Network Working Group   V. Smyslov
Internet-Draft   ELVIS-PLUS
Intended status: Informational   February 28, 2020
Expires: August 31, 2020

                     Using GOST algorithms in IKEv2
                       draft-smyslov-ike2-gost-03

Abstract

   This document defines a set of cryptographic transforms for use in
   the Internet Key Exchange version 2 (IKEv2) protocol. The transforms
   are based on Russian cryptographic standard algorithms (GOST).

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 August 31, 2020.

Copyright Notice

Table of Contents

1. Introduction

   This document defines a number of transforms for the Internet Key
   Exchange version 2 (IKEv2) [RFC7296]. These transforms are based on
   Russian cryptographic standard algorithms (often called "GOST"
   algorithms) for hash function, digital signature and key exchange
   method. Along with transforms defined in [I-D.smyslov-esp-gost], the
   transforms defined in this specification allow using GOST
   cryptographic algorithms in IPsec protocols.

2. Terminology and Notation

   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.

3. Overview

   Russian cryptographic standard (GOST) algorithms are a set of
   cryptographic algorithms of different types - ciphers, hash
   functions, digital signatures etc. In particular, Russian
   cryptographic standard [GOST3412-2015] defines block ciphers
   "Kuznyechik" (also defined in [RFC7801]) and "Magma" (also defined in
   [I-D.dolmatov-magma]). Cryptographic standard [GOST3410-2012]
   defines elliptic curve digital signature algorithm (also defined in

[RFC7091]), while [GOST3411-2012] defines two cryptographic hash
functions "Stribog", with different output length (also defined in
[RFC6986]). The parameters for the elliptic curves used in GOST
signature and key exchange algorithms are defined in [RFC7836].

4. IKE SA Protection

Specification [I-D.smyslov-esp-gost] defines two transforms of type 1
(Encryption Algorithm Transform IDs) based on GOST block ciphers that
may be used for IKE SA protection: ENCR_KUZNYECHIK_MGM_KTREE (32)
based on "Kuznyechik" block cipher and ENCR_MAGMA_MGM_KTREE (33)
based on "Magma" block cipher. Since they are AEAD transforms and
provide both encryption and authentication, there is no need for new
transform type 3 (Integrity Algorithm Transform IDs), because it must
not be used with these transforms (or must have a value NONE).

5. Pseudo Random Function

This specification defines a new transform of type 2 (Pseudorandom
Function Transform IDs) - PRF_HMAC_STRIBOG_512 (<TBA by IANA>). This
transform uses PRF HMAC_GOSTR3411_2012_512 defined in Section 4.1.2
of [RFC7836]. The PRF uses GOST R 34.11-2012 ("Stribog") hash-
function with 512-bit output defined in [RFC6986][GOST3411-2012] with
HMAC [RFC2104] construction. The PRF has a 512-bit block size and a
512-bit output length.

6. Shared Key Calculation

This specification defines two new transforms of type 4 (Diffie-
Hellman Group Transform IDs): GOST3410_2012_256 (<TBA by IANA>) and
GOST3410_2012_512 (<TBA by IANA>). These transforms uses Elliptic
Curve Diffie-Hellman (ECDH) key exchange algorithm over Twisted
Edwards curves. The parameters for these curves are defined in
Section A.2 of [RFC7836]. In particular, transform GOST3410_2012_256
uses id-tc26-gost-3410-2012-256-paramSetA parameter set and
GOST3410_2012_512 uses id-tc26-gost-3410-2012-512-paramSetC parameter
set (both defined in [RFC7836]).

Shared secret is computed as follows. The initiator randomly selects
its private key d_i from $\{1,..,q - 1\}$, where q is the group order and
is a parameter of the selected curve. Then a public key Q_i is
computed as a point on the curve: $Q_i = d_i * G$, where G is the
generator for the selected curve, and then is sent to the responder.
The responder makes the same calculations to get d_r and Q_r and
sends Q_r to the initiator. After peers exchange Q_i and Q_R both
sides can compute a point on the curve $S = ((m / q) * d_i) * Q_r =
((m / q) * d_r) * Q_i$, where m is the subgroup order and is a
parameter of the selected curve. The shared secret K is an x

   coordinate of S in a little-endian representation. The size of K is
   determined by the size of used curve and is either 256 or 512 bit.

   When GOST public key is transmitted in the KE payload, it MUST be
   represented as x coordinate immediately followed by y coordinate,
   each in a little-endian representation. The size of each coordinate
   is determined by the size of the used curve and is either 256 or 512
   bits, so that the size of the Key Exchange Data field in the KE
   payload is either 64 or 128 octets.

6.1. Recipient Tests

   Upon receiving peer's public key implementations MUST check that the
   key is actually a point on the curve, otherwise the exchange fails.
   Implementations MUST check that the calculated public value S is not
   an identity element of the curve, in which case the exchange fails.

7. Authentication

   GOST digital signatures algorithm GOST R 34.10-2012 is defined in
   [RFC7091][GOST3410-2012]. There are two variants of GOST signature
   algorithm - one over 256-bit elliptic curve and the other over
   512-bit key elliptic curve.

   When GOST digital signature is used in IKEv2 for authentication
   purposes, an Authentication Method "Digital Signature" (14) MUST be
   specified in the AUTH payload. The AlgorithmIdentifier ASN.1 objects
   for GOST digital signature algorithm are defined in Section 7.2.

   The signature value, as defined in [RFC7091][GOST3410-2012], consists
   of two integers r and s. The size of each integer is either 256 bit
   or 512 bit depending on the used elliptic curve. The content of the
   Signature Value field in the AUTH payload MUST consist of s
   immediately followed by r, each in a big-endian representation, so
   that the size of the field is either 64 or 128 octets.

7.1. Hash Functions

   GOST digital signatures algorithm uses GOST hash functions GOST R
   34.11-2012 ("Stribog") defined in [RFC6986][GOST3411-2012]. There
   are two "Stribog" hash functions - one with 256-bit output length and
   the other with 512-bit output length.

   This specification defines two new values for IKEv2 Hash Algorithms
   registry: STRIBOG_256 (<TBA by IANA>) for GOST hash function with
   256-bit output length and STRIBOG_512 (<TBA by IANA>) for the 512-bit
   length output. These values MUST be included in the

SIGNATURE_HASH_ALGORITHMS notify if a corresponding GOST digital
signature algorithm is supported by the sender.

7.2. ASN.1 Objects

This section lists GOST signature algorithm ASN.1 objects in binary
form.

7.2.1. id-tc26-signwithdigest-gost3410-12-256

id-tc26-signwithdigest-gost3410-12-256 OBJECT IDENTIFIER ::= { iso(1)
member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1)
signwithdigest(3) gost3410-12-256(2) }

Parameters are absent.

Name = id-tc26-signwithdigest-gost3410-12-256
OID = 1.2.643.7.1.1.3.2
Length = 12
0000: 300a 0608 2a85 0307 0101 0302

7.2.2. id-tc26-signwithdigest-gost3410-12-512

id-tc26-signwithdigest-gost3410-12-512 OBJECT IDENTIFIER ::= { iso(1)
member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1)
signwithdigest(3) gost3410-12-512(3) }

Parameters are absent.

Name = id-tc26-signwithdigest-gost3410-12-256
OID = 1.2.643.7.1.1.3.3
Length = 12
0000: 300a 0608 2a85 0307 0101 0303

8. Security Considerations

The security considerations of [RFC7296] apply accordingly.

The security of GOST elliptic curves is discussed in
[GOST-EC-SECURITY]. The security of "Stribog" hash function is
discussed in [STRIBOG-SECURITY]. A second preimage attack on
"Stribog" is described in [STRIBOG-PREIMAGE] if message size exceeds
2^259 blocks. This attack is not relevant to how "Stribog" is used
in IKEv2.

9. IANA Considerations

   IANA has assigned one Transform ID in the "Transform Type 2 -
   Pseudorandom Function Transform IDs" registry (where RFCXXXX is this
   document):

   Number   Name   Reference
   ----
   9   PRF_HMAC_STRIBOG_512   [RFCXXXX]

   IANA has assigned two Transform IDs in the "Transform Type 4 -
   Diffie-Hellman Group Transform IDs" registry (where RFCXXXX is this
   document):

   Number   Name   Recipient Tests   Reference
   ----
   33   GOST3410_2012_256   [RFCXXXX] Sec. 6.1   [RFCXXXX]
   34   GOST3410_2012_512   [RFCXXXX] Sec. 6.1   [RFCXXXX]

   IANA has assigned two values in the "IKEv2 Hash Algorithms" registry
   (where RFCXXXX is this document):

   Number   Hash Algorithm   Reference
   ----
   6   STRIBOG_256   [RFCXXXX]
   7   STRIBOG_512   [RFCXXXX]

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>.

   [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>.

   [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>.

   [RFC7296]   Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.
               Kivinen, "Internet Key Exchange Protocol Version 2
               (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October
               2014, <https://www.rfc-editor.org/info/rfc7296>.

   [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>.

   [I-D.smyslov-esp-gost]
               Smyslov, V., "Using GOST ciphers in ESP and IKEv2", draft-
               smyslov-esp-gost-02 (work in progress), October 2019.

10.2. Informative References

   [RFC2104]   Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-
               Hashing for Message Authentication", RFC 2104,
               DOI 10.17487/RFC2104, February 1997,
               <https://www.rfc-editor.org/info/rfc2104>.

   [RFC7801]   Dolmatov, V., Ed., "GOST R 34.12-2015: Block Cipher
               "Kuznyechik"", RFC 7801, DOI 10.17487/RFC7801, March 2016,
               <https://www.rfc-editor.org/info/rfc7801>.

   [I-D.dolmatov-magma]
               Dolmatov, V. and D. Eremin-Solenikov, "GOST R 34.12-2015:
               Block Cipher "Magma"", draft-dolmatov-magma-05 (work in
               progress), November 2019.

   [GOST3410-2012]
               Federal Agency on Technical Regulating and Metrology,
               "Information technology. Cryptographic data security.
               Signature and verification processes of [electronic]
               digital signature", GOST R 34.10-2012, 2012.

               (In Russian)

   [GOST3411-2012]
               Federal Agency on Technical Regulating and Metrology,
               "Information technology. Cryptographic data security.
               Hashing function", GOST R 34.11-2012, 2012.

               (In Russian)

   [GOST3412-2015]
             Federal Agency on Technical Regulating and Metrology,
             "Information technology. Cryptographic data security.
             Block ciphers", GOST R 34.12-2015, 2015.

             (In Russian)

   [GOST-EC-SECURITY]
             Alekseev, E., Nikolaev, V., and S. Smyshlyaev, "On the
             security properties of Russian standardized elliptic
             curves", https://doi.org/10.4213/mvk260, 2018.

   [STRIBOG-SECURITY]
             Wang, Z., Yu, H., and X. Wang, "Cryptanalysis of GOST R
             hash function",
              https://doi.org/10.1016/j.ipl.2014.07.007, 2014.

   [STRIBOG-PREIMAGE]
             Guo, J., Jean, J., Leurent, G., Peyrin, T., and L. Wang,
             "The Usage of Counter Revisited: Second-Preimage Attack on
             New Russian Standardized Hash Function",
              https://eprint.iacr.org/2014/675, 2014.

Author's Address

   Valery Smyslov
   ELVIS-PLUS
   PO Box 81
   Moscow (Zelenograd) 124460
   RU

   Phone: +7 495 276 0211
   Email: svan@elvis.ru