfmjNiK/vj811bExa0V
                      HMOVD9ma8rpf0B+D+V4Q0CWu1Ayzu+H/SyndnOWGxw==
)
```

The GOST R 34.10-2012 signature algorithm uses random (pseudorandom) integer k as described in Section 6.1 of RFC 7091 [RFC7091]. The following value for k was used to produce the signature example.

```
k = 8BBD0CE7CAF3FC1C2503DF30D13ED5DB75EEC44060FA22FB7E29628407C1E34
```

This value for k **MUST NOT** be used when computing GOST R 34.10-2012 signatures. It is provided only so the above signature example can be reproduced. The actual signature value will differ between signature calculations.

4. DS Resource Records

The GOST R 34.11-2012 digest algorithm is denoted in DS RRs by the digest type 5. The wire format of a digest value is compatible with RFC 6986 [RFC6986].

4.1. DS RR Example

For Key Signing Key (KSK):

```
example.  IN  DNSKEY  257 3 23 (
                       p8Req8DLJOfPymO5vExuK4gCcihF5N1YL7veCJ47av+w
                       h/qs9yJpD064k02rYUHfWnr7IjvJlbn3Z0sTZe9GRQ==
                       ) ;{id = 29468 (ksk), size = 512b}
```

The DS RR will be:

```
example.  IN  DS  29468 23 5 (
                      6033725b0ccfc05d1e9d844d49c6cf89
                      0b13d5eac9439189947d5db6c8d1c1ec
                      )
```

5. Operational Considerations

5.1. Key Sizes

The key size of GOST R 34.10-2012 public keys conforming to this specification **MUST** be 512 bits according to RFC 7091 [RFC7091].

5.2. Signature Sizes

The size of a GOST R 34.10-2012 signature conforming to this specification **MUST** be 512 bits according to RFC 7091 [RFC7091].

5.3. Digest Sizes

The size of a GOST R 34.11-2012 digest conforming to this specification **MUST** be 256 bits according to RFC 6986 [RFC6986].

6. Implementation Considerations

The support of this cryptographic suite in DNSSEC-aware systems is **OPTIONAL**. According to RFC 6840 [RFC6840], Section 5.2, systems that do not support these algorithms **MUST** ignore the RRSIG, DNSKEY, and DS resource records associated with the GOST R 34.10-2012 digital signature algorithm.

7. IANA Considerations

The following entry has been added to the IANA registry for "DNS Security Algorithm Numbers":

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Reference
23	GOST R 34.10-2012	ECC-GOST12	Y	*	RFC 9558

Table 1

The following entry has been added to the IANA registry for "Digest Algorithms" in the "Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms" registry group:

Value	Description	Status	Reference
5	GOST R 34.11-2012	OPTIONAL	RFC 9558

Table 2

8. Security Considerations

It is recommended to use a dual KSK algorithm signed zone until GOST-aware DNSSEC software becomes more widespread, unless GOST-only cryptography is to be used. Otherwise, GOST-signed zones may be considered unsigned by the DNSSEC software currently in use.

Like all algorithms, it is possible that a significant flaw could be discovered with GOST R 34.11-2012. In that case, deployments should roll over to another algorithm. See RFC 7583 [RFC7583] on the timing of such changes.

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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3110] Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, DOI 10.17487/RFC3110, May 2001, <https://www.rfc-editor.org/info/rfc3110>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, DOI 10.17487/RFC6840, February 2013, <https://www.rfc-editor.org/info/rfc6840>.

[RFC6986] Dolmatov, V., Ed. and A. Degtyarev, "GOST R 34.11-2012: Hash Function", RFC 6986, DOI 10.17487/RFC6986, August 2013, <https://www.rfc-editor.org/info/rfc6986>.

[RFC7091] Dolmatov, V., Ed. and A. Degtyarev, "GOST R 34.10-2012: Digital Signature Algorithm", RFC 7091, DOI 10.17487/RFC7091, December 2013, <https://www.rfc-editor.org/info/rfc7091>.

[RFC7583] Morris, S., Ihren, J., Dickinson, J., and W. Mekking, "DNSSEC Key Rollover Timing Considerations", RFC 7583, DOI 10.17487/RFC7583, October 2015, <https://www.rfc-editor.org/info/rfc7583>.

[RFC7836] Smyshlyaev, S., Ed., Alekseev, E., Oshkin, I., Popov, V., Leontiev, S., Podobaev, V., and D. Belyavsky, "Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012", RFC 7836, DOI 10.17487/RFC7836, March 2016, <https://www.rfc-editor.org/info/rfc7836>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, DOI 10.17487/RFC4509, May 2006, <https://www.rfc-editor.org/info/rfc4509>.

[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, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5933] Dolmatov, V., Ed., Chuprina, A., and I. Ustinov, "Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC", RFC 5933, DOI 10.17487/RFC5933, July 2010, <https://www.rfc-editor.org/info/rfc5933>.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <https://www.rfc-editor.org/info/rfc5958>.

[RFC9215] Baryshkov, D., Ed., Nikolaev, V., and A. Chelpanov, "Using GOST R 34.10-2012 and GOST R 34.11-2012 Algorithms with the Internet X.509 Public Key Infrastructure", RFC 9215, DOI 10.17487/RFC9215, March 2022, <https://www.rfc-editor.org/info/rfc9215>.

Acknowledgments

This document is a minor extension to RFC 4034 [RFC4034]. Also, we tried to follow the documents RFC 3110 [RFC3110], RFC 4509 [RFC4509], and RFC 5933 [RFC5933] for consistency. The authors of and contributors to these documents are gratefully acknowledged for their hard work.

The following people provided additional feedback, text, and valuable assistance: Alexander Venedyukhin, Michael StJohns, Valery Smyslov, Tim Wicinski, and Stéphane Bortzmeyer.

Authors' Addresses

Boris Makarenko
The Technical center of Internet, LLC
8 marta St., 1, Bldg. 12
Moscow
127083
Russian Federation
Email: bmakarenko@tcinet.ru

Vasily Dolmatov (EDITOR)
JSC "NPK Kryptonite"
Spartakovskaya Sq., 14, Bldg. 2
Moscow
105082
Russian Federation
Email: vdolmatov@gmail.com