Network Working Group
Internet-Draft
Expires: July 18, 2020

D. Belyavskiy
TCINET
V. Dolmatov, Ed.
JSC "NPK Kryptonite"
January 15, 2020

Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
draft-belyavskiy-rfc5933-bis-00

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 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 https://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."

This Internet-Draft will expire on July 18, 2020.

Copyright Notice

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The Domain Name System (DNS) is the global hierarchical 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 ([GOST3410], [RFC7091]) and GOST R 34.11-6986 ([GOST3411], [RFC6986]), and specifies how to store DNSKEY data and

how to produce RRSIG resource records with these algorithms.

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

1.1. Terminology

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 [RFC2119].

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 TBA1.

The wire format of the public key is compatible with RFC 7091 [RFC7091]:

According to [GOST3410] and [RFC7091], a 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 GOST3410 and GOST3411 allows 2 variants of length of the output hash and signature and many variants of parameters of the digital signature, for the purpose of this document we use 256-bit variant of the digital signature algorithm, corresponding 256-bit variant of the digest algorithm. We also select the only parameters for the digital signature algorithm, specified as id-tc26-gost-3410-2012-256-paramSetA in RFC 7836 [RFC7836].

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 public keys via a generic X509 API if the key is encoded according to RFC 4491 [RFC7091],

Section 2.3.2.

To make this encoding from the wire format of a GOST public key with the parameters used in this document, prepend the 64 octets of key data with the following 32-byte sequence:

```
0x30 0x5e 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 0x43 0x00 0x04 0x40
```


2.2. GOST DNSKEY RR Example

Given a private key with the following value (the value of the Gost12Asn1 field is split here into two lines to simplify reading; in the private key file, it must be in one line):

```
Private-key-format: v1.2
Algorithm: 23 (ECC-GOST12)
Gost12Asn1: MD4CAQAwFwYIKoUDBwEBAQEwCwYJKoUDBwECAQEBBCA0zvTDpCSjdRCERkd6
            WDA2TF/ABQLp9MPZRl7hMXCVGg==
```

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

```
example.        600     IN      DNSKEY  256 3 23 XkZ6T+qQ9teOMsA/YK+kTzE
    LhuMPTsYggdy2b+sfzJ6tH9eniziMX3gjMnUZIyrnSIchLjup8xpy+
                UU5l1Eyjw== ;{id = 13439 (zsk), size = 512b}
```

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 the GOST R 34.10-2012 standard, and its wire format is compatible with RFC 4490 [RFC7091].

3.1. RRSIG RR Example

With the private key from this document, consisting of one MX record:

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

Setting the inception date to 2020-01-04 17:25:26 UTC and the expiration date to 2020-02-01 17:25:26 UTC, the following signature RR will be valid:

```
example.  600 IN  RRSIG MX 23 1 600 20200201172526 (
                                    20200104172526 13439 example.  Etrs
                                    AEGsNRf12HKjwNTg8U2HZ5JOSo34UaTcsho
```



```
                                    E1kwd5Ror4I7zltmWAgd4b9OBn80tsajtL0
                                    Vuf45u8kEAgA==

)
```

Note: The ECC-GOST12 signature algorithm uses random data, so the actual computed 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 TBA2. The wire format of a digest value is compatible with RFC 6986 [RFC6986], that is, the digest is in little-endian representation.

4.1. DS RR Example

For Key Signing Key (KSK):

```
example.  IN DNSKEY 257 3 23 hP3ISWPT8ehEEut8ozbqPcmbTAQK0jce7MHmK
0geOiRokFALGwsMrBf0H0AK2qrVJCWCJL+50v9UNZAS5mE70g== ;{id = 7574
```

(ksk), size = 512b}

The DS RR will be

example. IN DS 7574 23 5
990f40dc548a4dbcb4b80a0760f194ac0cc18484578834c1ac1f749f70c84103

5. Deployment Considerations

5.1. Key Sizes

According to RFC 7091 [RFC7091] and the decision made about the used variant, the key size of GOST public keys MUST be 512 bits.

5.2. Signature Sizes

According to the GOST R 34.10-2012 digital signature algorithm specification ([GOST3410], [RFC7091]), the size of a GOST signature for the selected parameters is 512 bits.

5.3. Digest Sizes

According to GOST R 34.11-2012 ([GOST3411], [RFC6986]), the size of a GOST digest matching the selected parameters of the signature is 256 bits.

6. Implementation Considerations

6.1. Support for GOST Signatures

DNSSEC-aware implementations MAY be able to support RRSIG and DNSKEY resource records created with the GOST algorithms as defined in this document.

6.2. Support for NSEC3 Denial of Existence

Any DNSSEC-GOST implementation MUST support both NSEC [RFC4035] and NSEC3 [RFC5155].

7. Security Considerations

Currently, the cryptographic resistance of the GOST R 34.10-2012 digital signature algorithm is estimated as 2**128 operations of multiple elliptic curve point computations on prime modulus of order 2**256.

Currently, the cryptographic resistance of the GOST R 34.11-2012 hash algorithm is estimated as 2**128 operations of computations of a step hash function.

8. IANA Considerations

This document updates the IANA registry "DNS Security Algorithm Numbers" [RFC4034]. The following entries have been added to the registry:

Value	Algorithm	Mnemonic	Zone Signing	Trans. Sec.	References	Status
TBA1	GOST R 34.10-2012	ECC-GOST12	Y	*	RFC 6986	OPTIONAL

This document updates the RFC 4034 Digest Types assignment ([RFC4034], Section A.2) by adding the value and status for the GOST R 34.11-94 algorithm:

Value	Algorithm	Status
TBA2	GOST R 34.11-2012	OPTIONAL

This paragraph shoud be removed before the publication of RFC: For the purpose of example computations, the following values were used: TBA1 = 23, TBA2 = 5.

9. 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: TODO

10. References

10.1. 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>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[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>.

[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>.

10.2. 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>.

[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>.

Authors' Addresses

Dmitry Belyavskiy
TCINET
8 marta st
Moscow
Russian Federation

Phone: +7 916 262 5593
Email: beldmit@gmail.com

Vasily Dolmatov (editor)
JSC "NPK Kryptonite"
Spartakovskaya sq., 14, bld 2, JSC "NPK Kryptonite"
Moscow 105082
Russian Federation

Email: vdolmatov@gmail.com