DNS Extensions working group
Internet-Draft
Intended status: Standards Track
Expires: Febuary 05, 2010

V.Dolmatov, Ed.
Cryptocom Ltd.

August 05, 2009

Use of GOST signature algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
draft-dolmatov-dnsext-dnssec-gost-01

Status of this Memo

This Internet-Draft will expire on February 05 2010.

Copyright Notice

Abstract

This document describes how to produce GOST signature and hash algorithms DNSKEY and RRSIG resource records for use in the Domain Name System Security Extensions (DNSSEC, RFC 4033, RFC 4034, and RFC 4035).

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 [GOST3410, GOST3411], and specifies how to store DNSKEY data and how to produce RRSIG resource records with these hash algorithms.

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

The term "GOST" is not officially defined, but is usually used to refer to the collection of the Russian cryptographic algorithms GOST R 34.10-2001, GOST R 34.11-94, GOST 28147-89. Since GOST 28147-89 is not used in DNSSEC, GOST will only refer to GOST R 34.10-2001 (signatire algorithm) and GOST R 34.11-94 (hash algorithm) in this document.

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 34.10-2001 public keys are stored with the algorithm number {TBA1}.

The public key parameters are those identified by id-GostR3410-2001-CryptoPro-A-ParamSet (1.2.643.2.2.35.1) [RFC4357]. The digest parameters for signature are those identified by id-GostR3411-94-CryptoProParamSet (1.2.643.2.2.30.1) [RFC4357].

The wire format of the public key is compatible with RFC 4491 [RFC4491]:

According to [GOSTR341001], 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. This corresponds to the binary representation of (<y>256||<x>256) from [GOSTR341001], ch. 5.3.

2.1. Using a public key with existing cryptographic libraries

Existing GOST-aware cryptographic libraries at time of this document writing are capable to read GOST public keys via generic X509 API if the key is encoded according to RFC 4491 [RFC4491], section 2.3.2.

To make this encoding from the wire format of a GOST public key, prepend a key data with the following 37-byte sequence:

```
0x30 0x63 0x30 0x1c 0x06 0x06 0x2a 0x85 0x03 0x02 0x02 0x13 0x30 0x12
0x06 0x07 0x2a 0x85 0x03 0x02 0x02 0x23 0x01 0x06 0x07 0x2a 0x85 0x03
0x02 0x02 0x1e 0x01 0x03 0x43 0x00 0x04 0x40
```

2.2. GOST DNSKEY RR Example

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

```
example.com. 86400 IN DNSKEY 256 3 {TBA1} ( RamuUwTG1r4RUqsgXu/xF6B+Y
                                            tJLzZEykiZ4C2Fa1gV1pI/8GA
                                            el2Wm69Cz5h1T9eYAQKFAGwzW
                                            m4Lke0E26aw== )
```

3. RRSIG Resource Records

The value of the signature field in the RRSIG RR follows the RFC 4490 [RFC4490] and is calculated as follows. The values for the RDATA fields that precede the signature data are specified in RFC 4034 [RFC4034].

```
hash = GOSTR3411(data)
```

where "data" is the wire format data of the resource record set that is signed, as specified in RFC 4034 [RFC4034]. Hash MUST be calculated with GOST R 34.11-94 parameters identified by id-GostR3411-94-CryptoProParamSet [RFC4357].

Signature is calculated from the hash according to the GOST R 34.10-2001 standard and its wire format is compatible with RFC 4490 [RFC4490]. Quoting RFC 4490:

"The signature algorithm GOST R 34.10-2001 generates a digital signature in the form of two 256-bit numbers, r and s. Its octet string representation consists of 64 octets, where the first 32 octets contain the big-endian representation of s and the second 32 octets contain the big-endian representation of r."

4. DS Resource Records

GOST R 34.11-94 digest algorithm is denoted in DS RR by the digest type {TBA2}. The wire format of a digest value is compatible with RFC 4490 [RFC4490]. Quoting RFC 4490:

"A 32-byte digest in little-endian representation."

The digest MUST always be calculated with GOST R 34.11-94 parameters identified by id-GostR3411-94-CryptoProParamSet [RFC4357].

5. Deployment Considerations

5.1. Key Sizes

According to RFC4357 [RFC4357] key size of GOST public keys MUST be 512 bits.

5.2. Signature Sizes

According to GOST signature algorithm [GOST3410] size of GOST signature is 512 bit.

5.3. Digest Sizes

According to GOST R 34.11-94 [GOST3411] size of GOST digest is 256 bit.

6. Implementation Considerations

6.1. Support for GOST signatures

DNSSEC aware implementations SHOULD 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

NSEC3 support is not described in this document.

7. Security considerations

Current cryptographic resistance of GOST 34.10-2001 digital signature algorithm is estimated as 2**128 operations of elliptic curve point computations on simple modulus 2**256.
Current cryptographic resistance of GOST 34.11-94 hash algorithm is estimated as 2**128 operations of copmutations of step hash function. (There is known method to reduce this estimate to 2**105 operations, but it demands padding the colliding message with 1024 random bit blocks each of 256 bit length, thus it cannot be used in any practical implementation).

8. IANA Considerations

This document updates the IANA registry "DNS SECURITY ALGORITHM NUMBERS -- per [RFC4035] " (http://www.iana.org/assignments/dns-sec-alg-numbers). The following entries are added to the registry:

			Zone	Trans.		
Value	Algorithm	Mnemonic	Signing	Sec.	References	Status
{TBA1}	GOST R 34.10-2001	GOST	Y	*	(this memo)	OPTIONAL

This document updates the RFC 4034 [RFC4034] Digest Types assignment (RFC 4034, section A.2):

Value	Algorithm	Status
{TBA2}	GOST R 34.11-94	OPTIONAL

9. Acknowledgments

This document is a minor extension to RFC 4034 [RFC4034]. Also, we try to follow the documents RFC 3110 [RFC3110], RFC 4509 [RFC4509] and RFC 4357 [RFC4357] for consistency. The authors of and contributors to these documents are gratefully acknowledged for their hard work.

The following people provided additional feedback and text: Dmitry Burkov, Jaap Akkerhuis, Olafur Gundmundsson,Jelte Jansen and Wouter Wijngaards.

10. References

10.1. Normative References

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

[RFC3110] Eastlake D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, May 2001.

[RFC4033] Arends R., Austein R., Larson M., Massey D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends R., Austein R., Larson M., Massey D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends R., Austein R., Larson M., Massey D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[GOST3410] "Information technology. Cryptographic data security. Signature and verification processes of [electronic] digital signature.", GOST R 34.10-2001, Gosudarstvennyi Standard of Russian Federation, Government Committee of the Russia for Standards, 2001. (In Russian)

[GOST3411] "Information technology. Cryptographic Data Security. Hashing function.", GOST R 34.11-94, Gosudarstvennyi Standard of Russian Federation, Government Committee of the Russia for Standards, 1994. (In Russian)

[RFC4357] Popov V., Kurepkin I., and S. Leontiev, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94

Algorithms", RFC 4357, January 2006.

[RFC4490] S. Leontiev and G. Chudov, "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)", RFC 4490, May 2006.

[RFC4491] S. Leontiev and D. Shefanovski, "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 4491, May 2006.

10.2. Informative References

[NIST800-57]
Barker E., Barker W., Burr W., Polk W., and M. Smid, "Recommendations for Key Management", NIST SP 800-57, March 2007.

[RFC3447] Jonsson J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC4509] Hardaker W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

[DRAFT1] Dolmatov V., Kabelev D., Ustinov I., Vyshensky S., "GOST R 34.10-2001 digital signature algorithm" draft-dolmatov-cryptocom-gost3410-2001-02, work in progress

[DRAFT2] Dolmatov V., Kabelev D., Ustinov I., Vyshensky S., "GOST R 34.11-94 Hash function algorithm" draft-dolmatov-cryptocom-gost341194-01, work in progress

[DRAFT3] Dolmatov V., Kabelev D., Ustinov I., Emelyanova I., "GOST 28147-89 encryption, decryption and MAC algorithms" draft-dolmatov-cryptocom-gost2814789-01, work in progress

Authors' Addresses

Vasily Dolmatov, Ed.
Cryptocom Ltd.
Bolotnikovskaya, 23
Moscow, 117303, Russian Federation

EMail: dol@cryptocom.ru

Artem Chuprina
Cryptocom Ltd.
Bolotnikovskaya, 23
Moscow, 117303, Russian Federation

EMail: ran@cryptocom.ru

Igor Ustinov
Cryptocom Ltd.
Bolotnikovskaya, 23
Moscow, 117303, Russian Federation

EMail: igus@cryptocom.ru