ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ПО ИСПОЛЬЗОВАНИЮ НАБОРОВ АЛГОРИТМОВ ШИФРОВАНИЯ НА ОСНОВЕ ГОСТ 28147-89 ДЛЯ ПРОТОКОЛА БЕЗОПАСНОСТИ ТРАНСПОРТНОГО УРОВНЯ (TLS)

Проект первой редакции,
июнь 2014
rus-popov-tls-gost-00-rf

Москва
2014

Введение

Настоящие методические рекомендации предназначены для регистрации новых наборов алгоритмов шифрования протокола безопасности транспортного уровня (Transport Layer Security, TLS) в соответствии с процедурой, указанной в стандартах протокола TLS. Эти наборы алгоритмов шифрования основаны на российских государственных криптографических стандартах – открытые ключи по ГОСТ Р 34.10, алгоритм шифрования по ГОСТ 28147-89, алгоритмы хэширования по ГОСТ Р 34.11.

Необходимость разработки настоящего документа вызвана потребностью в обеспечении совместимости реализаций протокола TLS с использованием российских государственных криптографических стандартов.

Содержание

1 Область применения

Настоящие методические рекомендации предназначены для регистрации новых наборов алгоритмов шифрования протокола безопасности транспортного уровня (Transport Layer Security, TLS) в соответствии с процедурой, указанной в стандартах протокола TLS. Эти наборы алгоритмов шифрования основаны на российских государственных криптографических стандартах – открытые ключи по ГОСТ Р 34.10, алгоритм шифрования по ГОСТ 28147-89, алгоритм хэширования по ГОСТ Р 34.11.

В этом документе определяются две конфигурации: анонимный клиент – аутентифицированный сервер (сертификат предоставляет только сервер); аутентифицированный клиент - аутентифицированный сервер (клиент и сервер обмениваются сертификатами).

Используемый здесь язык представления такой же, как и в [**IETF RFC 5246**].

Поскольку настоящая спецификация расширяет [**IETF RFC 5246**], её содержание должно быть объединено с содержанием спецификации протокола TLS и другими спецификациями, которые расширяют протокол TLS.

1.1 Текущий статус документа как проекта рекомендаций ТК26

Этот параграф следует удалить после принятия данного проекта рекомендаций.

Передача проекта настоящих рекомендаций в ТК26 означает, что каждый их автор соглашается с не эксклюзивным предоставлением IPR для ТК26, аналогично положениям стандарта Интернет IETF BCP 79.

Данный предварительный документ является открытым документом «Рабочей группы по сопутствующим криптографическим алгоритмам, определяющим ключевые системы» и Технического комитета по стандартизации «Криптографическая защита информации (ТК26)». Область распространения документа не ограничена.

Этот документ действителен в течении максимум девяти месяцев, и может быть в любое время изменён, заменён на другой или отозван его авторами в любое время.

При цитировании или ссылке на него из других документов следует ставить отметку «документ готовится к публикации».

Список предварительных документов ТК26 доступен по ссылке <http://www.tc26.ru/>.

Настоящий предварительный документ актуален (действителен) по март 2015 года.

2 Нормативные ссылки

В настоящем документе использованы нормативные ссылки на следующие стандарты и рекомендации:

ГОСТ 28147 - «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», ГОСТ 28147-89, Государственный стандарт Союза ССР, Государственный комитет СССР по стандартам, ИПК Издательство стандартов, 1996.

ГОСТ Р 34.10 - «Информационные технологии. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», ГОСТ Р 34.10-2012, Национальный стандарт Российской Федерации, Федеральное агентство по техническому регулированию и метрологии, Стандартинформ, 2012.

ГОСТ Р 34.11 - «Информационные технологии. Криптографическая защита информации. Функция хэширования», ГОСТ Р 34.11-2012, Национальный стандарт Российской Федерации, Федеральное агентство по техническому регулированию и метрологии, Стандартинформ, 2012.

ГОСТ Р ИСО/МЭК 8824-1 - «Информационные технологии. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации», ГОСТ Р ИСО/МЭК 8824-1-2001, Государственный стандарт Российской Федерации, Госстандарт России, Москва, 2001.

ГОСТ Р ИСО/МЭК 8825-1 - «Информационные технологии. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования», ГОСТ Р ИСО/МЭК 8825-1-2003, Государственный стандарт Российской Федерации, Госстандарт России, Москва, 2003.

ТК26АЛГ - (проект) «Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012», документ готовится к публикации.

ТК26ИОК - (проект) «Методические рекомендации. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509», документ готовится к публикации.

ТК26CMS - (проект) «Методические рекомендации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 И ГОСТ Р 34.10 в криптографических сообщениях формата CMS», документ готовится к публикации.

ТК26УЗ - (проект) «Методические рекомендации по заданию узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89», документ готовится к публикации.

2.1 Дополнительные ссылки

IETF RFC 2246 - Т. Диркс и К. Аллен, «Протокол TLS версии 1.0» (Dierks, T. and C. Allen, The TLS Protocol Version 1.0), RFC 2246, январь 1999.

IETF RFC 5246 - Т. Диркс и Э. Рескола, «Протокол протокола безопасности транспортного уровня (TLS) версии 1.2» (Dierks, T. and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2), RFC 5246, июнь 2006.

Примечание – При пользовании настоящим документом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования - на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменён (изменён), то при пользовании настоящим документом следует руководствоваться заменённым (изменённым) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Обозначения и сокращения

В настоящих рекомендациях используются следующие обозначения и сокращения:

Key Meshing	Алгоритм усложнения ключа [**ТК26CMS**].
CipherSuite	Набор алгоритмов шифрования, обеспечения целостности и аутентичности в протоколах семейства SSL/TLS.
EAP	Расширяемый протокол аутентификации (Extensible Authentication Protocol).
HASH_GOSTR3411_SUITE	Функция хэширования по ГОСТ Р 34.11, конкретный алгоритм и параметры определяются CipherSuite (HASH_GOSTR341194, HASH_GOSTR341112_256).
HASH_GOSTR3411_CERT	Функция хэширования по ГОСТ Р 34.11, конкретный алгоритм и параметры определяются сертификатом клиента (HASH_GOSTR341194, HASH_GOSTR341112_256, HASH_GOSTR341112_512).
HMAC	Код аутентификации сообщения на основе хэш-значения (Hash-based Message Authentication Code).
HMAC_GOSTR3411	Код аутентификации сообщения на основе хэш-кода, вычисленного согласно ГОСТ Р 34.11, конкретный алгоритм и параметры определяется CipherSuite (HMAC_GOSTR341194, HMAC_GOSTR3411_2012_256). Функция на основе ГОСТ Р 34.11-94 определена в [**IETF RFC 4357**], функции на основе ГОСТ Р 34.11-2012 определены в [**ТК26АЛГ**].
HMAC_GOSTR341194	Функция на основе ГОСТ Р 34.11-94, определена в [**IETF RFC 4357**] как HMAC_GOSTR3411.
IMIT_GOST28147	Алгоритм по ГОСТ 28147 в режиме имитовставки.
MAC	Код аутентификации сообщения (Message Authentication Code).
PRF	Семейство псевдослучайных функций (Pseudorandom Function family).
PRF_GOSTR3411	Псевдослучайная функция на основе кода аутентификации HMAC_GOSTR3411. Функция на основе ГОСТ Р 34.11-94 определена в [**IETF RFC 4357**], функции на основе ГОСТ Р 34.11-2012 определены в [**ТК26АЛГ**].
PRF_GOSTR341194	Псевдослучайная функция на основе кода аутентификации HMAC_GOSTR341194, определена в [**IETF RFC 4357**] как PRF_GOSTR3411.
UKM	Материал ключа пользователя (user key material).

4 Определения наборов алгоритмов шифрования

Настоящие методические рекомендации определяют четыре поточных набора алгоритмов шифрования (CipherSuite, Stream ciphers):

- TLS_GOSTR341112_256_WITH_28147_CNT_IMIT;
- TLS_GOSTR341112_256_WITH_NULL_GOSTR3411;
- TLS_GOSTR341001_WITH_28147_CNT_IMIT;
- TLS_GOSTR341001_WITH_NULL_GOSTR3411.

Предназначенные для использования в протоколе TLS версии 1.2.

4.1 Сертификаты сторон

Клиент TLS, поддерживающий настоящие рекомендации, может поддерживать все виды хэш функций, подписей и все типы сертификатов для всех CipherSuite, описанных в данном документе.

Сервер TLS имеющий сертификат ключа по ГОСТ Р 34.10-2012 для любой длины ключа может поддерживать CipherSuite:

- TLS_GOSTR341112_256_WITH_28147_CNT_IMIT;
- TLS_GOSTR341112_256_WITH_NULL_GOSTR3411.

Сервер TLS имеющий сертификат ключа по ГОСТ Р 34.10-2001 может поддерживать CipherSuite:

- TLS_GOSTR341001_WITH_28147_CNT_IMIT;
- TLS_GOSTR341001_WITH_NULL_GOSTR3411;
- TLS_GOSTR341112_256_WITH_28147_CNT_IMIT;
- TLS_GOSTR341112_256_WITH_NULL_GOSTR3411.

4.2 Обмен ключами

Определённые здесь наборы алгоритмов шифрования для передачи premaster_secret (256-бит) используют алгоритм передачи ключей определённый сертификатом сервера [**TK26CMS**].

4.3 Псевдослучайная функция

Описанные здесь наборы алгоритмов шифрования используют HMAC и псевдослучайную функцию (PRF) TLS в соответствии с разделом 5 [**IETF RFC 5246**], на основе функции хэширования ГОСТ Р 34.11 (HASH_GOSTR3411_SUITE, HMAC_GOSTR3411, PRF_GOSTR3411). Алгоритм ГОСТ Р 34.11 и его параметры определяются согласованным набором алгоритмов шифрования

Таблица 1. Алгоритмы хэширования и псевдослучайной функции

Набор алгоритмов шифрования	Хэш, HMAC и псевдослучайная функция
TLS_GOSTR341112_256_WITH_28147_CNT_IMIT	HASH_GOSTR341112_256 HMAC_GOSTR3411_2012_256 PRF_TLS_GOSTR3411_2012_256
TLS_GOSTR341001_WITH_28147_CNT_IMIT	HASH_GOSTR341194 HMAC_GOSTR341194 PRF_GOSTR341194
TLS_GOSTR341112_256_WITH_NULL_GOSTR3411	HASH_GOSTR341112_256 HMAC_GOSTR3411_2012_256 PRF_TLS_GOSTR3411_2012_256

TLS_GOSTR341001_WITH_NULL_GOSTR3411	HASH_GOSTR341194 HMAC_GOSTR341194 PRF_GOSTR341194

Зависимые протоколы, такие как SSTP, EAP-TLS [**IETF RFC 5216**], ДОЛЖНЫ использовать согласованную PRF.

4.4 Алгоритм шифрования и MAC

Используются следующие алгоритмы шифрования и MAC-функции (подробное описание алгоритмов шифрования приведено в разделе 5.1 настоящего документа):

Таблица 2. Алгоритмы шифрования и MAC-функции

Набор алгоритмов шифрования	Алгоритм шифрования и параметры	MAC
TLS_GOSTR341112_256_WITH_28147_CNT_IMIT	ГОСТ 28147-89 id-tc26-gost-28147-param-Z	IMIT_GOST28147
TLS_GOSTR341001_WITH_28147_CNT_IMIT	ГОСТ 28147-89 id-Gost28147-89-CryptoPro-A-ParamSet	IMIT_GOST28147
TLS_GOSTR341112_256_WITH_NULL_GOSTR3411	–	HMAC_GOSTR3411_2012_256
TLS_GOSTR341001_WITH_NULL_GOSTR3411	–	HMAC_GOSTR341194

Параметры алгоритма шифрования ГОСТ 28147-89 и IMIT_GOST28147 определяются согласованным набором алгоритмов шифрования.

Для стандартных потоковых CipherSuite MAC рассчитывается на следующие данные [**IETF RFC 5246**]:

```
MACed_data[seq_num] = seq_num +
                      TLSCompressed.type +
                      TLSCompressed.version +
                      TLSCompressed.length +
                      TLSCompressed.fragment;
```

Определённые в настоящих рекомендациях CipherSuite используют эти входные данные конкатенированные со всеми предыдущими записями. Таким образом, входными данными функций IMIT_GOST28147 и HMAC_GOSTR3411 являются:

```
MAC(MACed_data[n]) = IMIT_GOST28147(MACed_data[0] + ... + MACed_data[n]);
MAC(MACed_data[n]) = HMAC_GOSTR3411(MACed_data[0] + ... + MACed_data[n])
```

4.5 Алгоритм подписи и хэширования

Алгоритм и параметры подписи ГОСТ Р 34.10 и функции хэширования, которые используются при вычислении и проверке CertificateVerify, определяются выбором сертификата клиента.

Примечание:

С учетом того, что набор входных данных функции хэширования является конкатенацией всех сообщений вплоть до сообщения CertificateVerify (п. 7.4.8 [**IETF RFC 5246**]), совместимые реализации могут как накапливать эти сообщения, так и рассчитывать все потенциально возможные функции хэширования (функции хэширования для всех потенциально возможных сертификатов, [**IETF RFC 2246**]).

5 Структуры данных и вычисления

5.1 Алгоритм шифрования

ГОСТ 28147-89 использует 256-битный ключ и 8-байтовый вектор инициализации (IV).

Определённые здесь наборы алгоритмов шифрования используют ГОСТ 28147-89 в качестве потокового алгоритма шифрования в режиме гаммирования, параметры определяются согласованным набором алгоритмов шифрования.

IMIT_GOST28147 – это алгоритм по ГОСТ 28147-89 в режиме имитовставки (4 байта).

5.2 Вычисление ключей

Вычисление ключей производится в соответствии с разделом 6.3 [**IETF RFC 5246**] с использованием функции PRF_GOSTR3411. Используются следующие параметры:

- SecurityParameters.enc_key_length = 32
- SecurityParameters.mac_key_length = 32
- SecurityParameters.fixed_iv_length = 8

Длина необходимого ключевого материала составляет 144 байта.

5.3 Сертификат сервера (Server Certificate)

Для данных наборов алгоритмов шифрования требуется такое сообщение, и оно ДОЛЖНО содержать сертификат с алгоритмом открытого ключа, соответствующим полю ServerHello.cipher_suite.

5.4 Сообщение об обмене ключа со стороны сервера (Server Key Exchange Message)

В этих наборах алгоритмов шифрования данное сообщение использоваться НЕ ДОЛЖНО, так как все необходимые параметры присутствуют в сертификате сервера [**ТК26ИОК**].

5.5 Запрос на получение сертификата (Certificate Request)

Это сообщение используется в соответствии с [**IETF RFC 5246**] и расширяется следующим образом:

```
enum {
    gostr34102001(22), gostr34102012_256(<TBD>+2),
    gostr34102012_512(<TBD>+3), (255)
} ClientCertificateType;
```

Типы сертификатов gostr34102001, gostr34102012_256, gostr34102012_512 указывают на то, что сервер принимает сертификаты с открытыми ключами по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 с соответствующим размером закрытого ключа.

```
enum{
    gostr3411(<TBD>+1), gostr34112012_256(<TBD>+2),
    gostr34112012_512(<TBD>+3), (255)
} HashAlgorithm;
enum{
    gostr34102001(<TBD>+1), gostr34102012_256(<TBD>+3),
    gostr34102012_512(<TBD>+3), (255)
} SignatureAlgorithm;
```

Пары SignatureAndHashAlgorithm, (gostr3411, gostr34102001), (gostr34112012_256, gostr34102012_256) и (gostr34112012_512, gostr34102012_512) указывают на то, что сервер поддерживает данные алгоритмы при обработке сертификатов.

5.6 Сообщение об обмене ключа со стороны клиента (Client Key Exchange Message)

Это сообщение используется в соответствии с [**IETF RFC 5246**]. Оно необходимо для данных наборов алгоритмов шифрования и содержит закодированную в DER структуру TLSGostKeyTransportBlob [**ГОСТ Р ИСО/МЭК 8825-1**].

```
enum { vko_gost } KeyExchangeAlgorithm;

struct {
    select (KeyExchangeAlgorithm) {
        case vko_gost: TLSGostKeyTransportBlob;
    } exchange_keys;
} ClientKeyExchange;
```

Определение АСН.1 для этой структуры выглядит следующим образом:

```
TLSGostKeyTransportBlob ::= SEQUENCE {
    keyBlob           GostR3410-KeyTransport,
    proxyKeyBlobs     SEQUENCE OF TLSProxyKeyTransportBlob OPTIONAL
}
```

Определение структуры GostR3410-KeyTransport смотри в [**ТК26CMS**], в структуре keyBlob ДОЛЖНО присутствовать поле transportParameters.

В том случае, если сервер не запрашивал сертификат клиента или алгоритм и параметры открытого ключа клиента не совпадают с алгоритмом и параметрами открытого ключа сервера, то ДОЛЖНО присутствовать поле keyBlob.transportParameters.ephemeralPublicKey. В противном случае данное поле СЛЕДУЕТ пропустить.

```
TLSProxyKeyTransportBlob ::= SEQUENCE {
    keyBlob           GostR3410-KeyTransport,
    cert              OCTET STRING
}
```

proxyKeyBlobs – (не обязательно) содержит сообщения для обмена ключами для вторичных получателей (например, для межсетевого экрана, который проверяет соединения).

cert - содержит сертификат вторичного получателя.

5.6.1 Действия клиента

Клиент формирует структуру GostR3410-KeyTransport для передачи одноразового (случайного) 256-битного ключа premaster_secret согласно [**ТК26CMS**], для вычисления UKM используется хэш-функция HASH_GOSTR3411_SUITE определяемая согласованным набором алгоритмов шифрования:

```
UKM = HASH_GOSTR3411_SUITE(client_random|server_random)[0..7]
```

Если сервер запрашивает сертификат клиента, а так же если алгоритм и параметры сертификатов сервера и клиента совпадают, то в качестве ключа отправителя ДОЛЖЕН быть использован секретный ключ, соответствующий сертификату клиента. В противном случае клиент заполняет поле keyBlob.transportParameters.ephemeralPublicKey, и в качестве ключа отправителя ДОЛЖЕН быть использован соответствующий секретный ключ.

5.6.2 Действия сервера

Сервер обрабатывает структуру GostR3410-KeyTransport согласно [**ТК26CMS**], предварительно сервер ДОЛЖЕН проверить значение UKM до начала расшифрования premaster_secret.

5.7 Проверка сертификата (Certificate Verify)

Если клиент предоставил и сертификат клиента, и эфемерный открытый ключ, он ДОЛЖЕН отправить сообщение о проверке сертификата в качестве доказательства владения закрытым ключом для предоставленного сертификата.

При использовании CipherSuite в рамках TLS 1.2 [**IETF RFC 5246**]. Расширений структур не требуется.

5.8 Завершение (Finished)

Это сообщение используется в соответствии с описанием, приведённым в разделе 7.4.9 из [**IETF RFC 5246**]. Используются алгоритмы PRF_GOSTR3411 и HASH_GOSTR3411_SUITE, определяемые согласованным набором алгоритмов шифрования:

```
Finished.verify_data = PRF_GOSTR3411(master_secret, finished_label,
                 HASH_GOSTR3411_SUITE(handshake_messages)) [0..11]
```

6 Совместимость

Требования по реализации TLS на основе ГОСТ 28147-89:

- TLS_GOSTR341112_256_WITH_28147_CNT_IMIT – обязательно;
- gostr34112012_256 и gostr34102012_256 - обязательно.

По историческим причинам некоторые TLS сервера имеющие только один сертификат ключа по ГОСТ Р 34.10-2001, при отсутствии перечисленных CipherSuite в списке ClientHello.cipher_suites, могут отвечать ServerHello.cipher_suite со значением TLS_GOSTR341001_WITH_28147_CNT_IMIT.

По историческим причинам некоторые приложения используют наборы алгоритмов шифрования, определённые в настоящем документе в протоколе TLS версии 1.0 [**IETF RFC 2246**], частично используя функционал из [**IETF RFC 5246**], включая вычисление псевдослучайной функции (PRF), зависимой от набора алгоритмов шифрования, сообщения о завершении (Finished) и сообщения о проверке сертификата (Certificate Verify).

При использовании CipherSuite в рамках TLS 1.0 [**IETF RFC 2246**], тип Signature должен быть расширен:

```
select (SignatureAlgorithm) {
    case gostr34102001:
    case gostr34102012_256:
        digitally-signed struct {
            opaque gostr3411_256_hash[32];
        };
    case gostr34102012_512:
        digitally-signed struct {
            opaque gostr3411_512_hash[64];
        };
} Signature;
```

При использовании этого типа в сообщении "Certificate Verify", хэш-код вычисляется с помощью согласованной хэш функции от всех сообщений handshake: HASH_GOSTR3411_CERT(handshake_messages).

7 Вопросы безопасности

Перед началом использования значений подписи, открытых ключей субъекта и параметров алгоритма приложениям РЕКОМЕНДУЕТСЯ проводить проверку на предмет их соответствия стандартам ГОСТ Р 34.10.

И клиенту, и серверу РЕКОМЕНДУЕТСЯ выполнять проверку срока использования закрытого ключа другой стороны.

При согласовании используемой CipherSuite согласно [**IETF RFC 5246**]: сервер выбирает первую, удовлетворяющую политике безопасности сервера, CipherSuite из упорядоченного списка ClientHello.cipher_suites, который формируется согласно списку предпочтений политики безопасности клиента. При отсутствии дополнительных требований рекомендуется, чтобы TLS_GOSTR341112_256_WITH_28147_CNT_IMIT, TLS_GOSTR341112_256_WITH_NULL_GOSTR3411 предшествовали TLS_GOSTR341001_WITH_28147_CNT_IMIT и TLS_GOSTR341001_WITH_NULL_GOSTR3411 в списке предпочтений политики безопасности клиента.

При согласовании используемого сертификата клиента согласно [**IETF RFC 5246**]: клиент выбирает первый сертификат (с цепочкой сертификатов) удовлетворяющий политике безопасности клиента из упорядоченного списка поля supported_signature_algorithms (certificate_types) с ограничением по списку УЦ в поле certificate_authorities структуры CertificateRequest, который формируется согласно списку предпочтений политики безопасности сервера. При отсутствии дополнительных требований рекомендуется, чтобы gostr34112012_512, gostr34112012_256 (gostr34102012_512, gostr34102012_256) предшествовали gostr3411 (gostr34102001) в списке предпочтений политики безопасности сервера.

8 Согласование с IANA

В этом документе определяются следующие новые наборы алгоритмов шифрования, значения которых используются в нескольких реализациях наборов алгоритмов шифрования протокола TLS 1.0. В настоящее время они перечислены в реестре в качестве зарезервированных. Произведён запрос в IANA на обновление реестра набора алгоритмов шифрования протокола TLS, определённого в [**IETF RFC 5246**] такими значениями:

- CipherSuite TLS_GOSTR341001_WITH_28147_CNT_IMIT = {0x00,0x81}
- CipherSuite TLS_GOSTR341001_WITH_NULL_GOSTR3411 = {0x00,0x83}

В этом документе определяются следующие новые типы клиентских сертификатов. Их значения, представленные здесь, используются несколькими реализациями одних и тех же наборов алгоритмов шифрования протокола TLS 1.0 и описаны в предыдущих проектах.

В настоящее время они перечислены в реестре в качестве зарезервированных. Произведён запрос в IANA на обновление реестра идентификаторов TLS ClientCertificateType, определённого в [**IETF RFC 5246**], следующими значениями:

```
enum {
    gostr34102001(22), gostr34102012_256(<TBD>+2),
    gostr34102012_512(<TBD>+3), (255)
} ClientCertificateType;
```

В этом документе определяются следующие новые типы алгоритмов подписи, чьи значения следует присвоить из реестра TLS SignatureAlgorithm, определённого в [**IETF RFC 5246**]:

```
enum{
    gostr34102001(<TBD>+1), gostr34102012_256(<TBD>+3),
    gostr34102012_512(<TBD>+3), (255)
} SignatureAlgorithm;
```

В этом документе определяются следующие новые типы алгоритма хэширования, чьи значения следует присвоить из реестра TLS HashAlgorithm, определённого в [**IETF RFC 5246**]:

```
enum{
    gostr3411(<TBD>+1), gostr34112012_256(<TBD>+2),
    gostr34112012_512(<TBD>+3), (255)
} HashAlgorithm;
```

8.1 Приватные типы алгоритмов

До регистрации в IANA предварительные реализации используют следующие приватные номера преобразований:

- CipherSuite TLS_GOSTR341112_256_WITH_28147_CNT_IMIT = {0xFF,0x85}
- CipherSuite TLS_GOSTR341112_256_WITH_NULL_GOSTR3411 = {0xFF,0x87}

```
enum {
    gostr34102001(22), gostr34102012_256(238),
    gostr34102012_512(239), (255)
} ClientCertificateType;
enum{
    gostr34102001(237), gostr34102012_256(238),
    gostr34102012_512(239), (255)
} SignatureAlgorithm;
enum{
    gostr3411(237), gostr34112012_256(238),
    gostr34112012_512(239), (255)
} HashAlgorithm;
```

Приложение А Примеры (информативное)

A.1. TLS 1.0 аутентификация клиента с ключом 512 бит и сервера с ключом 512 бит

```
client -> server:

header type
16 (handshake)
major version
03
minor version
01
length
004F
message type
01 (client hello)
Length
00004B
TLS VERSION
                  major version
                  03
                  minor version
                  01
client random
52E78ECF 8CF81884 8F016AA5 2ED29277 66015AC6 24648148 A58D736D 83216A7D
session id length
00
session id

ciphersuite length
0004
ciphersuite
0081               TLS_CIPHER_2001
FF85               TLS_CIPHER_2012
compression methods
                  length
                  01
                  compression method
                  00
extensions
  extensions length
  001E
  renegotiation info (FF01)
  length
  0001
  Renegotiation Info extension
  00
  server name (0000)
  length
  0015
  server name list length
  0013
  server name type
```

```
  00
  server name length
  0010
  server name
  746C7363 6F6E665F 73727631 30323465

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


client <- server:

header type
16 (handshake)
major version
03
minor version
01
Length
03C0

message type
02 (server hello)
Length
000046
TLS VERSION
                   major version
                   03
                   minor version
                   01
server random
52E78ECF 1800D27D 3FDA35F1 F4907B18 583CBDA5 D2B2F5BC EDDD21EF 4966674C
session id length
20
session id
A28858D3 84BB1D06 E5FD5D83 20716257 A2C470C4 5D126B00 44272A5D 67888A02
ciphersuite
FF85                TLS_CIPHER_2012
compression method
00
extensions

message type
0B (certificate)
length
000324
server certificate chain
00032100 031E3082 031A3082 02C9A003 02010202 0A427E7B CC000000 8B927330
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 375A170D 32343031 32383131
30343237 5A304931 19301706 03550403 0C10746C 73636F6E 665F7372 76313032
3465312C 302A0609 2A864886 F70D0109 01161D74 6C73636F 6E665F73 72763130
32346540 63727970 746F7072 6F2E7275 3081AA30 2106082A 85030701 01010230
1506092A 85030701 02010201 06082A85 03070101 02030381 84000481 80F0DBBD
44A22D19 AFCB22A0 CAD421A0 2E7930D5 C6E549C1 3BBF7D14 377C67CA E87D45E7
9E27E96D 631A0AA6 C71E6B35 3C66A023 62F9D43F C3F53DDF AB567CDF B92909DC
```

```
B62A9318 96ED1F1D 1655AC58 4DC8D674 5C51EA68 CAC8EBF4 9CAC305E FA642850
9799F30D 219A8407 827EB276 293E7BC1 AE68DCB9 39FAD9BF BCAD938C 84A38201
56308201 52301306 03551D25 040C300A 06082B06 01050507 0301300B 0603551D
0F040403 02043030 1D060355 1D0E0416 04141275 ECCDF8B0 38C7FD18 379C2C4E
B1ECCC93 2792301F 0603551D 23041830 1680149E 03F0B89C FC60DC8A 181EE800
DFA85B32 CD737630 3F060355 1D1F0438 30363034 A032A030 862E6874 74703A2F
2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E 726F6C6C 2F746573
742D6361 2E63726C 3081AC06 082B0601 05050701 0104819F 30819C30 4B06082B
06010505 07300286 3F687474 703A2F2F 766D2D74 6573742D 63612E63 702E7275
2F436572 74456E72 6F6C6C2F 766D2D74 6573742D 63612E63 702E7275 5F746573
742D6361 2E637274 304D0608 2B060105 05073002 86416669 6C653A2F 2F5C5C76
6D2D7465 73742D63 612E6370 2E72755C 43657274 456E726F 6C6C5C76 6D2D7465
73742D63 612E6370 2E72755F 74657374 2D63612E 63727430 0806062A 85030202
03034100 25D1D3FC E78525E7 6CE8CAC6 D511B9F4 47BA8471 6A1B235D DF9BE280
1C6E56D3 01E8909E 1E7DDAEA 5A897272 072C3AB3 F130205F 87298A74 74A4011B
E7543ABB

message type
0D (certificate request)
length
000046
certificate request
  certificate types length
  03
  certificate_types
  16   gostr34102001
  EE   gostr34102012_256
  EF   gostr34102012_512
  certificate authorities length
  0040
  certificate authorities
  003E303C 31123010 060A0992 268993F2 2C640119 16027275 31123010 060A0992
  268993F2 2C640119 16026370 31123010 06035504 03130974 6573742D 6D736361

message type
0E (server hello done)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

client certificate chain
00032100 031E3082 031A3082 02C9A003 02010202 0A427E7E 1E000000 8B927430
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 385A170D 32343031 32383131
30343238 5A304931 19301706 03550403 0C10746C 73636F6E 665F636C 6E313032
3465312C 302A0609 2A864886 F70D0109 01161D74 6C73636F 6E665F63 6C6E3130
32346540 63727970 746F7072 6F2E7275 3081AA30 2106082A 85030701 01010230
1506092A 85030701 02010201 06082A85 03070101 02030381 84000481 80603433
F7BA1D9F 46A3DECD E0895A62 5498B344 1383D954 A313B245 2B554FBC 67B08064
16FDC7CA 36E913A4 59555336 09BF8590 4A08E34B 351EB1B3 5742924F 65FCE58F
74ABBB6F 13270A9F 72F9E678 B5F58A9A C6AEB36E 8DB7034F 769C587B 01EFB862
```

```
102311F1 3F585D50 D6456DA3 7B3E6E63 9D0F584A 6AB114F7 68E27619 92A38201
56308201 52301306 03551D25 040C300A 06082B06 01050507 0302300B 0603551D
0F040403 02043030 1D060355 1D0E0416 0414E8EF 647D662D 0B86647A D9525E02
A8ABF409 6A43301F 0603551D 23041830 1680149E 03F0B89C FC60DC8A 181EE800
DFA85B32 CD737630 3F060355 1D1F0438 30363034 A032A030 862E6874 74703A2F
2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E 726F6C6C 2F746573
742D6361 2E63726C 3081AC06 082B0601 05050701 0104819F 30819C30 4B06082B
06010505 07300286 3F687474 703A2F2F 766D2D74 6573742D 63612E63 702E7275
2F436572 74456E72 6F6C6C2F 766D2D74 6573742D 63612E63 702E7275 5F746573
742D6361 2E637274 304D0608 2B060105 05073002 86416669 6C653A2F 2F5C5C76
6D2D7465 73742D63 612E6370 2E72755C 43657274 456E726F 6C6C5C76 6D2D7465
73742D63 612E6370 2E72755F 74657374 2D63612E 63727430 0806062A 85030202
03034100 DE24ECA8 3C9A6226 4AF6D978 4E71AE0D FB4694CC CE21A16E 3D1EA426
B8E1A4C2 274C762A 0F6A1CE2 087116E1 0DDDB2B5 A6AA3F99 7F4BA6CD D8FCF026
623B5A62

premastersecret
0619ECC1 161CB54D 391B3610 CEDD90E5 C858DC3C AF199005 C45F9821 2B21A761
client private key
D95C536A 47657160 032FAEE5 CE9465DE DACE5058 B0F51891 87A21CA5 87A1C4AA
408AD861 230A239E 7BD15632 EE1DEDFC CBF9A051 F46C6186 02309605 31AEB500
server public key blob header
06200100 3D2E0000 4D414731 00040000 30150609 2A850307 01020102 0106082A
85030701 010203F0
server public key
F0DBBD44 A22D19AF CB22A0CA D421A02E 7930D5C6 E549C13B BF7D1437 7C67CAE8
7D45E79E 27E96D63 1A0AA6C7 1E6B353C 66A02362 F9D43FC3 F53DDFAB 567CDFB9
2909DCB6 2A931896 ED1F1D16 55AC584D C8D6745C 51EA68CA C8EBF49C AC305EFA
64285097 99F30D21 9A840782 7EB27629 3E7BC1AE 68DCB939 FAD9BFBC AD938C84
hash(client_random, server_random)
F2249B00 0ACEDF36 FF45A3F3 F71C5EBC E45723CC C73C86BA 1BF8C287 97CD9539
ukm
F2249B00 0ACEDF36
Inner Point
5DB5F416 EBE212CF F33C790C BCF2E39F 28F1C24A 731CB518 AA0BB418 B9BFAF0F
EB71132F A1677F4B A033340A 5093543A B1C2C273 D25C94D4 6D24D63A ACD5D9D1
9CEFFF01 719A677B 0A6DE8A1 605E243F 267452B8 4BDECB5E CE36A881 2D2E4ACC
A805B1E2 89331E73 2E695FD6 AD5D3C6D 916E6371 721D4D3A B4F8D4D4 325E5354
VKO result
7835B7D8 5E0E3B28 8D99BF0E 3451C5FB 8F63808E EF9B3DEA 2066A000 AEB10358
diversified key
BE797602 638CEFBB BB338DEF 1AA233BF A6B5F254 9F33AAA1 21E30000 A3FE66E2
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in ECB mode
                  37C36990 7DAA1C4C 195B7C02 2C4CFA09 AE6A7F60 124EE1AB
8443EA35 A6FDE0B0
                  MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                  D250C063

client key exchange
30433041 30280420 37C36990 7DAA1C4C 195B7C02 2C4CFA09 AE6A7F60 124EE1AB
8443EA35 A6FDE0B0 0404D250 C063A015 06092A85 03070102 05010104 08F2249B
000ACEDF 36
```

client -> server:

header type
16 (handshake)
major version
03
minor version
01
Length
0371

message type
0B (certificate)
Length
000324
client certificate chain
00032100 031E3082 031A3082 02C9A003 02010202 0A427E7E 1E000000 8B927430
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 385A170D 32343031 32383131
30343238 5A304931 19301706 03550403 0C10746C 73636F6E 665F636C 6E313032
3465312C 302A0609 2A864886 F70D0109 01161D74 6C73636F 6E665F63 6C6E3130
32346540 63727970 746F7072 6F2E7275 3081AA30 2106082A 85030701 01010230
1506092A 85030701 02010201 06082A85 03070101 02030381 84000481 80603433
F7BA1D9F 46A3DECD E0895A62 5498B344 1383D954 A313B245 2B554FBC 67B08064
16FDC7CA 36E913A4 59555336 09BF8590 4A08E34B 351EB1B3 5742924F 65FCE58F
74ABBB6F 13270A9F 72F9E678 B5F58A9A C6AEB36E 8DB7034F 769C587B 01EFB862
102311F1 3F585D50 D6456DA3 7B3E6E63 9D0F584A 6AB114F7 68E27619 92A38201
56308201 52301306 03551D25 040C300A 06082B06 01050507 0302300B 0603551D
0F040403 02043030 1D060355 1D0E0416 0414E8EF 647D662D 0B86647A D9525E02
A8ABF409 6A43301F 0603551D 23041830 1680149E 03F0B89C FC60DC8A 181EE800
DFA85B32 CD737630 3F060355 1D1F0438 30363034 A032A030 862E6874 74703A2F
2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E 726F6C6C 2F746573
742D6361 2E63726C 3081AC06 082B0601 05050701 0104819F 30819C30 4B06082B
06010505 07300286 3F687474 703A2F2F 766D2D74 6573742D 63612E63 702E7275
2F436572 74456E72 6F6C6C2F 766D2D74 6573742D 63612E63 702E7275 5F746573
742D6361 2E637274 304D0608 2B060105 05073002 86416669 6C653A2F 2F5C5C76
6D2D7465 73742D63 612E6370 2E72755C 43657274 456E726F 6C6C5C76 6D2D7465
73742D63 612E6370 2E72755F 74657374 2D63612E 63727430 0806062A 85030202
03034100 DE24ECA8 3C9A6226 4AF6D978 4E71AE0D FB4694CC CE21A16E 3D1EA426
B8E1A4C2 274C762A 0F6A1CE2 087116E1 0DDDB2B5 A6AA3F99 7F4BA6CD D8FCF026
623B5A62

message type
10 (client key exchange)
length
000045
client key exchange
30433041 30280420 37C36990 7DAA1C4C 195B7C02 2C4CFA09 AE6A7F60 124EE1AB
8443EA35 A6FDE0B0 0404D250 C063A015 06092A85 03070102 05010104 08F2249B
000ACEDF 36

>>>

client -> server:

header
header type
14 (change cipher spec)
major version
03
minor version
01
Length
0001
message type
01 (change cipher spec)
length
000000

>>

client internals:

master secret = GOSTR3411_PRF(PreMasterSecret, “master secret”, client_random, server_random)

2CD29016 223017C6 DFB127E9 3DB82D41 3F2F4AFA 15F09E61 A8C5EB57 172196AF
D6FD841F A4C96323 F8B358DC A627BBD0
hash(master secret)
10AE7D45 BB1C6156 6ED33DA7 D3AB658C 41F9189F 8835C24F A1ECCA4E D6BCE054
key_block = PRF_GOSTR3411(hash(master secret), “key expansion”, server_random, client_random)
8A6825F7 E9F38F40 66A0B95B 39831FAF 4394D119 7E01F55B 10DC2C90 7D2FF862
6DBF6CDE 5F5DEA46 9076782D F559AE47 122299BF BB471CB1 3FF7FE1E 34F174C1
B83D8BD4 AE9BE933 AF3BC270 A49F6A15 DC6F906D CCEA7E05 FB83E6AB 51E29BCC
3077B22B E660A3EB F5A781DE 323026EF 1B25BE3E 82AB22BA 5027FE5C AB8FE7FD
601B3168 2C42B8BC FD2D4A6B C08C5B8F

client write key
B83D8BD4 AE9BE933 AF3BC270 A49F6A15 DC6F906D CCEA7E05 FB83E6AB 51E29BCC
client write MAC secret
8A6825F7 E9F38F40 66A0B95B 39831FAF 4394D119 7E01F55B 10DC2C90 7D2FF862
client write IV
601B3168 2C42B8BC
hash(handshake messages)
FB795F88 38555ADA B86EB09B D44166A2 558B2CBA 7618E41E EA75124B 114604EB
finished label
client finished
verify data = PRF_GOSTR3411(hash(master secret), finished label, hash(handshake messages))
E9554B78 39F9BA2D DDDA50BF

message type
14 (finished)
length
00000C
verify data
E9554B78 39F9BA2D DDDA50BF

```
client -> server:

write_sequence
00000000 00000000
header type
16 (handshake)
major version
03
minor version
01
Length
0010
message encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
0EDCDB75 6C1701F7 1B55C37E A855B745
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
3A34A4B9

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


server internals:

server private key
CAA00F9C 2F6E2CFF 3CC9AE17 2AC130ED B7517D29 FD58DC00 D50C49B7 819D9C26
FFBD82E6 91D2B370 1DF39C62 BAB8AB79 DA5C1AD5 E3A5E6F0 D4DB9531 624A34EC
public key blob header
06200100 3D2E0000 4D414731 00040000 30150609 2A850307 01020102 0106082A
85030701 01020360
client public key
603433F7 BA1D9F46 A3DECDE0 895A6254 98B34413 83D954A3 13B2452B 554FBC67
B0806416 FDC7CA36 E913A459 55533609 BF85904A 08E34B35 1EB1B357 42924F65
FCE58F74 ABBB6F13 270A9F72 F9E678B5 F58A9AC6 AEB36E8D B7034F76 9C587B01
EFB86210 2311F13F 585D50D6 456DA37B 3E6E639D 0F584A6A B114F768 E2761992
hash(client random, server random)
F2249B00 0ACEDF36 FF45A3F3 F71C5EBC E45723CC C73C86BA 1BF8C287 97CD9539
ukm
F2249B00 0ACEDF36
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1(id-tc26-gost-28147-param-Z) in ECB mode
                   37C36990 7DAA1C4C 195B7C02 2C4CFA09 AE6A7F60 124EE1AB
8443EA35 A6FDE0B0
                   MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                   D250C063
Inner Point
5DB5F416 EBE212CF F33C790C BCF2E39F 28F1C24A 731CB518 AA0BB418 B9BFAF0F
EB71132F A1677F4B A033340A 5093543A B1C2C273 D25C94D4 6D24D63A ACD5D9D1
9CEFFF01 719A677B 0A6DE8A1 605E243F 267452B8 4BDECB5E CE36A881 2D2E4ACC
A805B1E2 89331E73 2E695FD6 AD5D3C6D 916E6371 721D4D3A B4F8D4D4 325E5354
VKO result
7835B7D8 5E0E3B28 8D99BF0E 3451C5FB 8F63808E EF9B3DEA 2066A000 AEB10358
diversified key
BE797602 638CEFBB BB338DEF 1AA233BF A6B5F254 9F33AAA1 21E30000 A3FE66E2
```

premastersecret
0619ECC1 161CB54D 391B3610 CEDD90E5 C858DC3C AF199005 C45F9821 2B21A761

master secret = PRF_GOSTR3411(premastersecret, “master secret”, client random, server random)
2CD29016 223017C6 DFB127E9 3DB82D41 3F2F4AFA 15F09E61 A8C5EB57 172196AF D6FD841F A4C96323 F8B358DC A627BBD0
hash(master secret)
10AE7D45 BB1C6156 6ED33DA7 D3AB658C 41F9189F 8835C24F A1ECCA4E D6BCE054
key block = PRF_GOSTR3411(hash(master secret), “key expansion”, server random, client random)
8A6825F7 E9F38F40 66A0B95B 39831FAF 4394D119 7E01F55B 10DC2C90 7D2FF862 6DBF6CDE 5F5DEA46 9076782D F559AE47 122299BF BB471CB1 3FF7FE1E 34F174C1 B83D8BD4 AE9BE933 AF3BC270 A49F6A15 DC6F906D CCEA7E05 FB83E6AB 51E29BCC 3077B22B E660A3EB F5A781DE 323026EF 1B25BE3E 82AB22BA 5027FE5C AB8FE7FD 601B3168 2C42B8BC FD2D4A6B C08C5B8F

server read key
B83D8BD4 AE9BE933 AF3BC270 A49F6A15 DC6F906D CCEA7E05 FB83E6AB 51E29BCC
server read MAC secret
8A6825F7 E9F38F40 66A0B95B 39831FAF 4394D119 7E01F55B 10DC2C90 7D2FF862
server read IV
601B3168 2C42B8BC

client <- server:

header type
14 (change cipher spec)
major version
03
minor version
01
Length
01
message type
01 (change cipher spec)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

server internals:

server write key
3077B22B E660A3EB F5A781DE 323026EF 1B25BE3E 82AB22BA 5027FE5C AB8FE7FD
server write MAC secret
6DBF6CDE 5F5DEA46 9076782D F559AE47 122299BF BB471CB1 3FF7FE1E 34F174C1
server write IV
FD2D4A6B C08C5B8F
hash(handshake messages)
D65CC82D 4534E592 9CAD6B7A 8E2C4853 BFA0CDBB 320677FA 399C88FC 3769CF27
finished label
server finished
verify data = PRF_GOSTR3411(hash(master secret), finished label, hash(handshake messages))

```
A5433E5F FB287C51 DFEF7072


message type
14 (finished)
length
00000C
verify data
A5433E5F FB287C51 DFEF7072

client <- server:

write_sequence
00000000 00000000
header
header type
16 (handshake)
major version
03
minor version
01
Length
0010
message encrypted on server write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
2278F6C2 FE52F507 32C8059A 6759A97E
MAC on server write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
C4BB94D6

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

client read key
3077B22B E660A3EB F5A781DE 323026EF 1B25BE3E 82AB22BA 5027FE5C AB8FE7FD
client read MAC secret
6DBF6CDE 5F5DEA46 9076782D F559AE47 122299BF BB471CB1 3FF7FE1E 34F174C1
client read IV
FD2D4A6B C08C5B8F

client message

04030201 08070605 0C0B0A09 100F0E0D 14131211 18171615 1C1B1A19 201F1E1D
24232221 28272625 2C2B2A29 302F2E2D 34333231 38373635 3C3B3A39 403F3E3D
44434241 48474645 4C4B4A49 504F4E4D 54535251 58575655 5C5B5A59 605F5E5D
64636261 68676665 6C6B6A69 706F6E6D 74737271 78777675 7C7B7A79 807F7E7D
84838281 88878685 8C8B8A89 908F8E8D 94939291 98979695 9C9B9A99 A09F9E9D
A4A3A2A1 A8A7A6A5 ACABAAA9 B0AFAEAD B4B3B2B1 B8B7B6B5 BCBBBAB9 C0BFBEBD
C4C3C2C1 C8C7C6C5 CCCBCAC9 D0CFCECD D4D3D2D1 D8D7D6D5 DCDBDAD9 E0DFDEDD
E4E3E2E1 E8E7E6E5 ECEBEAE9 F0EFEEED F4F3F2F1 F8F7F6F5 FCFBFAF9 03020100
07060504 0B0A0908 0F0E0D0C 13121110 17161514 1B1A1918 1F1E1D1C 23222120
27262524 2B2A2928 2F2E2D2C 33323130 37363534 3B3A3938 3F3E3D3C 43424140
47464544 4B4A4948 4F4E4D4C 53525150 57565554 5B5A5958 5F5E5D5C 63626160
67666564 6B6A6968 6F6E6D6C 73727170 77767574 7B7A7978 7F7E7D7C 83828180
87868584 8B8A8988 8F8E8D8C 93929190 97969594 9B9A9998 9F9E9D9C A3A2A1A0
```

A7A6A5A4 ABAAA9A8 AFAEADAC B3B2B1B0 B7B6B5B4 BBBAB9B8 BFBEBDBC C3C2C1C0
C7C6C5C4 CBCAC9C8 CFCECDCC D3D2D1D0 D7D6D5D4 DBDAD9D8 DFDEDDDC E3E2E1E0
E7E6E5E4 EBEAE9E8 EFEEEDEC F3F2F1F0 F7F6F5F4 FBFAF9F8 020100FC 06050403
0A090807 0E0D0C0B 1211100F 16151413 1A191817 1E1D1C1B 2221201F 26252423
2A292827 2E2D2C2B 3231302F 36353433 3A393837 3E3D3C3B 4241403F 46454443
4A494847 4E4D4C4B 5251504F 56555453 5A595857 5E5D5C5B 6261605F 66656463
6A696867 6E6D6C6B 7271706F 76757473 7A797877 7E7D7C7B 8281807F 86858483
8A898887 8E8D8C8B 9291908F 96959493 9A999897 9E9D9C9B A2A1A09F A6A5A4A3
AAA9A8A7 AEADACAB B2B1B0AF B6B5B4B3 BAB9B8B7 BEBDBCBB C2C1C0BF C6C5C4C3
CAC9C8C7 CECDCCCB D2D1D0CF D6D5D4D3 DAD9D8D7 DEDDDCDB E2E1E0DF E6E5E4E3
EAE9E8E7 EEEDECEB F2F1F0EF F6F5F4F3 FAF9F8F7 0100FCFB 05040302 09080706
0D0C0B0A 11100F0E 15141312 19181716 1D1C1B1A 21201F1E 25242322 29282726
2D2C2B2A 31302F2E 35343332 39383736 3D3C3B3A 41403F3E 45444342 49484746
4D4C4B4A 51504F4E 55545352 59585756 5D5C5B5A 61605F5E 65646362 69686766
6D6C6B6A 71706F6E 75747372 79787776 7D7C7B7A 81807F7E 85848382 89888786
8D8C8B8A 91908F8E 95949392 99989796 9D9C9B9A A1A09F9E A5A4A3A2 A9A8A7A6
ADACABAA B1B0AFAE B5B4B3B2 B9B8B7B6 BDBCBBBA C1C0BFBE C5C4C3C2 C9C8C7C6
CDCCCBCA D1D0CFCE D5D4D3D2 D9D8D7D6 DDDCDBDA E1E0DFDE E5E4E3E2 E9E8E7E6
EDECEBEA F1F0EFEE F5F4F3F2 F9F8F7F6 00FCFBFA 04030201 080706

client -> server:

write_sequence
00000000 00000001
header type
17 (application data)
major version
03
minor version
01
Length
03FB
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
B105F95F 98A7E3B5 B9C9FA1D 6CECC918 118135C8 3F544257 2D6249EA C7B4C2DE
16E89EEE 9627378B 77CE9CDF 9AE08748 834C28C5 83D8F831 630036AD 0F45716D
CF40AE65 F370EF6A 8352197C 1C831D15 6DCF82CB F63EC447 A1FD7B9B AE16FC20
ACEB573E 8D74C088 02D39923 00A55B4D 0B0966F9 255AF13B 45C8D429 3AE34268
7C88A87B 8076EBB6 B68E4BA3 664538AA 76E4BFBE 3DA20CB2 E2749B3B 71E1CB9E
02AB330A 84FEABC7 7563E4BE 34F918EC 238D9479 7661B96A C2FBE919 4C68971C
F03E11D2 5F32DB37 FF8D7636 1C9C4C13 01AB3B33 595619BB 2772B3B7 6239F653
E8FB98BC CA533DC9 3C9A6AC3 3FF8C5BC E359573B C0349389 D08145C6 F7A6DBF4
DFDDC42C A822148C 437DDA5E 28275A31 A9277739 08BFBDDC 9294130F 40E36D72
22A2ACA1 17F57FB5 CBC4553D A0BE1EF0 F59D1753 9967C9F0 B1A2DEC3 D29F0E55
2612CA9C 8CF08BA9 C15D3C44 7013DC7B E70085CC 5F7BFB00 BB743013 4330BB51
AF31C999 90AADEA9 AEFF1297 B89E2870 04233A87 44994E7D 493D84C6 E3CF3A50
5EC220C3 74050820 53E107F2 B34C38CA FF012FF5 DFD541E6 1F145230 C4AD73E1
7439F6C5 1E718C59 9A1504C5 F2209CEA CDBA7532 DE58A62F F8C215BE 04AEB7FB
0AA9B456 6616B9BA 8E082D4B BB0C44D7 5CCC28A6 1CCAE9CC 34D491E5 4B652B55
7CA7CAFB 9AE40199 AD963AE0 19595CE4 30FA2B78 B9F0A58F 974ED710 34346C28
4C6C5561 2111B6E2 8B481E6D 8504926C 6671810B D82FFF80 18BF728D A63A4AE7
8A9F16F6 500F6128 0B4501C6 7DACBD33 81FD7C98 6EA2683B B63F9CD9 2F59AD51
B732F1EC D34E594D C253DF3C 29F0A9B3 80EB50AA 35756475 28C1100E 2D6B6443
3826DB38 3EDE2819 A6D3E1E5 67401D7C C5B2E5CC 1ACEBB20 7BC76C7B 81E58A2C
FDE5C2D4 8D7D2021 AEA28287 9E01180C 32391F84 38BEF35A 16625049 34A6973A
F36A3E2C 971A37DE EF695B70 FF896284 7D358CFB A4978042 F38A88E6 786274F0

```
561F4E25 F5D5D1CA 4F72BE1A 02C38695 199305FF 167BEFB5 26E6A715 627F35F0
B41E7DC7 9E701697 014F6A8E C9A3CFA1 4FB8F623 98DF12B5 9E6C51CA 25759868
DE716AC4 D0281D3D 6615EB34 351C05BB 83B0ADCC 29CDEF0B 3F53F738 1747E33A
1BD5BA19 3952A165 D4CFAB66 B99ED653 B89E7A09 BFBD1E03 77288A5B 8C3CEC5A
83F5ECD1 1B66E597 EE8DAB63 EA85BA51 0F8F97B4 AD1F5949 E6A5863C 01E2E42D
ED2CD5C8 A447B0CC 4233E5A5 9B6C656D 80A3B70E B3C3BA56 203915E3 0271A866
905CD50A F7F52C31 BC808642 75CB3C15 7159AF31 4BB74EB8 148E7FE6 999F29AF
DCADACA1 7E794542 D5C7C134 B3AB6528 EC07CEF2 3774F2AA 37420FAF D9443574
4AB5CE9C 0363B02C DBCF6E89 5521D820 4840D83B 6BD3618B 36F2DECF 40D565E6
E22BC5A4 17F0BDCD 408D47B8 626A46B0 DF53C318 99B12730 3524CD
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
88AF2B49

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

client message

0403

client -> server:

write_sequence
00000000 00000002
header type
17 (application data)
major version
03
minor version
01
Length
0002
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
6C11
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
2860BC29
```

A.2. TLS 1.0 аутентификация клиента с ключом 256 бит и сервера с ключом 256 бит

```
client -> server:

header type
16 (handshake)
major version
```

```
03
minor version
01
Length
004E

message type
01 (client hello)
length
00004A
TLS VERSION
                  major version
                  03
                  minor version
                  01
client random
52E78F3A CEC5D045 D7D96B88 1D5B1880 BC3242CC CC452503 F000C728 3766B7FD
session id length
00
session id

ciphersuite length
0004
CipherSuite
0081                TLS_CIPHER_2001
FF85                TLS_CIPHER_2012
compression methods
                  length
                  01
                  compression method
                  00
extensions
  extensions length
  001D
  renegotiation_info (FF01)
  length
  0001
  Renegotiation Info extension
  00
  server name (0000)
  length
  0014
  server name list length
  0012
  server name type
  00
  server name length
  000F
  server name
  746C7363 6F6E665F 73727635 313265

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

client <- server:

header type
```

```
16 (handshake)
major version
03
minor version
01
Length
032F

message type
02 (server hello)
length
000046
TLS VERSION
                  major version
                  03
                  minor version
                  01
server random
52E78F3A 621D00F7 DFE637A4 179899F8 1570C14B B47D450B 53A474DC 7E4FFF19
session id length
20
session id
85FD2947 6E8E968D E34347F6 7736EFF1 12E3E149 3F7F1CA8 283BBE03 363A9F3A
ciphersuite
FF85                TLS_CIPHER_2012
compression method
00
extensions

message type
0B (certificate)
length
0002DD
server certificate chain
0002DA00 02D73082 02D33082 0282A003 02010202 0A427E80 21000000 8B927530
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 385A170D 32343031 32383131
30343238 5A304731 18301606 03550403 0C0F746C 73636F6E 665F7372 76353132
65312B30 2906092A 864886F7 0D010901 161C746C 73636F6E 665F7372 76353132
65406372 7970746F 70726F2E 72753066 301F0608 2A850307 01010101 30130607
2A850302 02240006 082A8503 07010102 02034300 0440442B 2744A488 9B1F456F
A23BC840 9FC272E8 F36A65EB 2548038B B0E10A8A FE2CFCB7 5AAAD185 D2F18B5A
ED28F747 B3C72D5C C5BA870A 2CC76F57 5A9BC7EF 25E7A382 01563082 01523013
0603551D 25040C30 0A06082B 06010505 07030130 0B060355 1D0F0404 03020430
301D0603 551D0E04 1604146B BF36F2E8 0DEB1254 4478CE0B 55CC7C84 E1B83430
1F060355 1D230418 30168014 9E03F0B8 9CFC60DC 8A181EE8 00DFA85B 32CD7376
303F0603 551D1F04 38303630 34A032A0 30862E68 7474703A 2F2F766D 2D746573
742D6361 2E63702E 72752F43 65727445 6E726F6C 6C2F7465 73742D63 612E6372
6C3081AC 06082B06 01050507 01010481 9F30819C 304B0608 2B060105 05073002
863F6874 74703A2F 2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E
726F6C6C 2F766D2D 74657374 2D63612E 63702E72 755F7465 73742D63 612E6372
74304D06 082B0601 05050730 02864166 696C653A 2F2F5C5C 766D2D74 6573742D
63612E63 702E7275 5C436572 74456E72 6F6C6C5C 766D2D74 6573742D 63612E63
702E7275 5F746573 742D6361 2E637274 30080606 2A850302 02030341 000FDCCB
2BEDB244 BB93D103 A9F058BA 46474261 300D87B8 6AD845AA B22CD64A B057AD90
```

```
FF5C09AC 218E34F5 B9EFF672 3C5FB110 BEE14933 65D588D4 C8B8098C 76

message type
0D (certificate request)
length
000046
certificate request
  certificate types length
  03
  certificate_types
  16   gostr34102001
  EE   gostr34102012_256
  EF   gostr34102012_512
  certificate authorities length
  0040
  certificate authorities
  003E303C 31123010 060A0992 268993F2 2C640119 16027275 31123010 060A0992
  268993F2 2C640119 16026370 31123010 06035504 03130974 6573742D 6D736361

message type
0E (server hello done)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

client certificate chain
0002DA00 02D73082 02D33082 0282A003 02010202 0A427E82 35000000 8B927630
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 395A170D 32343031 32383131
30343239 5A304731 18301606 03550403 0C0F746C 73636F6E 665F636C 6E353132
65312B30 2906092A 864886F7 0D010901 161C746C 73636F6E 665F636C 6E353132
65406372 7970746F 70726F2E 72753066 301F0608 2A850307 01010101 30130607
2A850302 02240006 082A8503 07010102 02034300 0440EBCE 8AB9C7C8 400ED94A
C055529E DA2B3110 2615BD63 225227E5 2FF8D9E8 6E6F7D1F BA5E292D EECED28B
AB6F8B82 D34FB71B 24573838 D279E9DB F1D9AC71 1AD9A382 01563082 01523013
0603551D 25040C30 0A06082B 06010505 07030230 0B060355 1D0F0404 03020430
301D0603 551D0E04 16041483 51A75EF8 F9450E71 DC49382D 2D3BD3F0 0E5ABF30
1F060355 1D230418 30168014 9E03F0B8 9CFC60DC 8A181EE8 00DFA85B 32CD7376
303F0603 551D1F04 38303630 34A032A0 30862E68 7474703A 2F2F766D 2D746573
742D6361 2E63702E 72752F43 65727445 6E726F6C 6C2F7465 73742D63 612E6372
6C3081AC 06082B06 01050507 01010481 9F30819C 304B0608 2B060105 05073002
863F6874 74703A2F 2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E
726F6C6C 2F766D2D 74657374 2D63612E 63702E72 755F7465 73742D63 612E6372
74304D06 082B0601 05050730 02864166 696C653A 2F2F5C5C 766D2D74 6573742D
63612E63 702E7275 5C436572 74456E72 6F6C6C5C 766D2D74 6573742D 63612E63
702E7275 5F746573 742D6361 2E637274 30080606 2A850302 02030341 00850B51
588B2C0E 4C9AB975 778130DF E3F6D654 D7326F90 370A3C38 A2470D5C 8CB91E5B
580BA724 418CC995 7A3BF2F3 1DA5B8DB 3A0091A0 EE150FCB CFBEB2EB 2B

premastersecret
9F82C8A2 D3A235C9 DEBE5E34 C1D5AE45 88B77B21 C3051BFD 3FAB5546 9D09C124
```

```
client private key
E0C6D1EB 9AE63CF0 E07CA8C0 B6A04080 FBE89CCB B1C84997 8620D973 26696FC8
server public key blob header
06200100 492E0000 4D414731 00020000 30130607 2A850302 02240006 082A8503
07010102 02442B27
server public key
442B2744 A4889B1F 456FA23B C8409FC2 72E8F36A 65EB2548 038BB0E1 0A8AFE2C
FCB75AAA D185D2F1 8B5AED28 F747B3C7 2D5CC5BA 870A2CC7 6F575A9B C7EF25E7
hash(client random, server random)
50D55A4B B4D33355 987586D0 0F9CA5BA EB6CCD90 F64F5459 EBD90D23 DC40BDDE
ukm
50D55A4B B4D33355
Inner Point
50E03566 E44AC879 46640AF2 F5A286A7 2F9DF455 42BB60CB 152CE8EA 97BAF55D
4334089D F4E0FAF9 44D63A59 FABD132C 111D7924 AE96E25B 324D2F26 826D73AA
VKO result
2308FEBF 49F951F9 55650450 D90A4182 E12A48EF A932E8A0 214FBF8B 198DCE79
diversified key
7577FC0A 004E1801 9961BD3C 08C1E160 8BA355E3 02EDE8CA C627C6AA 86BC0026
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in ECB mode
                  83BE410A 078B3130 50F47E89 124DE9DC EC591B77 0D0AB638
712E6F84 12A874BA
                  MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                  6EE7685F

client key exchange
30433041 30280420 83BE410A 078B3130 50F47E89 124DE9DC EC591B77 0D0AB638
712E6F84 12A874BA 04046EE7 685FA015 06092A85 03070102 05010104 0850D55A
4BB4D333 55

client -> server:

header type
16 (handshake)
major version
03
minor version
01
length
032A

message type
0B (certificate)
length
0002DD
client certificate chain
0002DA00 02D73082 02D33082 0282A003 02010202 0A427E82 35000000 8B927630
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 395A170D 32343031 32383131
30343239 5A304731 18301606 03550403 0C0F746C 73636F6E 665F636C 6E353132
65312B30 2906092A 864886F7 0D010901 161C746C 73636F6E 665F636C 6E353132
65406372 7970746F 70726F2E 72753066 301F0608 2A850307 01010101 30130607
2A850302 02240006 082A8503 07010102 02034300 0440EBCE 8AB9C7C8 400ED94A
```

```
C055529E DA2B3110 2615BD63 225227E5 2FF8D9E8 6E6F7D1F BA5E292D EECED28B
AB6F8B82 D34FB71B 24573838 D279E9DB F1D9AC71 1AD9A382 01563082 01523013
0603551D 25040C30 0A06082B 06010505 07030230 0B060355 1D0F0404 03020430
301D0603 551D0E04 16041483 51A75EF8 F9450E71 DC49382D 2D3BD3F0 0E5ABF30
1F060355 1D230418 30168014 9E03F0B8 9CFC60DC 8A181EE8 00DFA85B 32CD7376
303F0603 551D1F04 38303630 34A032A0 30862E68 7474703A 2F2F766D 2D746573
742D6361 2E63702E 72752F43 65727445 6E726F6C 6C2F7465 73742D63 612E6372
6C3081AC 06082B06 01050507 01010481 9F30819C 304B0608 2B060105 05073002
863F6874 74703A2F 2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E
726F6C6C 2F766D2D 74657374 2D63612E 63702E72 755F7465 73742D63 612E6372
74304D06 082B0601 05050730 02864166 696C653A 2F2F5C5C 766D2D74 6573742D
63612E63 702E7275 5C436572 74456E72 6F6C6C5C 766D2D74 6573742D 63612E63
702E7275 5F746573 742D6361 2E637274 30080606 2A850302 02030341 00850B51
588B2C0E 4C9AB975 778130DF E3F6D654 D7326F90 370A3C38 A2470D5C 8CB91E5B
580BA724 418CC995 7A3BF2F3 1DA5B8DB 3A0091A0 EE150FCB CFBEB2EB 2B

message type
10 (client key exchange)
length
000045
client key exchange
30433041 30280420 83BE410A 078B3130 50F47E89 124DE9DC EC591B77 0D0AB638
712E6F84 12A874BA 04046EE7 685FA015 06092A85 03070102 05010104 0850D55A
4BB4D333 55

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


client -> server:

header
header type
14 (change cipher spec)
major version
03
minor version
01
Length
0001
message type
01 (change cipher spec)
length
000000

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


client internals:

master secret = PRF_GOSTR3411(premastersecret, “master secret”, client
random, server random)
57380114 BB1FA165 D40DF7CF C56375FE F23D80FF 06000A53 FBA6D596 50C31B11
98B2808B 2E2A623C 4B546B26 0428DBA2
hash(master secret)
1386F6F2 946BE70C 02AA1777 BF8A862F 8CB15046 FC9E35EA F16D4D09 5464D5FE
```

key block = PRF_GOSTR3411(hash(master secret), “key expansion”, server random, client random)
A5E1F809 F154CF9C DE7C3300 398D1EAF 1CDE3F35 B1572301 AA423DFA CBD60936
1563C9CD FEBC7DFF 42AD43DA 3322F0D3 5F52D230 27737CF6 8AE46510 F2FDC59B
4A2A9D2C 4FAF9BFE 05D2A004 FC245911 2D66AC99 9CF6BE7D 333FE44F 213C3F86
5ACDE82E 844CFE5C 2141C51D 16C96784 DCBEAB64 FC952146 575CFA3A EB4EC8CB
47AA2337 EB8BFC56 400CC991 58A3E03E

client write key
4A2A9D2C 4FAF9BFE 05D2A004 FC245911 2D66AC99 9CF6BE7D 333FE44F 213C3F86
client write MAC secret
A5E1F809 F154CF9C DE7C3300 398D1EAF 1CDE3F35 B1572301 AA423DFA CBD60936
client write IV
47AA2337 EB8BFC56
hash(handshake messages)
34E7861C 1DD87B19 0FCE8E5E 44983F1C DDF7B3F6 49CDAADF CBF5E045 2F2D73BC
finished label
client finished
verify data = PRF_GOSTR3411(hash(master secret), finished label, hash(handshake messages))
B97A54E7 C455B60A F9264B1B

message type
14 (finished)
length
00000C
verify data
B97A54E7 C455B60A F9264B1B

client -> server:

write_sequence
00000000 00000000
header type
16 (handshake)
major version
03
minor version
01
length
0010
message encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in CNT mode
14FFA776 46B7F3A4 8F9A40F3 BFE6C0A6
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z)
2F1FC718

>>

server internals:

server private key
836E71F6 3FF7D8B1 5117ABC9 B9730197 1352D2C3 392BD09F 828CE530 502C8FF8

```
client public key blob header
06200100 492E0000 4D414731 00020000 30130607 2A850302 02240006 082A8503
07010102 02EBCE8A
client public key
EBCE8AB9 C7C8400E D94AC055 529EDA2B 31102615 BD632252 27E52FF8 D9E86E6F
7D1FBA5E 292DEECE D28BAB6F 8B82D34F B71B2457 3838D279 E9DBF1D9 AC711AD9
hash(client random, server random)
50D55A4B B4D33355 987586D0 0F9CA5BA EB6CCD90 F64F5459 EBD90D23 DC40BDDE
ukm
50D55A4B B4D33355
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1(id-tc26-gost-28147-param-Z) in ECB mode
                  83BE410A 078B3130 50F47E89 124DE9DC EC591B77 0D0AB638
712E6F84 12A874BA
                  MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                  6EE7685F
Inner Point
50E03566 E44AC879 46640AF2 F5A286A7 2F9DF455 42BB60CB 152CE8EA 97BAF55D
4334089D F4E0FAF9 44D63A59 FABD132C 111D7924 AE96E25B 324D2F26 826D73AA
VKO result
2308FEBF 49F951F9 55650450 D90A4182 E12A48EF A932E8A0 214FBF8B 198DCE79
diversified key
7577FC0A 004E1801 9961BD3C 08C1E160 8BA355E3 02EDE8CA C627C6AA 86BC0026
premastersecret
9F82C8A2 D3A235C9 DEBE5E34 C1D5AE45 88B77B21 C3051BFD 3FAB5546 9D09C124

master secret = PRF_GOSTR3411(premastersecret, “master secret”, client
random, server random)
57380114 BB1FA165 D40DF7CF C56375FE F23D80FF 06000A53 FBA6D596 50C31B11
98B2808B 2E2A623C 4B546B26 0428DBA2
hash(master secret)
1386F6F2 946BE70C 02AA1777 BF8A862F 8CB15046 FC9E35EA F16D4D09 5464D5FE
key_block = PRF_GOSTR3411(hash(master secret), “key expansion”, server
random, client random)
A5E1F809 F154CF9C DE7C3300 398D1EAF 1CDE3F35 B1572301 AA423DFA CBD60936
1563C9CD FEBC7DFF 42AD43DA 3322F0D3 5F52D230 27737CF6 8AE46510 F2FDC59B
4A2A9D2C 4FAF9BFE 05D2A004 FC245911 2D66AC99 9CF6BE7D 333FE44F 213C3F86
5ACDE82E 844CFE5C 2141C51D 16C96784 DCBEAB64 FC952146 575CFA3A EB4EC8CB
47AA2337 EB8BFC56 400CC991 58A3E03E

server read key
4A2A9D2C 4FAF9BFE 05D2A004 FC245911 2D66AC99 9CF6BE7D 333FE44F 213C3F86
server read MAC secret
A5E1F809 F154CF9C DE7C3300 398D1EAF 1CDE3F35 B1572301 AA423DFA CBD60936
server read IV
47AA2337 EB8BFC56

client <- server:

header
header type
14 (change cipher spec)
major version
03
minor version
```

```
01
length
0001
message type
01 (change cipher spec)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

server internals:

server write key
5ACDE82E 844CFE5C 2141C51D 16C96784 DCBEAB64 FC952146 575CFA3A EB4EC8CB
server write MAC secret
1563C9CD FEBC7DFF 42AD43DA 3322F0D3 5F52D230 27737CF6 8AE46510 F2FDC59B
server write IV
400CC991 58A3E03E
hash(handshake messages)
7069FFC1 2895D4EB AD22872A 829A0378 DCD9903B EBC98D64 EABAE4F3 8E4B457A
finished label
server finished
verify data = PRF_GOSTR3411(hash(master secret), finished label,
hash(handshake messages))
E76E9632 26E2557C BC2C79FD


message type
14 (finished)
length
00000C
verify data
E76E9632 26E2557C BC2C79FD

client <- server:

write_sequence
00000000 00000000
header type
16 (handshake)
major version
03
minor version
01
Length
0010
message encrypted on server write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
7B694462 9AA0E9A7 3B0353AC 143CA782
MAC on server write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
A5193C36

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

client internals:

client read key
5ACDE82E 844CFE5C 2141C51D 16C96784 DCBEAB64 FC952146 575CFA3A EB4EC8CB
client read MAC secret
1563C9CD FEBC7DFF 42AD43DA 3322F0D3 5F52D230 27737CF6 8AE46510 F2FDC59B
client read IV
400CC991 58A3E03E

Client message

04030201 08070605 0C0B0A09 100F0E0D 14131211 18171615 1C1B1A19 201F1E1D
24232221 28272625 2C2B2A29 302F2E2D 34333231 38373635 3C3B3A39 403F3E3D
44434241 48474645 4C4B4A49 504F4E4D 54535251 58575655 5C5B5A59 605F5E5D
64636261 68676665 6C6B6A69 706F6E6D 74737271 78777675 7C7B7A79 807F7E7D
84838281 88878685 8C8B8A89 908F8E8D 94939291 98979695 9C9B9A99 A09F9E9D
A4A3A2A1 A8A7A6A5 ACABAAA9 B0AFAEAD B4B3B2B1 B8B7B6B5 BCBBBAB9 C0BFBEBD
C4C3C2C1 C8C7C6C5 CCCBCAC9 D0CFCECD D4D3D2D1 D8D7D6D5 DCDBDAD9 E0DFDEDD
E4E3E2E1 E8E7E6E5 ECEBEAE9 F0EFEEED F4F3F2F1 F8F7F6F5 FCFBFAF9 03020100
07060504 0B0A0908 0F0E0D0C 13121110 17161514 1B1A1918 1F1E1D1C 23222120
27262524 2B2A2928 2F2E2D2C 33323130 37363534 3B3A3938 3F3E3D3C 43424140
47464544 4B4A4948 4F4E4D4C 53525150 57565554 5B5A5958 5F5E5D5C 63626160
67666564 6B6A6968 6F6E6D6C 73727170 77767574 7B7A7978 7F7E7D7C 83828180
87868584 8B8A8988 8F8E8D8C 93929190 97969594 9B9A9998 9F9E9D9C A3A2A1A0
A7A6A5A4 ABAAA9A8 AFAEADAC B3B2B1B0 B7B6B5B4 BBBAB9B8 BFBEBDBC C3C2C1C0
C7C6C5C4 CBCAC9C8 CFCECDCC D3D2D1D0 D7D6D5D4 DBDAD9D8 DFDEDDDC E3E2E1E0
E7E6E5E4 EBEAE9E8 EFEEEDEC F3F2F1F0 F7F6F5F4 FBFAF9F8 020100FC 06050403
0A090807 0E0D0C0B 1211100F 16151413 1A191817 1E1D1C1B 2221201F 26252423
2A292827 2E2D2C2B 3231302F 36353433 3A393837 3E3D3C3B 4241403F 46454443
4A494847 4E4D4C4B 5251504F 56555453 5A595857 5E5D5C5B 6261605F 66656463
6A696867 6E6D6C6B 7271706F 76757473 7A797877 7E7D7C7B 8281807F 86858483
8A898887 8E8D8C8B 9291908F 96959493 9A999897 9E9D9C9B A2A1A09F A6A5A4A3
AAA9A8A7 AEADACAB B2B1B0AF B6B5B4B3 BAB9B8B7 BEBDBCBB C2C1C0BF C6C5C4C3
CAC9C8C7 CECDCCCB D2D1D0CF D6D5D4D3 DAD9D8D7 DEDDDCDB E2E1E0DF E6E5E4E3
EAE9E8E7 EEEDECEB F2F1F0EF F6F5F4F3 FAF9F8F7 0100FCFB 05040302 09080706
0D0C0B0A 11100F0E 15141312 19181716 1D1C1B1A 21201F1E 25242322 29282726
2D2C2B2A 31302F2E 35343332 39383736 3D3C3B3A 41403F3E 45444342 49484746
4D4C4B4A 51504F4E 55545352 59585756 5D5C5B5A 61605F5E 65646362 69686766
6D6C6B6A 71706F6E 75747372 79787776 7D7C7B7A 81807F7E 85848382 89888786
8D8C8B8A 91908F8E 95949392 99989796 9D9C9B9A A1A09F9E A5A4A3A2 A9A8A7A6
ADACABAA B1B0AFAE B5B4B3B2 B9B8B7B6 BDBCBBBA C1C0BFBE C5C4C3C2 C9C8C7C6
CDCCCBCA D1D0CFCE D5D4D3D2 D9D8D7D6 DDDCDBDA E1E0DFDE E5E4E3E2 E9E8E7E6
EDECEBEA F1F0EFEE F5F4F3F2 F9F8F7F6 00FCFBFA 04030201 080706

client -> server:

write_sequence
00000000 00000001
header type
17 (application data)
major version
03
minor version
01
length
03FB

data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in CNT mode
4B2FBD4A ED27ADDD CF1B1436 DEAC8AFB B60E88BD D5BAAF94 FB2CADAF B3BC74B5
EB482B1D D16AEE6E 3FB3CB7E CCF93BB2 05C7CD95 47A93D49 7E614FFB FF2D3B0A
C9BDCF96 AB759A14 59132DF6 A34C2B91 58932428 3F90EBDF 2887F469 247FC08F
61DB285B D533DAF3 090C35E4 5E486286 286C0E6E 85968AF4 391C9EBD BF9A28D9
9823A770 084341BD B520641A EBAE283D 09655AE8 793B142F 07DEBA3C EC259804
1D887E44 E22F9D48 909A6E06 2F329C62 B57F7D25 420ACD21 1F427CD3 C2265E62
C1EAC566 F703B6CB 912AF8E8 28F177C0 296E5060 1AFB9673 1BF77EEC 4843AFC2
0713651E C375985F CA6CF055 75FABA87 D861C8D6 AE43637F 9DDDFB3D A77717ED
4D371800 9730256D 73618E7B 8473E52A 0809378F 24884C0A 9F3B9D63 31A14F6B
66FEB16B 0CB770BD C7B14C63 92D33F84 F6A4088C 272969FC D83D2668 A8364312
CDC19766 A9730F70 789D4D6D 506010F6 94E535D9 45F88B46 9707F95A 8C0FCE77
D181ADC3 884E02A6 B24C096A ADD99A86 526906E4 74F7C624 79043371 E7281A3C
878AFA76 84987B08 4D3D0CBF F738D4B4 6B02C3EA 07864CCF CAB35DBD 6977471C
DEB359D3 BA411EB1 426AFC0F 87D60B00 11E3CD3C 3158A757 3CAF6825 5068594D
F99348C2 58538FD4 D922923B B65AC529 E7AC084E 9B959016 4DB5E37E 1C21D31A
F7456D0E C84D852F 9796161A A9C929CC 2DEE6860 747AACDA 2A1F2D41 7F1344C2
B9CF04C2 8DE629FD FB6F2834 3E62BC0A 5132DC5B 0844813B E3740B81 A5C985B9
71DEE52B 3A3C31E5 21399416 DE769BF8 79E49A42 72B62AF5 9BFB76F1 30D92D56
9956CB0A DE1EFA41 BE9265EC 7768E568 5EE9DCF0 92647DD6 CE92535B 54B9E3E2
37339CA5 9AA38AAA B5D27D1A C02397B0 20367B6A 58547E09 6D4B2A55 ECFA1B37
869F063C 56303A91 F007E4E8 6813A960 8B304CF3 6051A03F E5BF57A0 D0AEC2E2
0EFBF432 3659022C 7DC453C1 7BBAC218 27D39B2F 90F258C9 D84A1E36 4B3D4635
FD44280C AA1B4A6B F0390C57 504B38C5 4E6D9482 526A7D3D 91FD3D2B 1C05FB34
59592FD1 578225C5 1B145EDC A6A5BE60 7E23F222 D0BA5090 36E97AB2 1059F04A
032C7F74 06C1BAB7 9369353C AECBDDA0 3AFA7E59 2BA3CCFB 80E493C8 F94C96EE
22A74308 1AF4D1CD A34F8FE0 5D984DBE 51C68918 E8CE4E07 1FF7F510 6093D2A9
0276A645 B5D05CC0 1EEEDA1C 80C2967C A4C66C76 2820C85D FCD8B5D0 CD60A57E
F32E5753 24CB8A96 2539A149 CA4C2643 42113F52 D13907C0 2A6B4580 92954DC3
E460CD55 C48FA290 3A934F96 B81D6C8A 4CDE5410 54D1E756 423D921C 00911042
FF3E9168 8B330947 A1848C0B 22721593 956B7C56 BA18CD03 CDC9F2F7 6C4390D1
392D8363 1E1B425C A40E3369 D744C671 353EFD55 1C7AB779 4BAF417C D63D1C0D
1FD19A72 0952A276 6FE61518 E4E652F3 A5E55C6A 379F81B6 41E480
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z)
6904C610

>>

Client message

0403

client -> server:

write_sequence
00000000 00000002
header type
17 (application data)
major version
03
minor version
01
Length

```
0002
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
F835
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
E1236D00
```

A.3. TLS 1.0 аутентификация клиента с ключом 256 бит и сервера с ключом 512 бит

```
client -> server:

header type
16 (handshake)
major version
03
minor version
01
Length
004F

message type
01 (client hello)
length
00004B
TLS VERSION
                  major version
                  03
                  minor version
                  01
client random
52E78EFE 6E681041 EC766E3D E0B54F24 3AE4C48C 5CE47EEE 84FBDA38 F5C50D64
session id length
00
session id

ciphersuite length
0004
ciphersuite
0081               TLS_CIPHER_2001
FF85               TLS_CIPHER_2012
compression methods
                  length
                  01
                  compression method
                  00
extensions
  extensions length
  001E
  renegotiation info (FF01)
  length
  0001
  Renegotiation Info extension
  00
```

```
  server name (0000)
  length
  0015
  server name list length
  0013
  server name type
  00
  server name length
  0010
  server name
  746C7363 6F6E665F 73727631 30323465

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

client <- server:

header type
16 (handshake)
major version
03
minor version
01
Length
03C0

message type
02 (server hello)
length
000046
TLS VERSION
                  major version
                  03
                  minor version
                  01
server random
52E78EFE 1B11A86A CE9CF0CD 6D9E814E 5C025DF5 3361A984 A711C9D5 CE078CEE
session id length
20
session id
A7C31AF2 CCECAB7B 8E090DEB 2BFAD6C0 79F9B44D 3A8F0593 8DB21716 BC45E9CB
ciphersuite
FF85                TLS_CIPHER_2012
compression method
00
extensions

message type
0B (certificate)
length
000324
server certificate chain
00032100 031E3082 031A3082 02C9A003 02010202 0A427E7B CC000000 8B927330
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 375A170D 32343031 32383131
30343237 5A304931 19301706 03550403 0C10746C 73636F6E 665F7372 76313032
```

```
3465312C 302A0609 2A864886 F70D0109 01161D74 6C73636F 6E665F73 72763130
32346540 63727970 746F7072 6F2E7275 3081AA30 2106082A 85030701 01010230
1506092A 85030701 02010201 06082A85 03070101 02030381 84000481 80F0DBBD
44A22D19 AFCB22A0 CAD421A0 2E7930D5 C6E549C1 3BBF7D14 377C67CA E87D45E7
9E27E96D 631A0AA6 C71E6B35 3C66A023 62F9D43F C3F53DDF AB567CDF B92909DC
B62A9318 96ED1F1D 1655AC58 4DC8D674 5C51EA68 CAC8EBF4 9CAC305E FA642850
9799F30D 219A8407 827EB276 293E7BC1 AE68DCB9 39FAD9BF BCAD938C 84A38201
56308201 52301306 03551D25 040C300A 06082B06 01050507 0301300B 0603551D
0F040403 02043030 1D060355 1D0E0416 04141275 ECCDF8B0 38C7FD18 379C2C4E
B1ECCC93 2792301F 0603551D 23041830 1680149E 03F0B89C FC60DC8A 181EE800
DFA85B32 CD737630 3F060355 1D1F0438 30363034 A032A030 862E6874 74703A2F
2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E 726F6C6C 2F746573
742D6361 2E63726C 3081AC06 082B0601 05050701 0104819F 30819C30 4B06082B
06010505 07300286 3F687474 703A2F2F 766D2D74 6573742D 63612E63 702E7275
2F436572 74456E72 6F6C6C2F 766D2D74 6573742D 63612E63 702E7275 5F746573
742D6361 2E637274 304D0608 2B060105 05073002 86416669 6C653A2F 2F5C5C76
6D2D7465 73742D63 612E6370 2E72755C 43657274 456E726F 6C6C5C76 6D2D7465
73742D63 612E6370 2E72755F 74657374 2D63612E 63727430 0806062A 85030202
03034100 25D1D3FC E78525E7 6CE8CAC6 D511B9F4 47BA8471 6A1B235D DF9BE280
1C6E56D3 01E8909E 1E7DDAEA 5A897272 072C3AB3 F130205F 87298A74 74A4011B
E7543ABB

message type
0D (certificate request)
length
000046
certificate request
  certificate types length
  03
  certificate_types
  16   gostr34102001
  EE   gostr34102012_256
  EF   gostr34102012_512
  certificate authorities length
  0040
  certificate authorities
  003E303C 31123010 060A0992 268993F2 2C640119 16027275 31123010 060A0992
  268993F2 2C640119 16026370 31123010 06035504 03130974 6573742D 6D736361

message type
0E (server hello done)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

client certificate chain
0002DA00 02D73082 02D33082 0282A003 02010202 0A427E82 35000000 8B927630
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 395A170D 32343031 32383131
30343239 5A304731 18301606 03550403 0C0F746C 73636F6E 665F636C 6E353132
65312B30 2906092A 864886F7 0D010901 161C746C 73636F6E 665F636C 6E353132
```

```
65406372 7970746F 70726F2E 72753066 301F0608 2A850307 01010101 30130607
2A850302 02240006 082A8503 07010102 02034300 0440EBCE 8AB9C7C8 400ED94A
C055529E DA2B3110 2615BD63 225227E5 2FF8D9E8 6E6F7D1F BA5E292D EECED28B
AB6F8B82 D34FB71B 24573838 D279E9DB F1D9AC71 1AD9A382 01563082 01523013
0603551D 25040C30 0A06082B 06010505 07030230 0B060355 1D0F0404 03020430
301D0603 551D0E04 16041483 51A75EF8 F9450E71 DC49382D 2D3BD3F0 0E5ABF30
1F060355 1D230418 30168014 9E03F0B8 9CFC60DC 8A181EE8 00DFA85B 32CD7376
303F0603 551D1F04 38303630 34A032A0 30862E68 7474703A 2F2F766D 2D746573
742D6361 2E63702E 72752F43 65727445 6E726F6C 6C2F7465 73742D63 612E6372
6C3081AC 06082B06 01050507 01010481 9F30819C 304B0608 2B060105 05073002
863F6874 74703A2F 2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E
726F6C6C 2F766D2D 74657374 2D63612E 63702E72 755F7465 73742D63 612E6372
74304D06 082B0601 05050730 02864166 696C653A 2F2F5C5C 766D2D74 6573742D
63612E63 702E7275 5C436572 74456E72 6F6C6C5C 766D2D74 6573742D 63612E63
702E7275 5F746573 742D6361 2E637274 30080606 2A850302 02030341 00850B51
588B2C0E 4C9AB975 778130DF E3F6D654 D7326F90 370A3C38 A2470D5C 8CB91E5B
580BA724 418CC995 7A3BF2F3 1DA5B8DB 3A0091A0 EE150FCB CFBEB2EB 2B

premastersecret
26DBE1DA A8757A2F FD12E2BB 1ABA62CC A69C37B1 80C12B7D 8FEF63AC 17723A25
client private key
E0C6D1EB 9AE63CF0 E07CA8C0 B6A04080 FBE89CCB B1C84997 8620D973 26696FC8
client private key (ephemeral)
4CE22FCB 57E076BB B68E3231 C30D6B93 FA388247 78C7179C 4A668BF4 B9A0BA57
1D0EA2DA D4DD03A8 BAF18AEA 3FAE5E41 DFDA273C 4E63948D DC1A06F9 D61A869E
server public key blob header
06200100 3D2E0000 4D414731 00040000 30150609 2A850307 01020102 0106082A
85030701 010203F0
server public key
F0DBBD44 A22D19AF CB22A0CA D421A02E 7930D5C6 E549C13B BF7D1437 7C67CAE8
7D45E79E 27E96D63 1A0AA6C7 1E6B353C 66A02362 F9D43FC3 F53DDFAB 567CDFB9
2909DCB6 2A931896 ED1F1D16 55AC584D C8D6745C 51EA68CA C8EBF49C AC305EFA
64285097 99F30D21 9A840782 7EB27629 3E7BC1AE 68DCB939 FAD9BFBC AD938C84
hash(client random, server random)
F528F112 8286A80F 19405393 1267A151 17455680 C30C1600 84B400B3 867208B2
ukm
F528F112 8286A80F
Inner Point
02756997 5C3DEF17 6C9407B4 D26A87D0 35BAA977 74EE19D0 B7B37109 2BE9B3C7
9C9174A1 9371CD74 F4C86ECF 9BD5952D AE967D91 B44FB899 D0608B68 753F6604
81317270 F68976BD 893A9D6E FE942CF3 6A002385 5F76B986 C4FD8449 CFBC56D9
9F91E5C1 DD62778D FAAB3640 DDB4E7E0 4DEC3FDF CECBA04D 978CAB7C 7689E5EF
VKO result
8A2D3569 221F2B2B 3207450E 9D32E9D0 973ED97E 67E96D5B A06131DF 4DA75AA8
diversified key
D83FE5FA 27803F24 AB15153D 4CCDB351 343B6BE3 CCAAAA29 E2CCC38E CB771524
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in ECB mode
                  2B9733F1 F6EFEB45 30354151 19E46D3E 1798A037 488BE6B5
836CF8CF B81BB597
                  MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                  E2897619

client key exchange
3081F230 81EF3028 04202B97 33F1F6EF EB453035 415119E4 6D3E1798 A037488B
```

E6B5836C F8CFB81B B5970404 E2897619 A081C206 092A8503 07010205 0101A081
AA302106 082A8503 07010101 02301506 092A8503 07010201 02010608 2A850307
01010203 03818400 04818094 505C443B 6C2685C5 FD88888F 00177F56 2F28FEB2
6461389D 2BC70730 B94B903D 526103DA AF2F360B 47EEDCC4 BA07F733 D83D33AF
0CA81936 8C3C5F08 26A67D44 14BF92A2 4A89C784 1B81C101 674EDC77 1D092BEA
46ACD877 C60F7DA1 60B959A1 428A2F72 D2DDDE4B 741D79E5 9878F02E 12241798
1C67A557 4CEF3F48 9E679504 08F528F1 128286A8 0F
hash(handshake messages)
76DC62A9 89673B8D E1B4C947 600DDE62 6383CBB7 3A6BCC53 9D66F7B0 42AB654A
certificate verify
F17A142A 4D306C61 1C5FE211 055A40A1 18A3080F 2A82771F 9447E4C9 A5AEC9C6
4411AC5A BDBDBA1F 6FBD23CD 3AC0873C ED7B0C90 8CAFDB07 60E8B20E DEA72A9F

client -> server:

header type
16 (handshake)
major version
03
minor version
01
Length
041E

message type
0B (certificate)
length
02DD
client certificate chain
0002DA00 02D73082 02D33082 0282A003 02010202 0A427E82 35000000 8B927630
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 395A170D 32343031 32383131
30343239 5A304731 18301606 03550403 0C0F746C 73636F6E 665F636C 6E353132
65312B30 2906092A 864886F7 0D010901 161C746C 73636F6E 665F636C 6E353132
65406372 7970746F 70726F2E 72753066 301F0608 2A850307 01010101 30130607
2A850302 02240006 082A8503 07010102 02034300 0440EBCE 8AB9C7C8 400ED94A
C055529E DA2B3110 2615BD63 225227E5 2FF8D9E8 6E6F7D1F BA5E292D EECED28B
AB6F8B82 D34FB71B 24573838 D279E9DB F1D9AC71 1AD9A382 01563082 01523013
0603551D 25040C30 0A06082B 06010505 07030230 0B060355 1D0F0404 03020430
301D0603 551D0E04 16041483 51A75EF8 F9450E71 DC49382D 2D3BD3F0 0E5ABF30
1F060355 1D230418 30168014 9E03F0B8 9CFC60DC 8A181EE8 00DFA85B 32CD7376
303F0603 551D1F04 38303630 34A032A0 30862E68 7474703A 2F2F766D 2D746573
742D6361 2E63702E 72752F43 65727445 6E726F6C 6C2F7465 73742D63 612E6372
6C3081AC 06082B06 01050507 01010481 9F30819C 304B0608 2B060105 05073002
863F6874 74703A2F 2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E
726F6C6C 2F766D2D 74657374 2D63612E 63702E72 755F7465 73742D63 612E6372
74304D06 082B0601 05050730 02864166 696C653A 2F2F5C5C 766D2D74 6573742D
63612E63 702E7275 5C436572 74456E72 6F6C6C5C 766D2D74 6573742D 63612E63
702E7275 5F746573 742D6361 2E637274 30080606 2A850302 02030341 00850B51
588B2C0E 4C9AB975 778130DF E3F6D654 D7326F90 370A3C38 A2470D5C 8CB91E5B
580BA724 418CC995 7A3BF2F3 1DA5B8DB 3A0091A0 EE150FCB CFBEB2EB 2B

message type
10 (client key exchange)
length

```
0000F5
client key exchange
3081F230 81EF3028 04202B97 33F1F6EF EB453035 415119E4 6D3E1798 A037488B
E6B5836C F8CFB81B B5970404 E2897619 A081C206 092A8503 07010205 0101A081
AA302106 082A8503 07010101 02301506 092A8503 07010201 02010608 2A850307
01010203 03818400 04818094 505C443B 6C2685C5 FD88888F 00177F56 2F28FEB2
6461389D 2BC70730 B94B903D 526103DA AF2F360B 47EEDCC4 BA07F733 D83D33AF
0CA81936 8C3C5F08 26A67D44 14BF92A2 4A89C784 1B81C101 674EDC77 1D092BEA
46ACD877 C60F7DA1 60B959A1 428A2F72 D2DDDE4B 741D79E5 9878F02E 12241798
1C67A557 4CEF3F48 9E679504 08F528F1 128286A8 0F

message type
0F
length
000040
certificate verify
F17A142A 4D306C61 1C5FE211 055A40A1 18A3080F 2A82771F 9447E4C9 A5AEC9C6
4411AC5A BDBDBA1F 6FBD23CD 3AC0873C ED7B0C90 8CAFDB07 60E8B20E DEA72A9F


>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


client -> server:

header
header type
14 (change cipher spec)
major version
03
minor version
01
Length
0001
message type
01 (change cipher spec)
length
000000

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


client internals:

master secret = PRF_GOSTR3411(PreMasterSecret, “master secret”, client
random, server random)

A9953B3D 2F36CEF7 600E6068 171E1C75 99164F6E 3FCC4321 F77A9AB4 963D2AFA
41A54CF9 8FCFAE40 ADF42F8F E668FD75
hash(master secret)
56E69592 B7D44D4D 0D5A00A7 F8CDA91D C2AE886E 34C856B4 E5B98BB9 1CD5459E
key block = PRF_GOSTR3411(hash(master secret), “key expansion”, server
random, client random)
B826AA51 EB0A4DEB 0BF5689D 2C7E7997 6744B69C 9F16DEF4 77BFF655 023F4964
831B5706 AC8AB7C5 1BD12D17 40D61837 97F6874E 31EFED44 A1C64BDB D6D3AED2
4F0520AA D7A6825F D2D73C61 5801EB0E CC41644F 8FF488EB 34635D33 7644BF76
```

328D89F9 36B29ACC 703CE9B5 203149BD BD0BED66 D896B5EE 08D4CB8D 90D99E66
34F71DD0 409DFB54 956B327C C1B606FE

client write key
4F0520AA D7A6825F D2D73C61 5801EB0E CC41644F 8FF488EB 34635D33 7644BF76
client write MAC secret
B826AA51 EB0A4DEB 0BF5689D 2C7E7997 6744B69C 9F16DEF4 77BFF655 023F4964
client write IV
34F71DD0 409DFB54
hash(handshake messages)
9B75B5FB 4EB87691 AC78D1EB 85331F55 F32FFB00 C26B522E 7719FE2C F26A3C80
finished label
client finished
verify data = PRF_GOSTR3411(hash(master secret), finished label,
hash(handshake messages))
666C982A 77970F44 ABD253F7

message type
14 (finished)
length
00000C
verify data
666C982A 77970F44 ABD253F7

client -> server:

write_sequence
00000000 00000000
header
header type
16 (handshake)
major version
03
minor version
01
Length
0010
message encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
844CA0E3 91D51F31 2F0CF0B0 F9388A96
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
1A1D479C

>>

server internals:

server private key

CAA00F9C 2F6E2CFF 3CC9AE17 2AC130ED B7517D29 FD58DC00 D50C49B7 819D9C26
FFBD82E6 91D2B370 1DF39C62 BAB8AB79 DA5C1AD5 E3A5E6F0 D4DB9531 624A34EC
client public key blob header (ephemeral)
06200100 3D2E0000 4D414731 00040000 30150609 2A850307 01020102 0106082A
85030701 01020394

```
client public key (ephemeral)
94505C44 3B6C2685 C5FD8888 8F00177F 562F28FE B2646138 9D2BC707 30B94B90
3D526103 DAAF2F36 0B47EEDC C4BA07F7 33D83D33 AF0CA819 368C3C5F 0826A67D
4414BF92 A24A89C7 841B81C1 01674EDC 771D092B EA46ACD8 77C60F7D A160B959
A1428A2F 72D2DDDE 4B741D79 E59878F0 2E122417 981C67A5 574CEF3F 489E6795
hash(client random, server random)
F528F112 8286A80F 19405393 1267A151 17455680 C30C1600 84B400B3 867208B2
ukm
F528F112 8286A80F
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1(id-tc26-gost-28147-param-Z) in ECB mode
                  2B9733F1 F6EFEB45 30354151 19E46D3E 1798A037 488BE6B5
836CF8CF B81BB597
                  MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                  E2897619
Inner Point
02756997 5C3DEF17 6C9407B4 D26A87D0 35BAA977 74EE19D0 B7B37109 2BE9B3C7
9C9174A1 9371CD74 F4C86ECF 9BD5952D AE967D91 B44FB899 D0608B68 753F6604
81317270 F68976BD 893A9D6E FE942CF3 6A002385 5F76B986 C4FD8449 CFBC56D9
9F91E5C1 DD62778D FAAB3640 DDB4E7E0 4DEC3FDF CECBA04D 978CAB7C 7689E5EF
VKO result
8A2D3569 221F2B2B 3207450E 9D32E9D0 973ED97E 67E96D5B A06131DF 4DA75AA8
diversified key
D83FE5FA 27803F24 AB15153D 4CCDB351 343B6BE3 CCAAAA29 E2CCC38E CB771524
premastersecret
26DBE1DA A8757A2F FD12E2BB 1ABA62CC A69C37B1 80C12B7D 8FEF63AC 17723A25
client public key blob header
06200100 492E0000 4D414731 00020000 30130607 2A850302 02240006 082A8503
07010102 02EBCE8A
client public key
EBCE8AB9 C7C8400E D94AC055 529EDA2B 31102615 BD632252 27E52FF8 D9E86E6F
7D1FBA5E 292DEECE D28BAB6F 8B82D34F B71B2457 3838D279 E9DBF1D9 AC711AD9

master secret = PRF_GOSTR3411(premastersecret, “master secret”, client
random, server random)
A9953B3D 2F36CEF7 600E6068 171E1C75 99164F6E 3FCC4321 F77A9AB4 963D2AFA
41A54CF9 8FCFAE40 ADF42F8F E668FD75
hash(master secret)
56E69592 B7D44D4D 0D5A00A7 F8CDA91D C2AE886E 34C856B4 E5B98BB9 1CD5459E
key_block = PRF_GOSTR3411(hash(master secret), “key expansion”, server
random, client random)
B826AA51 EB0A4DEB 0BF5689D 2C7E7997 6744B69C 9F16DEF4 77BFF655 023F4964
831B5706 AC8AB7C5 1BD12D17 40D61837 97F6874E 31EFED44 A1C64BDB D6D3AED2
4F0520AA D7A6825F D2D73C61 5801EB0E CC41644F 8FF488EB 34635D33 7644BF76
328D89F9 36B29ACC 703CE9B5 203149BD BD0BED66 D896B5EE 08D4CB8D 90D99E66
34F71DD0 409DFB54 956B327C C1B606FE

server read key
4F0520AA D7A6825F D2D73C61 5801EB0E CC41644F 8FF488EB 34635D33 7644BF76
server read MAC secret
B826AA51 EB0A4DEB 0BF5689D 2C7E7997 6744B69C 9F16DEF4 77BFF655 023F4964
server read IV
34F71DD0 409DFB54

client <- server:
```

```
header
header type
14 (change cipher spec)
major version
03
minor version
01
length
0001
message type
01 (change cipher spec)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

server internals:

server write key
328D89F9 36B29ACC 703CE9B5 203149BD BD0BED66 D896B5EE 08D4CB8D 90D99E66
server write MAC secret
831B5706 AC8AB7C5 1BD12D17 40D61837 97F6874E 31EFED44 A1C64BDB D6D3AED2
server write IV
956B327C C1B606FE
hash(handshake messages)
5D759532 3B144755 4C5794AD 18CDA95A F947335C FC653012 8C460C65 03A117AC
finished label
server finished
verify data = PRF_GOSTR3411(hash(master secret), finished label,
hash(handshake messages))
23B4C66C 00D3557D A8A2C1B6


message type
14 (finished)
length
00000C
verify data
23B4C66C 00D3557D A8A2C1B6

client <- server:

write_sequence
00000000 00000000
header type
16 (handshake)
major version
03
minor version
01
Length
0010
message encrypted on server write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
```

```
6110DD0C C0772D66 06DE24BD E7644347
MAC on server write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
9247FFAB

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

client read key
328D89F9 36B29ACC 703CE9B5 203149BD BD0BED66 D896B5EE 08D4CB8D 90D99E66
client read MAC secret
831B5706 AC8AB7C5 1BD12D17 40D61837 97F6874E 31EFED44 A1C64BDB D6D3AED2
client read IV
956B327C C1B606FE

client message

04030201 08070605 0C0B0A09 100F0E0D 14131211 18171615 1C1B1A19 201F1E1D
24232221 28272625 2C2B2A29 302F2E2D 34333231 38373635 3C3B3A39 403F3E3D
44434241 48474645 4C4B4A49 504F4E4D 54535251 58575655 5C5B5A59 605F5E5D
64636261 68676665 6C6B6A69 706F6E6D 74737271 78777675 7C7B7A79 807F7E7D
84838281 88878685 8C8B8A89 908F8E8D 94939291 98979695 9C9B9A99 A09F9E9D
A4A3A2A1 A8A7A6A5 ACABAAA9 B0AFAEAD B4B3B2B1 B8B7B6B5 BCBBBAB9 C0BFBEBD
C4C3C2C1 C8C7C6C5 CCCBCAC9 D0CFCECD D4D3D2D1 D8D7D6D5 DCDBDAD9 E0DFDEDD
E4E3E2E1 E8E7E6E5 ECEBEAE9 F0EFEEED F4F3F2F1 F8F7F6F5 FCFBFAF9 03020100
07060504 0B0A0908 0F0E0D0C 13121110 17161514 1B1A1918 1F1E1D1C 23222120
27262524 2B2A2928 2F2E2D2C 33323130 37363534 3B3A3938 3F3E3D3C 43424140
47464544 4B4A4948 4F4E4D4C 53525150 57565554 5B5A5958 5F5E5D5C 63626160
67666564 6B6A6968 6F6E6D6C 73727170 77767574 7B7A7978 7F7E7D7C 83828180
87868584 8B8A8988 8F8E8D8C 93929190 97969594 9B9A9998 9F9E9D9C A3A2A1A0
A7A6A5A4 ABAAA9A8 AFAEADAC B3B2B1B0 B7B6B5B4 BBBAB9B8 BFBEBDBC C3C2C1C0
C7C6C5C4 CBCAC9C8 CFCECDCC D3D2D1D0 D7D6D5D4 DBDAD9D8 DFDEDDDC E3E2E1E0
E7E6E5E4 EBEAE9E8 EFEEEDEC F3F2F1F0 F7F6F5F4 FBFAF9F8 020100FC 06050403
0A090807 0E0D0C0B 1211100F 16151413 1A191817 1E1D1C1B 2221201F 26252423
2A292827 2E2D2C2B 3231302F 36353433 3A393837 3E3D3C3B 4241403F 46454443
4A494847 4E4D4C4B 5251504F 56555453 5A595857 5E5D5C5B 6261605F 66656463
6A696867 6E6D6C6B 7271706F 76757473 7A797877 7E7D7C7B 8281807F 86858483
8A898887 8E8D8C8B 9291908F 96959493 9A999897 9E9D9C9B A2A1A09F A6A5A4A3
AAA9A8A7 AEADACAB B2B1B0AF B6B5B4B3 BAB9B8B7 BEBDBCBB C2C1C0BF C6C5C4C3
CAC9C8C7 CECDCCCB D2D1D0CF D6D5D4D3 DAD9D8D7 DEDDDCDB E2E1E0DF E6E5E4E3
EAE9E8E7 EEEDECEB F2F1F0EF F6F5F4F3 FAF9F8F7 0100FCFB 05040302 09080706
0D0C0B0A 11100F0E 15141312 19181716 1D1C1B1A 21201F1E 25242322 29282726
2D2C2B2A 31302F2E 35343332 39383736 3D3C3B3A 41403F3E 45444342 49484746
4D4C4B4A 51504F4E 55545352 59585756 5D5C5B5A 61605F5E 65646362 69686766
6D6C6B6A 71706F6E 75747372 79787776 7D7C7B7A 81807F7E 85848382 89888786
8D8C8B8A 91908F8E 95949392 99989796 9D9C9B9A A1A09F9E A5A4A3A2 A9A8A7A6
ADACABAA B1B0AFAE B5B4B3B2 B9B8B7B6 BDBCBBBA C1C0BFBE C5C4C3C2 C9C8C7C6
CDCCCBCA D1D0CFCE D5D4D3D2 D9D8D7D6 DDDCDBDA E1E0DFDE E5E4E3E2 E9E8E7E6
EDECEBEA F1F0EFEE F5F4F3F2 F9F8F7F6 00FCFBFA 04030201 080706

client -> server:

write sequence
00000000 00000001
header type
```

17 (application data)
major version
03
minor version
01
Length
03FB
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in CNT mode
D61BB281 40B84CE9 598B3CAF 22552815 8F70BF81 803D898D 447F6CEE 4C7115DD
88EA16A0 5DE24470 3A324343 CD04299B AACAD1F8 29B30CF5 3AC34A38 130A22DF
F041C9D4 F5D266FA AA092465 88C04751 7C089DC2 87B3258A E398FAAE 550E8AC9
CF1A82D1 6A3B2C71 3778DF26 6FAAD233 BE993FEC 784BBDA9 14BC3805 030B1C97
AAF5AD31 5E75A2BA 9127F810 86172831 E8BC207B 9516A7EA C5141C8B CF6A7C7D
9F1B6944 F368CF88 685F297F 021B6F77 67BDD199 577F8732 2F156081 F6BEB634
DDD42651 BB8B377B 2EB59C45 34FACAD8 34D53440 891BFA74 6885C11B 0FA8A235
C04E22FD C4A4D1DC D9000A74 1DEA3B02 19B8A582 8C0BBFC2 654DA0E6 AB184398
F549B258 A9808C4A 14721790 8506E170 8B9A3F00 ACC85667 CD42E6E1 8B69FEF3
D64BBCD4 C418EC38 D999694E AC08CE78 4D78F34D 32A51227 A0E47330 3DB6ACD5
2BA660A5 D6616492 A34C2F4E 2E0C28D7 2FD5E5ED 2645E4DB 44CA2825 3C0FA25B
6B8CFABA 840493F6 E091C4A4 4C7878C6 241FD8E5 D0C0DB46 FC73FAA9 24B1B225
58BDD0EB DBEB6819 84AA8A40 3FA21048 7E6AC2E0 1CD37619 A996362D 39D8FA82
2C021795 EBD5CF15 4780CE94 A6532474 1C62BE62 67DFDE4A CE1A8415 D9A5B174
1AD35BAB A3F5438C 1374D5A5 601349D2 29FA18BB 9D24F0C1 315F165D 05E62174
BCEFF20E 9C2A304B DF02E42C 634D4123 403B6BF2 E2984EBF 68D9F0EA F087F804
46EDD7FA 9437FAA0 CFF0055E E454A57E ED991489 73B15492 42C45FBB 83EDB238
48964396 86410685 21ED92AF FA07B923 735059F0 3D08DED2 7BA2510F 8C81882B
07AECB71 F63EFDD4 CFCDF848 82AE265F A18D9084 D4D5CC9B 19BBCA63 0FC93A25
A9130FD7 1DF8AD18 0DF6D78F 74D940C9 7579BA1C D69C6188 90DAADA0 FD81FCEC
134BD38D DFD1C6BC 0408A1E1 517A170D 8CA5209D DB09DBEA 8DD66963 7FD08CE1
A2B6CB79 A580B6B7 C8F02622 0E0B11C0 B8FFC964 9D17587A 56200DE3 4AFD5912
7CC79F4C C8F7C042 59EBA492 41F1782D 63144470 C746998D 0940C1FC 663EA5BC
4C912B8F 54F33E82 F9DA0627 882F4499 2576D7C4 835FFF74 7D96D806 1A261447
B99E443A 9C9913CD 7B3F2BB6 B6050E13 FACA7721 7EF79338 7A04904C DDF771B9
20AF6C8C 727CC89F 39478E9B EB2FF07E 157FC830 3DC2926E 87DE5B2C 9E2E7070
A88C7A24 464D739B 1E546513 369F3F76 E9B018AD 42D03A0D 450E2880 E9C27DD5
0984382E 2D75A6EA 3B1BDE8B ACCD50E5 3CBA2CF5 8FDC3BCA A0468102 8BB472B2
5BF5CF15 2119C173 C884ACD6 3BF2761F 60CC89E6 91C4F07E C3CF0D18 DF3E20C3
583CAF51 2096E90E 8702DD12 AF22B7EC B53B821B FC72228F DAC9F2EF A28161B7
AC88142A 785CAFE0 0A01ED68 62EE5DA9 8705AD07 E289CFEB 929FAF81 CE0A30F6
9AAB7AAF ED012834 34C363DD 9CB85AC6 AD1E405D 0827D6EE 6EFC8B
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z)
672E5BB8

>>

client message

0403

client -> server:

write sequence
00000000 00000002

```
header type
17 (application data)
major version
03
minor version
01
Length
02
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
6016
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
C477AD86
```

A.4. TLS 1.0 аутентификация сервера с ключом 256 бит

```
client -> server:

header type
16 (handshake)
major version
03
minor version
01
Length
004E

message type
01 (client hello)
length
00004A
TLS VERSION
                  major version
                  03
                  minor version
                  01
client random
52E78F4F 6AA0FE31 2217AEF6 91AD7639 32945E8C EDD7F96E 3C336B08 66A66698
session id length
00
session id

ciphersuite length
0004
CipherSuite
0081               TLS_CIPHER_2001
FF85               TLS_CIPHER_2012
compression methods
                  length
                  01
                  compression method
                  00
extensions
  extensions length
```

```
  001D
  renegotiation_info (FF01)
  length
  0001
  Renegotiation Info extension
  00
  server name (0000)
  length
  0014
  server name list length
  0012
  server name type
  00
  server name length
  000F
  server name
  746C7363 6F6E665F 73727635 313265

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

client <- server:

header type
16 (handshake)
major version
03
minor version
01
Length
032F

message type
02 (server hello)
length
000046
TLS VERSION
                  major version
                  03
                  minor version
                  01
server random
52E78F4F 4E131F8C ABAFD5D7 C9C62A5E DF62CADB 4D033131 FE9B83DE 9D459EFD
session id length
20
session id
107066A7 51DF204F 42FD4286 699FE85A B18689BE DD2598D0 4C5E5F12 145E0F3B
ciphersuite
FF85                TLS_CIPHER_2012
compression method
00
extensions

message type
0B (certificate)
length
0002DD
```

server certificate chain
0002DA00 02D73082 02D33082 0282A003 02010202 0A427E80 21000000 8B927530
0806062A 85030202 03303A31 12301006 0A099226 8993F22C 64011916 02727531
12301006 0A099226 8993F22C 64011916 02637031 10300E06 03550403 13077465
73742D63 61301E17 0D313430 31323830 34323432 385A170D 32343031 32383131
30343238 5A304731 18301606 03550403 0C0F746C 73636F6E 665F7372 76353132
65312B30 2906092A 864886F7 0D010901 161C746C 73636F6E 665F7372 76353132
65406372 7970746F 70726F2E 72753066 301F0608 2A850307 01010101 30130607
2A850302 02240006 082A8503 07010102 02034300 0440442B 2744A488 9B1F456F
A23BC840 9FC272E8 F36A65EB 2548038B B0E10A8A FE2CFCB7 5AAAD185 D2F18B5A
ED28F747 B3C72D5C C5BA870A 2CC76F57 5A9BC7EF 25E7A382 01563082 01523013
0603551D 25040C30 0A06082B 06010505 07030130 0B060355 1D0F0404 03020430
301D0603 551D0E04 1604146B BF36F2E8 0DEB1254 4478CE0B 55CC7C84 E1B83430
1F060355 1D230418 30168014 9E03F0B8 9CFC60DC 8A181EE8 00DFA85B 32CD7376
303F0603 551D1F04 38303630 34A032A0 30862E68 7474703A 2F2F766D 2D746573
742D6361 2E63702E 72752F43 65727445 6E726F6C 6C2F7465 73742D63 612E6372
6C3081AC 06082B06 01050507 01010481 9F30819C 304B0608 2B060105 05073002
863F6874 74703A2F 2F766D2D 74657374 2D63612E 63702E72 752F4365 7274456E
726F6C6C 2F766D2D 74657374 2D63612E 63702E72 755F7465 73742D63 612E6372
74304D06 082B0601 05050730 02864166 696C653A 2F2F5C5C 766D2D74 6573742D
63612E63 702E7275 5C436572 74456E72 6F6C6C5C 766D2D74 6573742D 63612E63
702E7275 5F746573 742D6361 2E637274 30080606 2A850302 02030341 000FDCCB
2BEDB244 BB93D103 A9F058BA 46474261 300D87B8 6AD845AA B22CD64A B057AD90
FF5C09AC 218E34F5 B9EFF672 3C5FB110 BEE14933 65D588D4 C8B8098C 76

message type
0E (server hello done)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

premastersecret
6BFF027B 125DC258 F07AD427 8093A408 B6F126E3 E949C585 3D6C0F5E 4072B6AA
client private key (ephemeral)
73502099 DE75AF08 1D69DA72 C3B436D3 AA6A96DF 9D3F22C7 83FF8ECF F402D9CF
server public key blob header
06200100 492E0000 4D414731 00020000 30130607 2A850302 02240006 082A8503
07010102 02442B27
server public key
442B2744 A4889B1F 456FA23B C8409FC2 72E8F36A 65EB2548 038BB0E1 0A8AFE2C
FCB75AAA D185D2F1 8B5AED28 F747B3C7 2D5CC5BA 870A2CC7 6F575A9B C7EF25E7
hash(client random, server random)
BDE6576E 0E5CCD9E 1F2AC612 51E5D620 64B61FB2 BCD14CB0 114C2FDB 3625086E
ukm
BDE6576E 0E5CCD9E
Inner Point
D6E9D490 B8538819 BF7D938D DB735AD7 194238F0 E0F9C132 6F0C6578 3D6C6C11
CC1ADC73 8FBD7E66 210B0431 D9A0D55E 2E97D042 C8911828 E736BDBA 8C42528D
VKO result
94DC0DCE F7BB36F7 5B94689E BB788B8B 8093DEA3 44062AC2 048194EC 078559B9
diversified key
1802FC0D 49350EBF F05E6015 9C36A2EB F76D256E F2CCB056 9524283F B3823FBA

```
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in ECB mode
                    6ED1C0AE A3B0832B 2B75937F 5954E3C0 D307F660 7290976A
F62791A8 6EB26A7B
                    MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                    83D12F2C

client key exchange
3081AC30 81A93028 04206ED1 C0AEA3B0 832B2B75 937F5954 E3C0D307 F6607290
976AF627 91A86EB2 6A7B0404 83D12F2C A07D0609 2A850307 01020501 01A06630
1F06082A 85030701 01010130 1306072A 85030202 24000608 2A850307 01010202
03430004 40193152 2C493DC6 42053736 879FD447 BC4E33B4 AA459900 9F458DBD
C16A2FF6 0C9D6DC6 BEC53B6C 78212636 B831EABE DD0B6B96 EDE1366C 7BF85053
E6DB87A4 A50408BD E6576E0E 5CCD9E

client -> server:

header type
16 (handshake)
major version
03
minor version
01
Length
0B3
message type
10 (client key exchange)
length
0000AF
client key exchange
3081AC30 81A93028 04206ED1 C0AEA3B0 832B2B75 937F5954 E3C0D307 F6607290
976AF627 91A86EB2 6A7B0404 83D12F2C A07D0609 2A850307 01020501 01A06630
1F06082A 85030701 01010130 1306072A 85030202 24000608 2A850307 01010202
03430004 40193152 2C493DC6 42053736 879FD447 BC4E33B4 AA459900 9F458DBD
C16A2FF6 0C9D6DC6 BEC53B6C 78212636 B831EABE DD0B6B96 EDE1366C 7BF85053
E6DB87A4 A50408BD E6576E0E 5CCD9E

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

client -> server:

header
header type
14 (change cipher spec)
major version
03
minor version
01
Length
0001
message type
01 (change cipher spec)
length
000000
```

```
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>


client internals:

master secret = PRF_GOSTR3411(PreMasterSecret, “master secret”, client
random, server random)
0DA86741 96F2496C 4EE1E477 9DE04990 BE3CE465 5252F196 1E707B61 17843613
1369D11E 7DA84C05 374535B9 5550DD0F
hash(master secret)
B9B7EA22 70A60D1A 1DE5C320 6B14E1DB F8AB5BF9 FADAC89C 4FE1325B 0AE5ED13
key block = PRF_GOSTR3411(hash(master secret), “key expansion”, server
random, client random)
168F892A 8A01136E 8B9F9E44 8600A9E2 A73376B2 8AD5C4C7 897F0638 997890FD
930340CB AD345A8B 0AB9D569 5D0806A6 A4883B4B 9D295B54 304910A6 E9C01AE3
353BC83D FC13F4F8 E45C763C 51CD7190 01CC0CE3 D81928AD 130452D4 D048F323
F1B4A8F3 E632FBD1 BBEA341E A77FF526 AB3D2414 0C4E373E 61C63A52 E5DC27B3
4E7F622A 23C84833 A53224D0 608EB006

client write key
353BC83D FC13F4F8 E45C763C 51CD7190 01CC0CE3 D81928AD 130452D4 D048F323
client write MAC secret
168F892A 8A01136E 8B9F9E44 8600A9E2 A73376B2 8AD5C4C7 897F0638 997890FD
client write IV
4E7F622A 23C84833
hash(handshake messages)
52D8FA5A B1CFB44F C591F6D3 AAA5E592 7F25A30F E00FEFA6 60A8442F 9A80E3AB
finished label
client finished
verify data = PRF_GOSTR3411(hash(master secret), finished label,
hash(handshake messages))
07E0B66F 9A775545 F6590C2E

message type
14 (finished)
length
00000C
verify data
07E0B66F 9A775545 F6590C2E

client -> server:

write_sequence
00000000 00000000
header type
16 (handshake)
major version
03
minor version
01
Length
0010
message encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
E8F8C00C EFE1804A 6E04D4F0 367AA0CB
```

```
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
E270E0C2

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

server internals:

server private key
836E71F6 3FF7D8B1 5117ABC9 B9730197 1352D2C3 392BD09F 828CE530 502C8FF8
client public key blob header (ephemeral)
06200100 492E0000 4D414731 00020000 30130607 2A850302 02240006 082A8503
07010102 02193152
client public key (ephemeral)
1931522C 493DC642 05373687 9FD447BC 4E33B4AA 4599009F 458DBDC1 6A2FF60C
9D6DC6BE C53B6C78 212636B8 31EABEDD 0B6B96ED E1366C7B F85053E6 DB87A4A5
hash(client_random, server_random)
BDE6576E 0E5CCD9E 1F2AC612 51E5D620 64B61FB2 BCD14CB0 114C2FDB 3625086E
ukm
BDE6576E 0E5CCD9E
premastersecret encrypted on exchange key using parameters
1.2.643.7.1.2.5.1.1(id-tc26-gost-28147-param-Z) in ECB mode
                    6ED1C0AE A3B0832B 2B75937F 5954E3C0 D307F660 7290976A
F62791A8 6EB26A7B
                    MAC on exchange key using parameters
1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) with ukm as IV
                    83D12F2C
Inner Point
D6E9D490 B8538819 BF7D938D DB735AD7 194238F0 E0F9C132 6F0C6578 3D6C6C11
CC1ADC73 8FBD7E66 210B0431 D9A0D55E 2E97D042 C8911828 E736BDBA 8C42528D
VKO result
94DC0DCE F7BB36F7 5B94689E BB788B8B 8093DEA3 44062AC2 048194EC 078559B9
diversified key
1802FC0D 49350EBF F05E6015 9C36A2EB F76D256E F2CCB056 9524283F B3823FBA
premastersecret
6BFF027B 125DC258 F07AD427 8093A408 B6F126E3 E949C585 3D6C0F5E 4072B6AA

master secret = PRF_GOSTR3411(premastersecret, “master secret”, client
random, server random)
0DA86741 96F2496C 4EE1E477 9DE04990 BE3CE465 5252F196 1E707B61 17843613
1369D11E 7DA84C05 374535B9 5550DD0F
hash(master secret)
B9B7EA22 70A60D1A 1DE5C320 6B14E1DB F8AB5BF9 FADAC89C 4FE1325B 0AE5ED13
key block = PRF_GOSTR3411(hash(master secret), “key expansion”, server
random, client random)
168F892A 8A01136E 8B9F9E44 8600A9E2 A73376B2 8AD5C4C7 897F0638 997890FD
930340CB AD345A8B 0AB9D569 5D0806A6 A4883B4B 9D295B54 304910A6 E9C01AE3
353BC83D FC13F4F8 E45C763C 51CD7190 01CC0CE3 D81928AD 130452D4 D048F323
F1B4A8F3 E632FBD1 BBEA341E A77FF526 AB3D2414 0C4E373E 61C63A52 E5DC27B3
4E7F622A 23C84833 A53224D0 608EB006

server read key
353BC83D FC13F4F8 E45C763C 51CD7190 01CC0CE3 D81928AD 130452D4 D048F323
server read MAC secret
168F892A 8A01136E 8B9F9E44 8600A9E2 A73376B2 8AD5C4C7 897F0638 997890FD
server read IV
```

```
4E7F622A 23C84833

client <- server:

header
header type
14 (change cipher spec)
major version
03
minor version
01
length
0001
message type
01 (change cipher spec)
length
000000

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

server internals:

server write key
F1B4A8F3 E632FBD1 BBEA341E A77FF526 AB3D2414 0C4E373E 61C63A52 E5DC27B3
server write MAC secret
930340CB AD345A8B 0AB9D569 5D0806A6 A4883B4B 9D295B54 304910A6 E9C01AE3
server write IV
A53224D0 608EB006
hash(handshake messages)
CF3013DA 70E6F6E7 C076CB4B 5C261E70 0C9CF6A4 583B6F2D B21A8703 01137E60
finished label
server finished
verify data = PRF_GOSTR3411(hash(master secret), finished label,
hash(handshake messages))
265216EB 000305DD D9BEBAD4


message type
14 (finished)
length
00000C
verify data
265216EB 000305DD D9BEBAD4

client <- server:

write_sequence
00000000 00000000
header type
16 (handshake)
major version
03
minor version
01
Length
```

0010
message encrypted on server write key using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z) in CNT mode
62839CDF CF4E5663 03222A33 FE5EC401
MAC on server write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-tc26-gost-28147-param-Z)
822B2705

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

client internals:

client read key
F1B4A8F3 E632FBD1 BBEA341E A77FF526 AB3D2414 0C4E373E 61C63A52 E5DC27B3
client read MAC secret
930340CB AD345A8B 0AB9D569 5D0806A6 A4883B4B 9D295B54 304910A6 E9C01AE3
client read IV
A53224D0 608EB006

Client message

04030201 08070605 0C0B0A09 100F0E0D 14131211 18171615 1C1B1A19 201F1E1D
24232221 28272625 2C2B2A29 302F2E2D 34333231 38373635 3C3B3A39 403F3E3D
44434241 48474645 4C4B4A49 504F4E4D 54535251 58575655 5C5B5A59 605F5E5D
64636261 68676665 6C6B6A69 706F6E6D 74737271 78777675 7C7B7A79 807F7E7D
84838281 88878685 8C8B8A89 908F8E8D 94939291 98979695 9C9B9A99 A09F9E9D
A4A3A2A1 A8A7A6A5 ACABAAA9 B0AFAEAD B4B3B2B1 B8B7B6B5 BCBBBAB9 C0BFBEBD
C4C3C2C1 C8C7C6C5 CCCBCAC9 D0CFCECD D4D3D2D1 D8D7D6D5 DCDBDAD9 E0DFDEDD
E4E3E2E1 E8E7E6E5 ECEBEAE9 F0EFEEED F4F3F2F1 F8F7F6F5 FCFBFAF9 03020100
07060504 0B0A0908 0F0E0D0C 13121110 17161514 1B1A1918 1F1E1D1C 23222120
27262524 2B2A2928 2F2E2D2C 33323130 37363534 3B3A3938 3F3E3D3C 43424140
47464544 4B4A4948 4F4E4D4C 53525150 57565554 5B5A5958 5F5E5D5C 63626160
67666564 6B6A6968 6F6E6D6C 73727170 77767574 7B7A7978 7F7E7D7C 83828180
87868584 8B8A8988 8F8E8D8C 93929190 97969594 9B9A9998 9F9E9D9C A3A2A1A0
A7A6A5A4 ABAAA9A8 AFAEADAC B3B2B1B0 B7B6B5B4 BBBAB9B8 BFBEBDBC C3C2C1C0
C7C6C5C4 CBCAC9C8 CFCECDCC D3D2D1D0 D7D6D5D4 DBDAD9D8 DFDEDDDC E3E2E1E0
E7E6E5E4 EBEAE9E8 EFEEEDEC F3F2F1F0 F7F6F5F4 FBFAF9F8 020100FC 06050403
0A090807 0E0D0C0B 1211100F 16151413 1A191817 1E1D1C1B 2221201F 26252423
2A292827 2E2D2C2B 3231302F 36353433 3A393837 3E3D3C3B 4241403F 46454443
4A494847 4E4D4C4B 5251504F 56555453 5A595857 5E5D5C5B 6261605F 66656463
6A696867 6E6D6C6B 7271706F 76757473 7A797877 7E7D7C7B 8281807F 86858483
8A898887 8E8D8C8B 9291908F 96959493 9A999897 9E9D9C9B A2A1A09F A6A5A4A3
AAA9A8A7 AEADACAB B2B1B0AF B6B5B4B3 BAB9B8B7 BEBDBCBB C2C1C0BF C6C5C4C3
CAC9C8C7 CECDCCCB D2D1D0CF D6D5D4D3 DAD9D8D7 DEDDDCDB E2E1E0DF E6E5E4E3
EAE9E8E7 EEEDECEB F2F1F0EF F6F5F4F3 FAF9F8F7 0100FCFB 05040302 09080706
0D0C0B0A 11100F0E 15141312 19181716 1D1C1B1A 21201F1E 25242322 29282726
2D2C2B2A 31302F2E 35343332 39383736 3D3C3B3A 41403F3E 45444342 49484746
4D4C4B4A 51504F4E 55545352 59585756 5D5C5B5A 61605F5E 65646362 69686766
6D6C6B6A 71706F6E 75747372 79787776 7D7C7B7A 81807F7E 85848382 89888786
8D8C8B8A 91908F8E 95949392 99989796 9D9C9B9A A1A09F9E A5A4A3A2 A9A8A7A6
ADACABAA B1B0AFAE B5B4B3B2 B9B8B7B6 BDBCBBBA C1C0BFBE C5C4C3C2 C9C8C7C6
CDCCCBCA D1D0CFCE D5D4D3D2 D9D8D7D6 DDDCDBDA E1E0DFDE E5E4E3E2 E9E8E7E6
EDECEBEA F1F0EFEE F5F4F3F2 F9F8F7F6 00FCFBFA 04030201 080706

client -> server:

```
write_sequence
00000000 00000001
header type
17 (application data)
major version
03
minor version
01
length
03FB
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
01AB8FC1 D1F4170C 0637E44D 50C8A219 3F10A704 A73570AD AE9DF251 5729865C
3C3BD703 0B886A3C 8B6153D5 4E1E04F2 EFE47A0B 2462FC67 DB899856 A426DDC1
017FBE74 425EFDF5 F8555C89 F9B21A97 BAD0C308 6D67DA15 BDF06211 BC769F79
3415B872 32452FF7 8D4C7153 CC460C28 2ACA6A1D 0E12D059 B5D422CC C1861E25
CA097DD7 4B7F8DB2 B58C25B8 839E9D42 55A9B0C3 83271CE9 EC9819C8 A66AD3AC
AAAACD9A 9BA57EEE 38BBC935 B1466DB2 4258B0D2 528752A1 C3F879F6 8CBE4DD5
58E910A8 58C8E0AA CDA72A6B 589DF9A2 057FCB49 95B38162 9E33110F 16578C91
D61A2021 552A2833 73B08B1E 09F15608 EE597136 EECD2532 48F9B25E 075ED3A9
54749095 0B7B4D1E 709D4160 8E7CFE95 6E154ABA 9DADA8A2 64AB0287 47694336
A1499C3A 20AC7100 D2011E6F 8A929C3C E36D9477 F5EC218B 3A581ADD 9B65CDD4
18060289 B0C9C7E5 A59F94A9 883624FD CC54E9BA 838CBE3A 164E2F8B 1124A35F
84CEC684 ABDDA78A 0123A024 58D78878 4B63F9E9 9721B71F 2AC574E9 B1F21795
85425B09 FDDFC2EB F0C13EF6 5C7646A0 90EC1168 1C469401 160D8616 3E1C2B5F
5E1A7BF5 BFE3BCBA 8C37FB5B F1646ECF 22428084 9C3F28C3 64784432 DE3CEC81
C6452A63 D33AF055 08B3ACD2 EE64C04E 206E8CA2 669614AE 1465D3C5 37A1AED2
4FB6A141 D91A6BE3 73F06FCF 6999E5AC 44CFC274 78A08F71 7C0D3E57 315C0F36
1ED2C534 22C4BE6F 767969DB 3B63F90C 6B158703 6485BE13 A1C2B9B0 9C773041
24DB600D 514BC0D7 8DF05AB7 A1712375 D0D37219 434B244B 418C7628 18A50E8C
78F45B7A C0D1BD1B 266A00B9 6C1E13FC 1C934D99 A6BE15E1 9136DF80 04F7E182
63E43CBE 3AA04122 AD076F92 70953AE4 88F7CDF5 517D46AD 7EFC4DA6 C622BEA1
E959E1FA C64D6641 B6D138B6 625AABEC F69C90B6 6F6FA989 C66ED113 26940583
3E796894 A0FFCE08 08E770C9 ECC7E5A7 18D26599 3248AB8E 7CFBC342 F9A74107
6BAF74FC C3059E8E 01CD3A8D 35E358A6 9C24A504 5727B130 8EED7AFA 418B0E4E
EBECA993 DB583AC9 B7E659DF 0271A584 FE59A840 05D212B3 61110831 8C1D55F4
387E55D0 179E0308 0346B344 A4C58D67 0CB62D17 CEC36FBD 95F76BA8 D0D5D643
FB0D3F27 FDDC29C0 38B4E589 1E657736 1F3B837F 482CA6D1 05022736 AFE3C669
6FDA5E66 AA4F632A 9C1B9B6A 7114D4AF CF16FF6F D4311160 1954FAC9 8FEEAFC6
EEAC2800 EDFA4089 6E4AE45D 9429C52B 7D926DB4 316D9842 DFC63E78 51415670
8095FB34 FFB2AEBE 3B16C1FE 0F7CDD24 74226AED 4356AB9B 217FE97D 6E2CFBA2
74389259 5BD2BE32 AEDA1CED 452B38AA 7A8CF638 B3092648 A683EF46 59644108
E7684A3C DD61D773 E020C0F1 C78478C0 EA53E700 DF75C22B 5E2A1E3D 1E1D791C
E1F264E2 82AF38C4 F63F7ACB 70CA5D4B EB65925C 57283857 A0E222
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
AC3E6ECD

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Client message

0403

client -> server:
```

```
write_sequence
00000000 00000002
header type
17 (application data)
major version
03
minor version
01
length
0002
data encrypted on client write key using parameters 1.2.643.7.1.2.5.1.1
(id-tc26-gost-28147-param-Z) in CNT mode
4A03
MAC on client write MAC secret using parameters 1.2.643.7.1.2.5.1.1 (id-
tc26-gost-28147-param-Z)
D913A774
```

Приложение В Модули ASN.1

```
Gost-CryptoPro-TLS
Gost-CryptoPro-TLS { iso(1) member-body(2) ru(643) rans(2)
    cryptopro(2) other(1) modules(1) gost-CryptoPro-TLS(16) 1 }

DEFINITIONS ::=
BEGIN
-- EXPORTS ALL --
-- Типы и значения, определенные в этом модуле, экспортируются для
-- использования в других модулях ASN.1, содержащихся в российских
-- криптографических спецификациях «ГОСТ» и «ГОСТ Р», и для использования
-- другими приложениями для получения доступа к российским службам
-- криптографии. Другие приложения могут использовать их в своих целях, но
-- это не накладывает ограничений на расширения и изменения, необходимые
-- для поддержания или улучшения российских служб криптографии.

IMPORTS

Certificate, AlgorithmIdentifier
FROM PKIX1Explicit88 {iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-pkix1-explicit-88(1)}

id-CryptoPro-algorithms, gostR3410-EncryptionSyntax
FROM Cryptographic-Gost-Useful-Definitions { iso(1) member-body(2)
    ru(643) rans(2) cryptopro(2) other(1) modules(1)
    cryptographic-Gost-Useful-Definitions(0) 1 }

GostR3410-KeyTransport
FROM GostR3410-EncryptionSyntax gostR3410-EncryptionSyntax;

id-PRF-GostR3411-94 OBJECT IDENTIFIER ::=
    { id-CryptoPro-algorithms prf-gostr3411-94(23) }

TLSProxyKeyTransportBlob ::= SEQUENCE {
    keyBlob             GostR3410-KeyTransport,
    cert                OCTET STRING
}

TLSGostKeyTransportBlob ::= SEQUENCE {
    keyBlob             GostR3410-KeyTransport,
    proxyKeyBlobs       SEQUENCE OF TLSProxyKeyTransportBlob OPTIONAL
}

TLSGostSrvKeyExchange ::= SEQUENCE OF OCTET STRING (CONSTRAINED BY {
    Certificate })

TLSGostExtensionHashHMACSelect ::= SEQUENCE {
    hashAlgorithm       AlgorithmIdentifier,
    hmacAlgorithm       AlgorithmIdentifier,
    prfAlgorithm        AlgorithmIdentifier
}
```

```
TLSGostExtensionHashHMACSelectClient ::=
    SEQUENCE OF TLSGostExtensionHashHMACSelect

TLSGostExtensionHashHMACSelectServer ::= TLSGostExtensionHashHMACSelect

END -- Gost-CryptoPro-TLS
```

Библиография

[**IETF RFC 4357**] В. Попов, И. Курепкин и С. Леонтьев, «Дополнительные алгоритмы шифрования для использования с алгоритмами по ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94» (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, январь 2006 г.

[**IETF RFC 4490**] Под ред. С. Леонтьева и Г. Чудова «Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 с синтаксисом криптографических сообщений (CMS)» (Leontiev, S., Ed. and G. Chudov, Ed., 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, май 2006.

[**IETF RFC 4491**] Под ред. С. Леонтьева и Д. Шефановского «Использование алгоритмов по ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 в профиле сертификата и списка отзыва сертификатов (CLR) инфраструктуры открытых ключей Интернет X.509» (Leontiev, S., Ed. and D. Shefanovskij, Ed., 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, май 2006.

[**IETF RFC 5216**] Д. Симон, Б. Абоба и Р. Харст, «Протокол аутентификации EAP-TLS» (Simon D., Aboba B. and R. Hurst, The EAP-TLS Authentication Protocol), RFC 5216, март 2008 г.

УДК 351.864.1:004:083.131 **ОКС 35.040** **П85**

Ключевые слова:*, электронная коммерция,, безопасность*

Руководитель организации-разработчика:

Генеральный директор
ООО «КРИПТО-ПРО»

_____ Чернова Н.Г.

Руководитель разработки:

Директор по науке
ООО «КРИПТО-ПРО»

_____ Попов В.О.

Авторы документа:

Технический Директор
ООО «КРИПТО-ПРО»

_____ Леонтьев С.Е.

Начальник отдела
защиты информации
ООО «КРИПТО-ПРО»

_____ Смышляев С.В.