TLS Working Group   Grigorij Chudov, CRYPTO-PRO
INTERNET-DRAFT   Serguei Leontiev, CRYPTO-PRO
Expires December 15, 2003   June 15, 2003
Intended Category: Informational

Addition of GOST Ciphersuites to Transport Layer Security (TLS)

<draft-chudov-cryptopro-cptls-00.txt>

Status of this Memo

Abstract

This document is intended to register new cipher suites for the Transport Layer Security (TLS) protocol, according to the procedure specified in section A.5 of [TLS]. Those cipher suites are based on Russian national cryptographic standards - key establishment algorithms based on GOST R 3410-94 and GOST R 3410-2001 public keys, GOST 28147-89 encryption algorithm and GOST R 34.11-94 digest algorithm.

Table of Contents

1 Introduction

This document only describes algorithm identifiers, data formats and protocol messages used in TLS (Transport Layer Security) protocol cipher suites, based on GOST R 34.10-94/2001 key exchange, GOST R 34.11-94 hash and GOST 28147-89 encryption algorithms. It does not describe those cryptographic algorithms. The cipher suites defined here were proposed by CRYPTO-PRO Company for "Russian Cryptographic Software Compatibility Agreement" community.

Algorithms GOST R 34.10-94, GOST R 34.10-2001, GOST 28147-89 and GOST R 34.11-94 have been developed by Russian Federal Agency of Governmental Communication and Information (FAGCI) and "All-Russian Scientific and Research Institute of Standardization". They are described in [GOSTR341094], [GOSTR34102001], [GOSTR3411] and [GOST28147]. GOST-based key agreement algorithm and PRF are described in [CPALGS].

This document defines two configurations:
anonymous client - authenticated server (only server provides a certificate);
authenticated client - authenticated server (client and server exchange certificates).

The presentation language used here is the same as in [TLS]. Since this specification extends TLS, these descriptions should be merged with those in the TLS specification and any others that extend TLS. This means, that enum types may not specify all possible values and structures with multiple formats chosen with a select() clause may not indicate all possible cases.

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 [RFC 2119].

2 Proposed CipherSuites

The new cipher suites proposed here have the following definitions:

```
CipherSuite TLS_GOST341094_WITH_GOST28147_CFB_GOST3411   = {0x00,0x80}
CipherSuite TLS_GOST34102001_WITH_GOST28147_CFB_GOST3411 = {0x00,0x81}
CipherSuite TLS_GOST341094_WITH_NULL_GOSTR3411           = {0x00,0x82}
CipherSuite TLS_GOST34102001_WITH_NULL_GOSTR3411         = {0x00,0x83}
```

Note: The above numeric definitions for CipherSuites have not yet been registered.

3 CipherSuite Definitions

3.1 Key exchange

The cipher suites defined here use the following key exchange algorithms:

CipherSuite	Key Exchange Algorithm
TLS_GOST341094_WITH_GOST28147_CFB_GOST3411	GOST R 3410-94
TLS_GOST34102001_WITH_GOST28147_CFB_GOST3411	GOST R 3410-2001
TLS_GOST341094_WITH_NULL_GOSTR3411	GOST R 3410-94
TLS_GOST34102001_WITH_NULL_GOSTR3411	GOST R 3410-2001

Key establishment algorithms based on GOST R 3410-94 and GOST R 3410-2001 public keys are described in [CPALGS].

3.2 PRF, Signature and Hash

For a PRF, described in section 5 of [TLS], the cipher suites described here use GOSTR3411_PRF (refer to section 4.1)

GOST R 3410-94/2001 signature is used for CertificateVerify message.

GOST R 34.11 digest algorithm ([GOSTR341194]) is used for CertificateVerify.signature.gostR3411_hash and Finished.verify_data (see sections 7.4.8 and 7.4.9 of [TLS])

3.3 Cipher and MAC

The following cipher algorithm and MAC functions are used (for details refer to section 4.1):

CipherSuite	Cipher	MAC

TLS_GOST341094_WITH_GOST28147_CFB_GOST3411	GOST28147	GOST28147_IMIT
TLS_GOST34102001_WITH_GOST28147_CFB_GOST3411	GOST28147	GOST28147_IMIT
TLS_GOST341094_WITH_NULL_GOSTR3411	-	GOSTR3411_HMAC
TLS_GOST34102001_WITH_NULL_GOSTR3411	-	GOSTR3411_HMAC

4 Data Structures and Computations

4.1 Algorithms

GOST28147 is a stream cipher GOST 28147-89 [GOST28147] in CFB mode, it uses 256-bit key size and 8-byte IV. Algorithm parameters are taken from the server certificate.

GOST28147_IMIT is GOST 28147-89 [GOST28147] in "IMITOVSTAVKA" mode (4 bytes)

GOSTR3411_HMAC(secret, data) is based on GOST R 34.11 digest and described in [CPCMS].

GOSTR3411_PRF(secret, label, seed) is based on GOSTR3411_HMAC and described in [CPALGS].

4.2 Key Calculation

Key calculation is done according to section 6.3 of [TLS], with GOSTR3411_PRF function used instead of PRF. The parameters are as follows:

SecurityParameters.hash_size = 32
SecurityParameters.key_material_length = 32
SecurityParameters.IV_size = 8

Length of necessary key material is 144 bytes.

4.3 Server Certificate

For these cipher suites this message is required and it MUST contain a certificate, with a public key algorithm matching ServerHello.cipher_suite.

4.4 Server Key Exchange

This message MUST NOT be used in these cipher suites, because all the parameters necessary are present in server certificate (see [CPPK]).

4.5 Certificate Request

This message is used as described in section 7.4.4 of [TLS], and extended as follows:

```
 enum {
     gost341094(21), gost34102001(22),(255)
 } ClientCertificateType;
```

gost341094 and gost34102001 certificate types identify that the server accepts GOST R 34.10-94 and GOST R 34.10-2001 public key certificates.

4.6 Client Key Exchange Message

This message is required and it MUST contain client ephemeral public key if server didn't request client certificate or client has no certificate with matching algorithm and parameters.

The TLS ClientKeyExchange message is extended as follows:

```
 struct
 {
    G28147_ENCRYPTION_BLOB          keyBlob;
    STACK_OF(TLS1_PROXY_KEY_BLOB)   proxyKeyBlobs;
 } ClientKeyExchange;
```

ASN.1 syntax for G28147_ENCRYPTION_BLOB is defined in [CPCMS] as GostR3410-94-KeyTransportEncryptedKeyOctetString/ GostR3410-2001-KeyTransportEncryptedKeyOctetString.

```
 struct
 {
    G28147_ENCRYPTION_BLOB    keyBlob;
    ASN1_OCTET_STRING         cert;
 } TLS1_PROXY_KEY_BLOB;
```

proxyKeyBlobs - (optional) contains key exchange for multiple recipients (for example, when using firewall). cert - contains recipient's certificate if several recipients are used.

4.7 Certificate Verify

This message is used as described in section 7.4.8 of [TLS]. If the client have sent both a client certificate and an ephemeral public key, it MUST send a certificate verify message, as a proof of possession of the private key for provided certificate.

The TLS structures are extended as follows:

```
 enum { gost341094, gost34102001 }
     SignatureAlgorithm;
```

```
    select (SignatureAlgorithm) {
        case gost341094:
            digitally-signed struct {
                opaque gost341194_hash[32];
            };
        case gost34102001:
            digitally-signed struct {
                opaque gost341194_hash[32];
            };
    } Signature;

    CertificateVerify.signature.gostR3411_hash =
        GOSTR3411(handshake_messages)
```

4.8 Finished

This message is used as described in section 7.4.9 of [TLS].

```
Finished.verify_data = GOSTR3411_PRF(master_secret, finished_label +
                           GOSTR3411(handshake_messages)) [0..11]
```

5 Security Considerations

Parameter values for using cryptographic algorithms affect rigidity of information protection system. It is RECCOMENDED, that software applications verify signature values, subject public keys and algorithm parameters to conform to [GOSTR34102001], [GOSTR341094] standards prior to their use.

The cipher suites TLS_GOST341094_WITH_GOST28147_CFB_GOST3411 and TLS_GOST34102001_WITH_GOST28147_CFB_GOST3411 proposed hereby, have been analyzed by special certification laboratory of Scientific and Technical Centre "ATLAS" in appropriate levels of target_of_evaluation (TOE).

It is RECCOMENDED to perform an examination of cipher suites implementations by authorized agency with approved methods of cryptographic analysis.

6 References

[GOST28147] "Cryptographic Protection for Data Processing System", GOST 28147-89, Gosudarstvennyi Standard of USSR, Government Committee of the USSR for Standards, 1989. (In Russian);

[GOSTR341094] "Information technology. Cryptographic Data Security. Produce and check procedures of Electronic Digital Signatures based on Asymmetric Cryptographic Algorithm.", GOST R 34.10-94, Gosudarstvennyi Standard of Russian Federation, Government Committee of the Russia for Standards, 1994. (In Russian);

[GOSTR34102001] "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);

[GOSTR341194] "Information technology. Cryptographic Data Security. Hashing function.", GOST R 34.10-94, Gosudarstvennyi Standard of Russian Federation, Government Committee of the Russia for Standards, 1994. (In Russian);

[CPALGS] "CryptoPro CSP" Cryptographic Algorithms;

[Schneier95] B. Schneier, Applied cryptography, second edition, John Wiley & Sons, Inc., 1995;

[RFC 3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC 3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. L. Bassham, W. Polk, R. Housley. April 2002.

[RFC 2219] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[TLS] The TLS Protocol Version 1.0. T. Dierks, C. Allen. January 1999, RFC 2246.

[X.660] ITU-T Recommendation X.660 Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1997.

[CPPK] "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificates and Certificate Revocation List (CRL), corresponding to the algorithms GOST R 34.10-94, GOST R 34.10-2001, GOST R 34.11-94", IETF draft, <draft-cryptopro-cppk-00.txt>, ...

[CPCMS] "Cryptographic Message Syntax (CMS) algorithms for GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, GOST R 34.11-94", IETF draft, <draft-cryptopro-cpcms-00.txt>, work in progress

Acknowledgments

This document was created in accordance with "Russian Cryptographic Software Compatibility Agreement", signed by FGUE STC "Atlas", CRYPTO-PRO, Factor-TC, MD PREI, Infotecs GmbH, SPRCIS (SPbRCZI), Cryptocom, R-Alpha. The aim of this agreement is to achieve mutual compatibility of the products and solutions.

The authors wish to thank:

Microsoft Corporation Russia for provided information about company products and solutions, and also for technical consulting in PKI.

RSA Security Russia and Demos Co Ltd for active colaboration and critical help in creation of this document.

NIP Informzachita for compatibility testing of the proposed data formats while incorporating them into company products.

Citrix Inc for help in compatibility testing Citrix products for Microsoft Windows.

Russ Hously (Vigil Security, LLC, housley@vigilsec.com) and Vasilij Sakharov (DEMOS Co Ltd, svp@dol.ru) for initiative, creating this document.

This document is based on a contribution of CRYPTO-PRO company. Any substantial use of the text from this document must acknowledge

CRYPTO-PRO. CRYPTO-PRO requests that all material mentioning or referencing this document identify this as "CRYPTO-PRO CPTLS".

Author's Addresses

Serguei Leontiev
CRYPTO-PRO
38, Obraztsova,
Moscow, 127018, Russian Federation
EMail: lse@CryptoPro.ru

Grigorij Chudov
CRYPTO-PRO
38, Obraztsova,
Moscow, 127018, Russian Federation
EMail: chudov@CryptoPro.ru

Alexandr Afanasiev
Factor-TC
office 711, 14, Presnenskij val,
Moscow, 123557, Russian Federation
EMail: aaaf@factor-ts.ru

Nikolaj Nikishin
Infotecs GmbH
p/b 35, 80-5, Leningradskij prospekt,
Moscow, 125315, Russian Federation
EMail: nikishin@infotecs.ru

Boleslav Izotov
FGUE STC "Atlas"
38, Obraztsova,
Moscow, 127018, Russian Federation
EMail: izotov@stcnet.ru

Elena Minaeva
MD PREI
build 3, 6A, Vtoroj Troitskij per.,
Moscow, Russian Federation
EMail: evminaeva@mo.msk.ru

Serguei Murugov
R-Alpha
4/1, Raspletina,
Moscow, 123060, Russian Federation
EMail: msm@office.ru

Igori Ustinov

Cryptocom
office 239, 51, Leninskij prospekt,
Moscow, 119991, Russian Federation
EMail: igus@cryptocom.ru

Anatolij Erkin
SPRCIS (SPbRCZI)
1, Obrucheva,
St.Petersburg, 195220, Russian Federation
EMail: erkin@nevsky.net

Full Copyright Statement