Using GOST Cryptographic Algorithms in the Internet Key Exchange
Protocol Version 2 (IKEv2)
draft-smyslov-ike2-gost-08

Abstract

This document defines a set of cryptographic transforms for use in
the Internet Key Exchange protocol version 2 (IKEv2). The transforms
are based on Russian cryptographic standard algorithms (GOST). Using
GOST ciphers in IKEv2 was defined in RFC 9227, this document aims to
define using GOST algorithms for the rest of cryptographic transforms
used in IKEv2.

This specification was developed to facilitate implementations that
wish to support the GOST algorithms. This document does not imply
IETF endorsement of the cryptographic algorithms used in this
document.

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 5 November 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the
document authors. All rights reserved.
1. Introduction

The Internet Key Exchange protocol version 2 (IKEv2) defined in [RFC7296] is an important part of the IP Security (IPsec) architecture. It is used for the authenticated key exchange and for the negotiation of various protocol parameters and features.

This document defines a number of transforms for IKEv2, based on Russian cryptographic standard algorithms (often referred to as "GOST" algorithms) for hash function, digital signature and key exchange method. These definitions are based on the recommendations [GOST-IKEv2] established by the Standardisation Technical Committee "Cryptographic information protection", which describe how Russian
cryptographic standard algorithms are used in IKEv2. Along with the transforms defined in [RFC9227], the transforms defined in this specification allow using GOST cryptographic algorithms in IPsec protocols.

This specification was developed to facilitate implementations that wish to support the GOST algorithms. This document does not imply IETF endorsement of the cryptographic algorithms used in this document.

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 [RFC8891]). Cryptographic standard [GOST3410-2012] defines elliptic curve digital signature algorithm (also defined in [RFC7091]), while [GOST3411-2012] defines two cryptographic hash functions "Streebog", 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

[RFC9227] defines two transforms of type 1 (Encryption Algorithm Transform IDs) based on GOST block ciphers that can 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 these transforms use ciphers in Multilinear Galois Mode (MGM), which provides Authenticated Encryption with Associated Data (AEAD) and thus provide both encryption and authentication,
there is no need for new transform type 3 (Integrity Algorithm Transform IDs) for use in IKEv2, because integrity transforms cannot be used with encryption transforms providing AEAD (see Section 3.3 of [RFC7296]).

5. Pseudo Random Function

This specification defines a new transform of type 2 (Pseudorandom Function Transform IDs) - PRF_HMAC_STREEBOG_512 (9). This transform uses PRF HMAC_GOSTR3411_2012_512 defined in Section 4.1.2 of [RFC7836]. The PRF uses GOST R 34.11-2012 ("Streebog") 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 (33) and GOST3410_2012_512 (34). 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 $\{1, \ldots, q - 1\}$, 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: $Q_i = d_i \ast G$, 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. The INVALID_SYNTAX notification MAY be sent in these cases.

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 ("Streebog") defined in [RFC6986][GOST3411-2012]. There are two "Streebog" 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: STREEBOG_256 (6) for GOST hash function with 256-bit output length and STREEBOG_512 (7) 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 AlgorithmIdentifier objects in binary form. This objects are defined in [RFC9215][USING-GOST-IN-CERTS] and are provided here for convenience.
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-gost3410-12-512
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 "Streebog" hash function is
discussed in [STREEBOG-SECURITY]. A second preimage attack on
"Streebog" is described in [STREEBOG-PREIMAGE] if message size
exceeds 2^259 blocks. This attack is not relevant to how "Streebog"
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):

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>PRF_HMAC_STREEBOG_512</td>
<td>[RFCXXXX]</td>
</tr>
</tbody>
</table>

IANA has assigned two Transform IDs in the "Transform Type 4 -
Diffie-Hellman Group Transform IDs" registry (where RFCXXXX is this
document):
IANA has assigned two values in the "IKEv2 Hash Algorithms" registry (where RFCXXXX is this document):

<table>
<thead>
<tr>
<th>Number</th>
<th>Hash Algorithm</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>STREEBOG_256</td>
<td>[RFCXXXX]</td>
</tr>
<tr>
<td>7</td>
<td>STREEBOG_512</td>
<td>[RFCXXXX]</td>
</tr>
</tbody>
</table>

10. References

10.1. Normative References


Smyslov Expires 5 November 2022

Internet-Draft GOST algorithms in IKEv2 May 2022


10.2. Informative References


[GOST3412-2015]

[GOST-IKEv2]

[USING-GOST-IN-CERTS]

[GOST-EC-SECURITY]

[STREEBOG-SECURITY]

[STREEBOG-PREIMAGE]

Author's Address
Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd)
124460
Russian Federation
Phone: +7 495 276 0211
Email: svan@elvis.ru