ТК26, рабочая группа IPsec
Предварительный документ
<rus-fedchenko-cpike-ipsecme-gost-00-rl>
Предполагаемый статус: Информационный
Действителен: Август 2010

С.Е. Леонтьев, Editor
М.В. Павлов, Editor
CRYPTO-PRO
А.А. Федченко, Editor
S-Terra
December 2009

Использование ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP

rus-fedchenko-cpike-ipsecme-gost-00-rl

Статус документа

[TODO: а надо ли в документе ТК26 авторам предоставлять права, и если надо, то как именно?]

Фактом передачи предварительного документа в ТК26, каждый автор соглашается с неэксклюзивным предоставлением IPR для ТК26, аналогично положениям стандарта Интернет IETF BCP 79.

Данный предварительный документ является открытым документом "Рабочей группы IPsec и IKE", "Технического комитета по стандартизации "Криптографическая защита информации" (ТК26). Область распространения документа не ограничена.

Данный предварительный документ действителен в течении максимум девяти месяцев, и может быть в любое время изменён, заменён на другой или отозван в любое время. При цитировании или ссылке на него из других документов следует ставить отметку, что “документ готовится к публикации”.

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

Этот предварительный документ действителен до Август 2010.

Аннотация

Это предварительный документ на русском языке предназначен для обеспечения совместимости реализаций IPsec IKE и ISAKMP российских производителей, а так же для создания проекта документа IETF.

Этот документ описывает соглашения по использованию алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами Internet Key Exchange (IKE) и Internet Security Association and Key Management Protocol (ISAKMP). Вводится дополнительный метод шифрования вложений ISAKMP, которые используется для управления ассоциациями безопасности (SA). Так же определяются дополнительные группы, параметры ISAKMP SA и методы аутентификации для IKE, который используется для аутентификации сторон, согласования ключей ISAKMP SA, IPsec SA и др.

Лист изменений

Предназначено для подготовки I-D и его поддержки. Убрать в момент публикации RFC.

00-ra 2008-07-26 ЛСЕ	"Рыба", только оглавление и ссылки;
00-rc 2009-02-15 ЛСЕ	Учёт изменений по окончании предварительного криптографического анализа; Изменил выравнивание пакета, с "NoName" по модулю 4 байта, на PKCS#5 по модулю 8 байт;
00-rd 2009-03-01 ЛСЕ	Описание PDF, XML Validated; Подготовлено для согласования с Владимиром Олеговичем Поповым; Вставлено забытая ссылка на UKM из VKO GOST R 34.10-2001. В алгоритме GOST-IKE-KEYEXCHANGE добавлено использование CKI-I/R в качестве UKM.
00-re 2009-03-16 ЛСЕ	Исправлены нестандартные по [KEYWORDS] термины; Уточнено использование encryptECB(K, D).
00-rf 2009-03-16 ЛСЕ	Учёл требования на СКЗИ "КриптоПро CSP".
00-rg 2009-03-01 ЛСЕ	Удалён алгоритм GOST-IKE-KEYEXCHANGE.
00-rh 2009-07-10 ЛСЕ	Уточнено описание по выравниванию PKCS#5.
00-ri 2009-03-16 ЛСЕ	Удалены метки конфиденциальности и Copyright; Добавлены рыбы тестовых примеров; Вставлен редактор английского перевода;
00-rj 2009-12-01 ПВО & ЛСЕ	Внесено описание хэш-функции ГОСТ Р 34.11-94, что бы убрать нормативную ссылку на [draft.СРАН]; Исправлены формулы вычисления SK_a и SK_e; Исправлена формула вычисления SKEYID для GOST-IKE-SIGNATURE;
00-rk 2009-12-07 ЛСЕ	Учтены остальные замечания Смыслова Валерия Анатольевича, ОАО "ЭЛВИС-ПЛЮС";
00-rl 2009-12-08 ПВО & ЛСЕ	Исправлены примеры.

Авторское замечание

Предназначено для подготовки I-D и его поддержки. Убрать в момент публикации RFC.

Описание формата проекта RFC в XML (Internet drafts или I-D), методы просмотра, форматирования и редактирования описаны [draft.RFC2629bis] [RFC2629] [XML2RFC] [ID-Checklist] [xml2rfc-validator]

Текущий регистр [DOI] http://www.iana.org/assignments/isakmp-registry [isakmp-registry]

Текущий регистр [IKE] http://www.iana.org/assignments/ipsec-registry [ipsec-registry]

Должен нормально просматриваться в любом достаточно современном browser-е при активном подключении к сети Интернет.

Извините за язык "падонков", но используем шаблон [XML2RFC] на английском языке, хотя и пишем по-русски.

При преобразовании в PDF следует настроить FO процессор на использование встраиваемых русских шрифтов, см. Кратчайший путь к DocBook [1].

[1] http://docbook.ru/doc/sw/foproc.html

В документе используются применяемые в IETF расширения " Draft HTML and PDF from XML source [2]", поэтому после перевода на английский надо будет применять XSLT преобразование "xml2rfc\rfc2629xslt\clean-for-DTD.xslt" перед вызовом "xml2rfc\xml2rfc.tcl" для получения текстового файла.

[2] http://greenbytes.de/tech/webdav/rfc2629xslt/rfc2629xslt.html

Содержание

1. Введение

Протокол [IKE] в архитектуре [ISAKMP] используется для обеспечения аутентификации сторон и согласований ключей, как ISAKMP SA, так и целевых не-ISAKMP SA (обычно IPsec SA).

Этот документ описывает использование ГОСТ 28147-89 [GOST28147], ГОСТ Р 34.11-94 [GOST3431095] [GOSTR341194] и ГОСТ Р 34.10-2001 [GOST3431004] [GOSTR341001] в IKE и ISAKMP, но не определяет сами алгоритмы и форматы представления криптографических типов данных. Алгоритмы описываются соответствующими национальными стандартами, а представление данных и параметров соответствует следующими документам IETF [CPALGS] [CPPK] [CPCMS].

Определяет хэш алгоритм GOST_R_34_10_94 для использования в [IKE].

ISAKMP вложения обрабатываются в рамках ISAKMP SA, параметры которой интерпретируются согласно [IKE]. Этот документ описывает также дополнительные идентификаторы расширяющие [IKE].

2. Терминология

Термины "ДОЛЖНО", "ДОЛЖНА", "ДОЛЖНЫ", "ДОЛЖЕН" (MUST, REQUIRED, SHALL), "НЕ ДОЛЖЕН", "НЕ ДОЛЖНЫ" (MUST NOT, SHALL NOT), "РЕКОМЕНДОВАНО" (SHOULD, RECOMMENDED), "НЕ РЕКОМЕНДОВАНО" (SHOULD NOT, NOT RECOMMENDED), "МОГУТ", "МОЖЕТ" (MAY, OPTIONAL) в рамках этого документа ДОЛЖНЫ интерпретироваться в соответствии с RFC 2119 [KEYWORDS].

Основные обозначения и определения к данном документе соответствуют принятым в [IKE]. Отличия связаны с использованием самостоятельных алгоритмов приведены ниже.

encryptCFB(IV, K, D):	шифрование ГОСТ 28147-89 в режиме "гаммирования с обратной связью" на ключе K данных D с начальным вектором IV (Section 1.1 of [CPALGS], Section 4 of [GOST28147], [Schneier95]). Узел замены согласовывается Раздел 7.2;
decryptCFB(IV, K, D):	расшифрование ГОСТ 28147-89 в режиме "гаммирования с обратной связью" на ключе K данных D с начальным вектором IV (Section 1.1 of [CPALGS], Section 4 of [GOST28147], [Schneier95]). Узел замены согласовывается Раздел 7.2;
encryptECB(K, D):	шифрование данных D ГОСТ 28147-89 в режиме "простой замены" на ключе K (Section 1.1 of [CPALGS], Section 2 of [GOST28147], [Schneier95]);
decryptECB(K, D):	расшифрование данных D ГОСТ 28147-89 в режиме "простой замены" на ключе K (Section 1.1 of [CPALGS], Section 2 of [GOST28147], [Schneier95]);
Divers(K,D):	алгоритм диверсификации ключа K по данным D (Section 7 of [CPALGS]). Узел замены определяется Раздел 7.2;
gost28147IMIT(IV, K, D):	выработка имитовставки ГОСТ 28147-89 на ключе K от данных D, с внутренним выравниванием нулями до границы блока 8 байт (Section 1.1 of [CPALGS], Section 5 of [GOST28147], описание и пример сетевого представления результата приведён в [CPCMS], Section 9.2, 9.3). Узел замены согласовывается Раздел 7.2;
HASH(D):	расчёт хэш функции с внутренним выравниванием по ГОСТ Р 34.11-94. Описана п. 3 [draft.CPAH], п. 2.1 [CPCMS];
KE:	открытый ключ асимметричной ключевой пары, представляется в виде последовательности октетов согласно п. 2.3.2 [CPPK], тип GostR3410-2001-PublicKey, длинной 64 байта;
K_i:	закрытый ключ Инициатора;
KE_i:	открытый ключ Инициатора;
K_r:	закрытый ключ Ответчика;
KE_r:	открытый ключ Ответчика;
gx:	открытый ключ без параметров, представляется в виде последовательности октетов согласно п. 2.3.2 [CPPK], тип GostR3410-2001-PublicKey, длинной 64 байта;
Crt_i:	значение открытого ключа сертификата Инициатора;
Crt_r:	значение открытого ключа сертификата Ответчика;
(x_i, gx_i):	значение асимметричной ключевой пары Инициатора на согласованных параметрах группы, параметры группы также

	могут наследоваться от сертификата получателя, что также может обозначаться (x_i , g(Crt_r)x_i);
(x_r, gx_r):	значение асимметричной ключевой пары Ответчика;
(x_i, g(Crt_r)x_i):	значение асимметричной ключевой пары Инициатора с параметрами сертификата Ответчика;
(x_r, g(Crt_i)x_r):	значение асимметричной ключевой пары Ответчика с параметрами сертификата Инициатора;
VKO(x_i, gx_r, ukm):	алгоритм выработки сессионного ключа на основе алгоритма Диффи-Хеллмана в соответствии с "VKO GOST R 34.10-2001", Section 5.2 of [CPALGS];
akey:	конкатенация одного или двух результатов VKO(), является согласованным ключом фазы 1;
prf(K,D):	ключевая функция порождения псевдослучайных величин HMAC_GOSTR3411(K,D). Описана Section 3 of [CPALGS];
Last_ICV:	накопленная имитовставка обмена фазы 1 (переданная в последнем пакете фазы 1);
AUTH-I, AUTH-R:	результаты аутентификации Инициатора и Ответчика соответственно, 32-байтовые величины;
substr(s..f, bytes):	последовательность байт с байта s, по байт f, выбранная из представленной в сетевом порядке последовательности bytes;
bits[s..f]:	последовательность бит с бита s, по бит f, выбранная из представленной в сетевом порядке последовательности bits;
Signature(d, h):	вычисляет значение ЭЦП ГОСТ Р 34.10-2001 по значению хэш-функции ГОСТ Р 34.11-94 h на основе закрытого ключа d [GOSTR341001];

3. Хэш функция ГОСТ Р 34.11-94

Данный документ определяет использование идентификатора GOST_R_34_10_94 хэш-функции ГОСТ Р 34.11-94 в [IKE]. Построение HMAC и PRF на её основе определяется [CPALGS], Section 3, 4. Представление значений ГОСТ Р 34.11-94, а так же HMAC и PRF на её основе, определяется Section 2.1 of [CPCMS].

В данном документе используется ГОСТ Р 34.11-94 с параметрами id-GostR3411-94-CryptoProParamSet, смотри Section 8.2 of [CPALGS].

4. Шифрование ISAKMP вложений по ГОСТ 28147-89

Если в заголовке ISAKMP установлен бит E(ncryption Bit) (такой заголовок изображается, как "HDR*"), то пакет (все вложения) шифруется, в рамках ISAKMP SA. Шифрование пакетов ISAKMP с одинаковым Message-ID осуществляется последовательно в порядке обмена. Последовательности с разными Message-ID != 0 могут обрабатываться параллельно.

4.1 Требования к фазе 1

Под фазой 1 понимаем обмен с M-ID == 0, при этом ISAKMP SA должна удовлетворять следующим условиям:

- Согласован алгоритм и параметры шифрования и имитозащиты ГОСТ 28147-89;
- Согласован алгоритм (параметры) хэширования ГОСТ Р 34.11-94;
- Согласованы эфемерные ключи Инициатора и Ответчика gx_i и gx_r;
- Вычислен ключ SKEYID-e;
- Аутентификация сторон фазы 1 ещё не закончена.

Message-Nonce - последовательность 8 нулей;

AUTH-I - пустая последовательность;

AUTH-R - пустая последовательность;

IV = substr(0..7, HASH(gx_i|gx_r))

4.2 Требования к фазе 2

Под фазой 2 понимаем обмен с Message-ID != 0, при этом ISAKMP SA должна удовлетворять следующим условиям:

- Согласован алгоритм и параметры шифрования и имитозащиты ГОСТ 28147-89;
- Согласован алгоритм (параметры) хэширования ГОСТ Р 34.11-94;
- Согласован ключ SKEYID_e;
- Имитовставка пакетов фазы 1 Last-phase-1-ICV успешно вычислена и проверена;
- Аутентификация сторон успешно завершена, в том числе рассчитаны AUTH-I и AUTH-R;

Message_Nonce = случайная величина, выработанная одновременно с Message-ID. Для всех пакетов с одинаковым Message-ID используется один и тот же Message-Nonce.

IV = substr(0..7, HASH(Last_ICV|Message-ID|Message-Nonce))

4.3 Шифрование и имитозащита

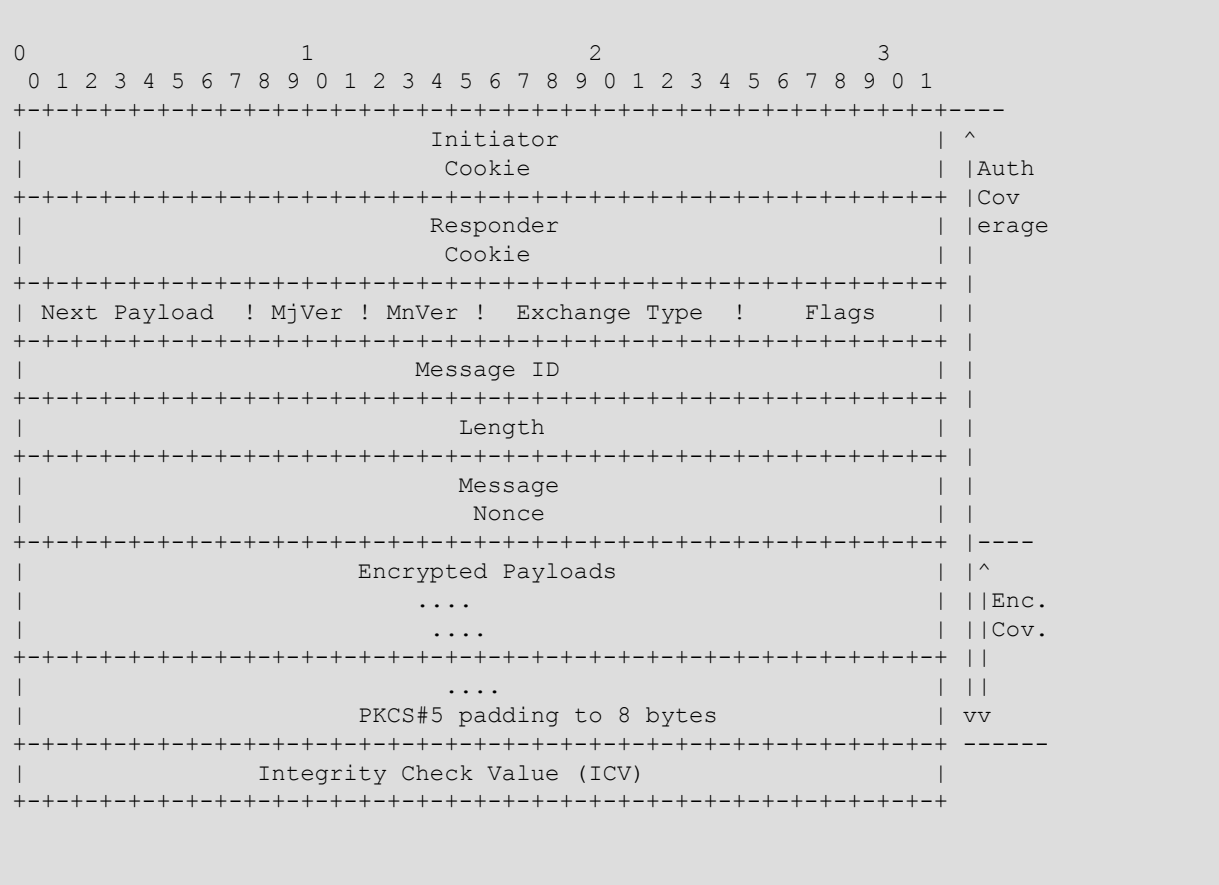

Figure 1: Формат зашифрованого по ГОСТ 28147-89 пакета ISAKMP

Данные для шифрования ГОСТ 28147-89 выравниваются до границы 8 байт по PKCS#5 до вычисления ICV.

Согласно Section 3.1 of [ISAKMP] (смотри так же, Appendix B, стр. 38 [3], 4-ый параграф сверху [IKE]), Length - Length of total message (header + payloads + Message Nonce Len (8) + Padding Length + ICV Len (4)) in bytes. Вычисляется и заполняется до имитозащиты и шифрования.

Message Nonce - не шифруется, участвует в вычислении имитовставки.

Ключ шифрования SK_e и ключ имитозащиты SK_a вычисляется по формулам:

SK_a = SK_e = prf(SKEYID_e, Message-ID|Message-Nonce|AUTH-I|AUTH-R)

Имитовставка вычисляется до зашифрования, но после выравнивания. Ключ SK_a используется в режиме CryptoPro Key Meshing (id-Gost28147-89-CryptoPro-KeyMeshing). Производится сквозное вычисление имитовставки по всей последовательности переданных пакетов с одинаковыми Message-ID и Message-Nonce.

ICV = gost28147IMIT(0, SK_a, [пакет 1]|[пакет 2]...|[текущий пакет])

Шифрование производится в режиме encryptCFB, Section 1.1 of [CPALGS], (режим гаммирования с обратной связью по алгоритму ГОСТ 28147-89, [GOST28147]) на ключе SK_e и синхропосылке IV, Section 3.2.3 of [CPALGS]. Ключ SK_e используется в режиме CryptoPro Key Meshing, Section 3.2.3 of [CPALGS].

Все пакеты с одинаковым Message-ID, кроме первого шифруются с использованием синхропосылки, полученной при обработке предыдущего пакета. Все пакеты на зашифрование и расшифрование обрабатываются последовательно в порядке передачи и приёма из канала связи.

[3] http://tools.ietf.org/html/rfc2409#page-38

При несовпадении рассчитанной имитовставки принятого и расшифрованного пакета со значением поля ICV, получателю РЕКОМЕНДОВАНО вернуть состояния ключа шифрования и объекта вычисления имитовставки в состояние, соответствующее состояниям этих объектов до начала обработки пакета.

5. Методы аутентификации по ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001

В протоколе IKE/GOST создаются ключи группы SKEYID, используемые для выработки ключей в фазах 1 и 2 IKE/GOST:

SKEYID_d = prf(SKEYID, akey | CKY-I | CKY-R | 0);

SKEYID_a = prf(SKEYID, SKEYID_d | akey | CKY-I | CKY-R | 1);

SKEYID_e = prf(SKEYID, SKEYID_a | akey | CKY-I | CKY-R | 2).

На фазе 1 IKE/GOST может использоваться один из двух методов аутентификации:

- аутентификация на предварительно распределяемых ключах (GOST-IKE-PSK);
- аутентификация с использованием ЭЦП (GOST-IKE-SIGNATURE).

В качестве аутентифицирующих элементов используются AUTH-I и AUTH-R и объекты типа "хэш":

HASH_I = prf(SKEYID, gx_i | gx_r | CKY-I | CKY-R | SAi_b | IDii_b);

HASH_R = prf(SKEYID, gx_r | gx_i | CKY-R | CKY-I | SAi_b | IDir_b).

Аутентификация фазы 1 завершается либо успехом, либо ошибкой аутентификации при ошибке проверки хотя бы одной величины HASH_I, HASH_R, SIG_I или SIG_R.

При использовании быстрого (агрессивного) режима в методах GOST-IKE-PSK и GOST-IKE-SIGNATURE НЕ ДОЛЖНА использоваться опциональнбая возможность протокола [IKE] по передаче последнего (3-го) пакета в открытом виде, поэтому последний пакет этого режима изображается, как HDR*.

5.1 Метод GOST-IKE-PSK

Аутентификация GOST-IKE-PSK требует, чтобы процессу ISAKMP был установлен предварительно распределённый ключ PSK, передаваемый модулю IKE/GOST на этапе согласования ключей.

```
 Initiator                              Responder
-----------                            -----------
HDR, SA                        -->
                               <--     HDR, SA
HDR, KE_i, Ni                  -->
                               <--     HDR, KE_r, Nr
HDR*, IDii, HASH_I             -->
                               <--     HDR*, IDir, HASH_R
```

Figure 2: Основной режим GOST-IKE-PSK

```
 Initiator                              Responder
-----------                            -----------
HDR, SA, KE_i, Ni, IDii        -->
                               <--  HDR, SA, KE_r, Nr, IDir, HASH_R
HDR*, HASH_I                   -->
```

Figure 3: Быстрый (агрессивный) режим GOST-IKE-PSK

Для данного режима определяются параметры:

akey = VKO(x_i, gx_r, 0) = VKO(x_r, gx_i, 0)

SKEYID = prf(PSK, Ni_b | Nr_b).

В процедуре выработки ключей защиты ISAKMP SA для алгоритмов шифрования id-Gost28147-89-CryptoPro-*-ParamSet Раздел 4.2 используются параметры:

AUTH-I = HASH(HASH_I)

AUTH-R = HASH(HASH_R)

5.2 Метод GOST-IKE-SIGNATURE

Аутентификация на ключах подписи GOST-IKE-SIGNATURE требует, чтобы процессом ISAKMP был установлен ключ подписи пользователя. Также ISAKMP должен либо найти сертификат оппонента в хранилищах сертификатов компьютера, либо запросить сертификат у противоположной стороны запросом CERTREQ. Сертификат противоположной стороны должен быть проверен, разобран, а сформированный по этому сертификату открытый ключ передан модулю IKE/GOST на этапе согласования ключей.

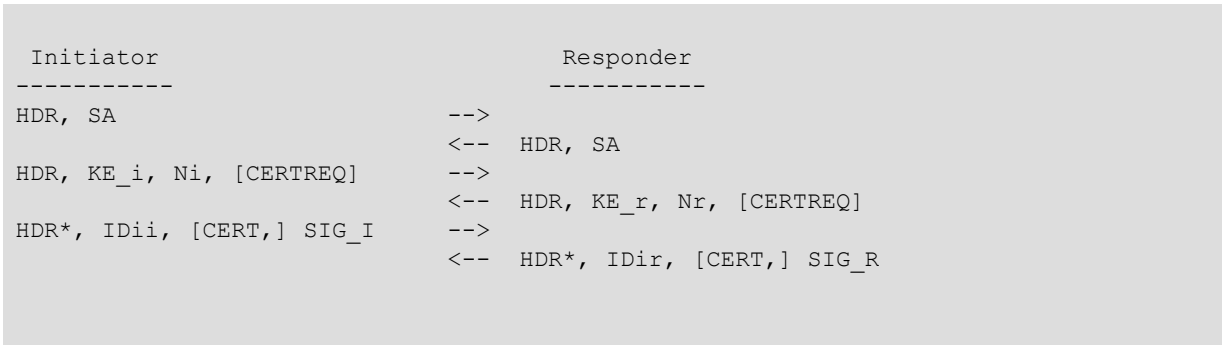

Figure 4: Основной режим GOST-IKE-SIGNATURE

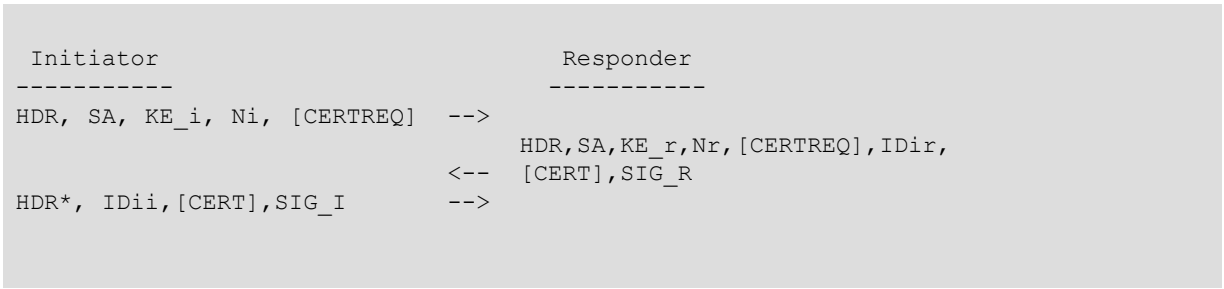

Figure 5: Быстрый (агрессивный) режим GOST-IKE-SIGNATURE

Для данного режима определяются параметры:

akey = VKO(x_i, gx_r, 0) = VKO(x_r, gx_i, 0);

SKEYID = prf(Ni_b | Nr_b, akey);

SIG_I = Signature(K_i, HASH_I);

SIG_R = Signature(K_r, HASH_R);

ЭЦП SIG_I и SIG_R определяется Section 3 of [CPCMS], как последовательность байт длины 64.

В процедуре выработки ключей защиты ISAKMP SA для алгоритмов шифрования id-Gost28147-89-CryptoPro-*-ParamSet Раздел 4.2 используются параметры:

AUTH-I = HASH(SIG_I | Cert_I);

AUTH-R = HASH(SIG_R | Cert_R).

6. Обмены фазы 2 протокола IKE/GOST

Каждый обмен IKE/GOST, следующий после окончания фазы, защиту пакетов ISAKMP SA на основе SKEYID_e. Каждая сессия идентифицируется собственным уникальным Message-ID, отличным от 0.

Сессия определяется одним из следующих режимов:

- Quick Mode;
- Новая группа параметров;
- Информационный обмен.

Реализация этих режимов должны удовлетворять [IKE].

Счётчик числа сессий ДОЛЖЕН увеличиваться в момент инициирования сесий "Quick Mode", "Новая группа параметров" и "Информационный обмен".

Сессии этих фаз завершается либо успехом, либо ошибкой аутентификации при несовпадении значений хотя бы одной из трёх величин HASH(1), HASH(2), HASH(3).

6.1 Уточнение использования ГОСТ Р 34.11-94 и ГОСТ 34.10-2001 в Quick Mode

Если при согласовании ISAKMP SA было согласовано значение "Disable Non-PFS" (65513) атрибута "PFS Control" (32507), то на фазе II согласуются "Quick Mode" только PFS.

Для каждого SPI вырабатывается, для ESP SA [draft.CPESP]:

- Kr_e (K1, Section 5.5 of [IKE]);
- Kr_i (K2, Section 5.5 of [IKE]);
- SPIcookie = substr(0..3, CKY-I) + substr(0..3, CKY-R) + substr(4..7, Message-Nonce) (mod 2^32);

Для AH SA [draft.CPAH]:

- Kr_i (K1, Section 5.5 of [IKE]);

Общее количество SPI, которые порождаются одной "Quick Mode" НЕ ДОЛЖНО превышать 100.

7. Дополнительные параметры и атрибуты ISAKMP SA

Для согласования атрибутов методов Раздел 5 в процессе согласования параметров ISAKMP SA [ISAKMP] [IKE] обе стороны ДОЛЖНЫ послать IKE_GOST vendor ID. Формат IKE_GOST vendor ID следующий:

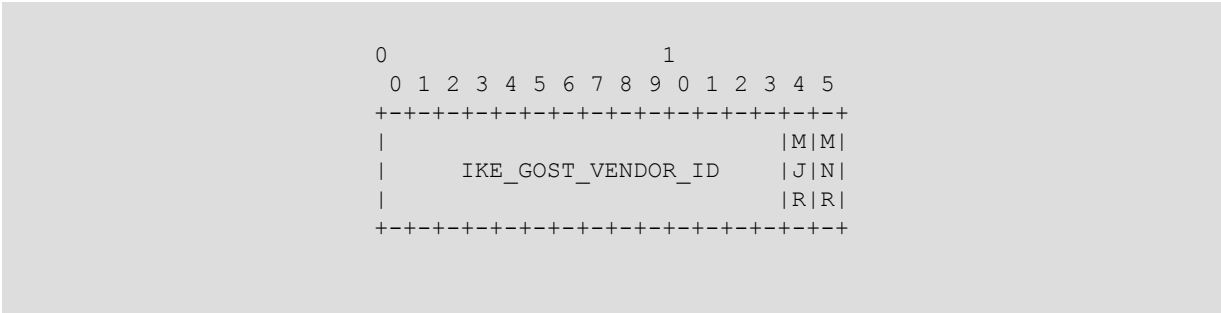

Figure 6: IKE_GOST-VENDOR-ID

где IKE_GOST_VENDOR_ID = { '\x03', '\x10', '\x17', '\xE0', '\x7F', '\x7A', '\x82', '\xE3', '\xAA', '\x69', '\x50', '\xC9', '\x99', '\x99' } (первые 14 байт ГОСТ Р 34.11-94 хэш от char строки "IKE/GOST"), а MJR и MNR соответствуют текущей major и minor версии преобразований IKE_GOST (т.е. 1 и 0). [rfc.comment.1]

Параметр	Атрибут	Формат	Умолчание
алгоритм шифрования	1	B	-
алгоритм хэширования	2	B	-
метод аутентификации IKE	3	B	-
описание группы	4	B	-
тип группы	5	B	-
Max Messages	32506	B	2^7
PFS Control	32507	B	Enable Non-PFS (65512)

Table 1: Параметры ГОСТ ISAKMP SA

7.1 Алгоритм хэширования ГОСТ Р 34.11-94 и параметры

Для атрибута "алгоритм хэширования" (2) используется идентификатор хэш функции GOST_R_34_10_94 <TBD+1>.

7.2 Алгоритм ГОСТ 28147-89 и параметры

Для атрибута "алгоритм шифрования" (1) используется идентификаторы режимов и параметров ГОСТ 28147-89:

Mode	GOST-28147-89 S-Box	Значение
CFB	id-Gost28147-89-CryptoPro-A-ParamSet	<TBD+2>
CFB	id-Gost28147-89-CryptoPro-B-ParamSet	<TBD+3>
CFB	id-Gost28147-89-CryptoPro-C-ParamSet	<TBD+4>
CFB	id-Gost28147-89-CryptoPro-D-ParamSet	<TBD+5>

Table 2: Параметры ГОСТ 28147-89 ISAKMP SA

7.3 Идентификаторы методов IKE/GOST

Для атрибута "метод аутентификации IKE" (3) используется:

[rfc.comment.1] Идею использования MJR и MNR в Vendor ID позаимствовали из RFC 3706

Метод	Значение
IKE-GOST-PSK	<TBD+6>
IKE-GOST-SIGNATURE	<TBD+8>

Table 3: Параметры ГОСТ 28147-89 ISAKMP SA

7.4 Описания групп типа VKO GOST R 34.10-2001

Для атрибута "описание группы" (4) используется:

Группа	Значение
id-GostR3410-2001-CryptoPro-XchA-ParamSet+id-GostR3410-94	<TBD+9>
id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3410-94	<TBD+10>

Table 4: Группы типа VKO GOST R 34.10-2001

7.5 Тип VKO GOST R 34.10-2001 для группы IKE

Для атрибута "тип группы" (5) используется:

Тип	Значение
VKO GOST R 34.10-2001	<TBD+11>

Table 5: Типы групп IKE

7.6 Max Messages

Если в режиме Quick Mode является обязательным использование PFS (значение "Disable Non-PFS" (65513) атрибута "PFS Control" (32507)),то максимально допустимое число инициированных сессий с Message-ID не равным 0, согласуемое этим параметром:

- НЕ ДОЛЖНО превышать 2^12;

в противном случае:

- НЕ ДОЛЖНО превышать 2^7.

Вне зависимости от их успешного или неуспешного завершения.

7.7 PFS Control

Для атрибута "PFS Control" (32507) используется:

PFS Control	Значение
Enable Non-PFS	65512
Disable Non-PFS	65513

Table 6: Параметры ГОСТ 28147-89 ISAKMP SA

8. Благодарности

Добрые слова в адрес российских CISCO, CheckPoint и Газпром...-а, который(е) инициировали попытку достижения совместимости...

Выражаем благодарность Чмора Андрею Львовичу, ОАО "Инфотекс", за дискуссию по определению понятия DoS.

Выражаем особую благодарность Смыслову Валерию Анатольевичу, ОАО "ЭЛВИС-ПЛЮС", за большое количество ценных замечаний и улучшений, как в сам протокол, так и в его описание.

Благодарности рецензентам, надеюсь такие найдутся...

9. Авторский коллектив

Адреса авторов


```
Дмитрий Г. Дьяченко
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Владимир О. Попов
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Кирилл А. Корнилов
S-Terra
Зеленоград, МГИЭТ, корпус 10, офис 110
Москва, 124498
Россия
Phone: +7 (495) 726 98 91
Fax: +7 (495) 531 9789
EMail: hell@s-terra.com
URI: http://www.s-terra.ru
```

10. Регистрация IANA

IANA выделяет номер хэш функции IKE для использования ГОСТ Р 34.11-94:

<TBD+1> для GOST_R_34_10_94.

IANA выделяет четыре номера алгоритмов шифрования IKE для использования ГОСТ 28147-89:

<TBD+2> для GOST-A-CFB-IMIT;

<TBD+3> для GOST-B-CFB-IMIT;

<TBD+4> для GOST-C-CFB-IMIT;

<TBD+5> для GOST-D-CFB-IMIT.

IANA выделяет два номера методов аутентификации IKE для использования ГОСТ 28147-89:

<TBD+6> для IKE-GOST-PSK;

<TBD+8> для IKE-GOST-SIGNATURE.

IANA выделяет два номера описания груп:

<TBD+9> для VKO GOST R 34.10-2001 XchA;

<TBD+10> для VKO GOST R 34.10-2001 XchB.

IANA выделяет номер типа группы:

<TBD+11> для VKO GOST R 34.10-2001.

10.1 Удалить после регистрации в IANA

Пока, предварительные реализации используют следующие приватные номера преобразований:

65501 для GOST_R_34_10_94;

65502 для GOST-A-CFB-IMIT;

65503 для GOST-B-CFB-IMIT;

65504 для GOST-C-CFB-IMIT;

65505 для GOST-D-CFB-IMIT;

65506 для IKE-GOST-PSK;

65508 для IKE-GOST-SIGNATURE;

65509 для VKO GOST R 34.10-2001 XchA;

65510 для VKO GOST R 34.10-2001 XchB;

65511 для VKO GOST R 34.10-2001.

10.2 Регистрации в IANA не подлежит

Используемые в этом документе приватные номера классов и значений:

Класс	Значения	Ссылка	Тип
Max Messages	32506	B	[draft.CPIKE]
PFS Control	32507	B	[draft.CPIKE]

Table 7: ESP_GOST "magic numbers"

и приватные значения, описанные Раздел 7.2.

11. Обсуждение требований по безопасности

Совместимые приложения ДОЛЖНЫ использовать случайные значения Message-Nonce, Ni, Nr, эфемерных ключей xi и xr. Получатель МОЖЕТ может проверять, что Message-Nonce, Ni, Nr, и эфемерные открытые ключи KEi and KEr, полученные от отправителя, являются уникальными.

РЕКОМЕНДОВАНО, что бы приложения контролировали подписи, открытые ключи и параметры алгоритмов на соотвествие стандарту [GOSTR341001] перед их использованием.

Параметры криптографических алгоритмов влияют на стойкость. Использование параметров, которые не перечислены в [CPALGS], НЕ РЕКОМЕНДОВАНО без соответствующих исследований Section 9 of [CPALGS].

При проектировании приложений следует учитывать степень защиты информации передаваемой на первой фазе протокола IKE (IDi*, CERT*):

GOST-IKE-PSK:	Полностью защищает информацию только третьего пакета быстрого (агрессивного) режима и 5(6) пакета основного режима. Информация передаваемая до этого передаётся в открытом виде, её целостность обеспечивается по результатам успешной аутентификации;
GOST-IKE-SIGNATURE:	Полностью защищает информацию только третьего пакета быстрого (агрессивного) режима и 6 пакета основного режима. Информация передаваемая в 5 пакете основного режима (IDii, CERTi и т.д.) может быть доступна "нарушителю посередине".

TODO: переработать требования к сертификатам
Use of the same key for signature and key derivation is NOT RECOMMENDED. When signed CMS documents are used as an analogue to a manual signing, in the context of Russian Federal Electronic Digital Signature Law [RFEDSL], signer certificate MUST contain the keyUsage extension, it MUST be critical, and keyUsage MUST NOT include keyEncipherment or keyAgreement (see [PROFILE], Section 4.2.1.3). Application SHOULD be submitted for examination by an authorized agency in appropriate levels of target_of_evaluation (TOE), according to [RFEDSL], [RFLLIC], and [CRYPTOLIC].

TODO: не забыть про опечатку в Section 4.4.2.1 of [ARCH] и OCSP.

Приложения РЕКОМЕНДОВАНО исследовать установленным порядком на соответствие заданным требованиям согласно [RFLLIC], и [CRYPTOLIC].

Приложениям РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA), как по времени, так и по объёму переданной информации Section 4.4.2.1 of [ARCH]. НЕ РЕКОМЕНДОВАНО согласовывать время жизни SA (Lifetime SA) в секундах более, чем на 86400 сек (1 сутки).

11.1 Рекомендации по согласованию безопасных параметров

11.2 Ограничение на IKE и ISAKMP

New Group... E(ncryption bit) и A(uthentification) bit...

12. Примеры

Представление данных в примерах:

0xNNNN:	Представление целого числа в шестнадцатеричной системе счисления, а также представление объктов в форме big-endian;
0xFFFFFFFF FF...:	Представление объктов в форме big-endian;
BBBBBBBB BB:	Представление в сетевой нотации. Числа в big-endian. Сетевое представление сложных объектов согласно стандартам их определяющих, в частности, ключей и хэшей согласно [CPALGS], [CPCMS] и [CPPK] [rfc.comment.2]

[rfc.comment.2] Рабочее название "little-endian", хотя это и не совсем так.

12.1 Примеры значений HMAC_GOSTR3411

Тестовый пример GOSTR3411(text)

```
Значение хэш-функции для сообщений с тестовыми параметрами
алгоритма id-GostR3411-94-TestParamSet (1.2.643.2.2.30.0)
согласно [CPALGS] и [GOSTR341194].

A) Сообщение ([GOSTR341194] п. A.3.1 и
   [draft.ENG-GOSTR341194] п. 7.3.1):

   text (ASCII) =   "This is message, length=32 bytes"
   text (in hex) =  54686973 20697320 6D657373 6167652C
                    206C656E 6774683D 33322062 79746573

   GOSTR3411 =      b1c466d3 7519b82e 8319819f f32595e0
                    47a28cb6 f83eff1c 6916a815 a637fffa


B) Сообщение ([GOSTR341194] п. A.3.2 и
   [draft.ENG-GOSTR341194] п. 7.3.2):

   text (ASCII) =   "Suppose the original message has length = 50 bytes"
   text (in hex) =  53757070 6F736520 74686520 6F726967
                    696E616C 206D6573 73616765 20686173
                    206C656E 67746820 3D203530 20627974
                    6573

   GOSTR3411 =      471aba57 a60a770d 3a761306 35c1fbea
                    4ef14de5 1f78b4ae 57dd893b 62f55208

Значение хэш-функции для сообщений с рабочими (применяемыми
в IPsec/IKE) параметрами алгоритма хэширования
(id-GostR3411-94-CryptoProParamSet или 1.2.643.2.2.30.1)
согласно [CPALGS] и [CPCMS].

C) Сообщение:

   text (ASCII) =   "Suppose the original message has length = 50 bytes"
   text (in hex) =  53757070 6F736520 74686520 6F726967
                    696E616C 206D6573 73616765 20686173
                    206C656E 67746820 3D203530 20627974
                    6573

   GOSTR3411 =      c3730c5c bccacf91 5ac29267 6f21e8bd
                    4ef75331 d9405e5f 1a61dc31 30a65011

[ENG-GOSTR341194.draft] [TODO: Взять реквизиты из текущего draft]
<http://tools.ietf.org/html/draft-dolmatov-cryptocom-gost341194-02>
(Work in progress)
```

Пример prf(K, text) (==HMAC_GOSTR3411(K, text))

```
K =              733d2c20 65686573 74746769 79676120
                 626e7373 20657369 326c6568 33206d54  (32 bytes)
text (ASCII) =   "This is message, length=32 bytes"
text (in hex) =  54686973 20697320 6D657373 6167652C
                 206C656E 6774683D 33322062 79746573

HMAC_GOSTR3411 = 4ff66c94 bddaae61 13360514 2b582b9c
                 0f38bbdf f3d7f0ee 6a9c935d 92bfa107
```

12.2 Пример GOST-IKE-PSK

TODOXX: предварительная версия примера

```
В примерах используются параметры ассоциации безопасности, принятые по умолчанию:
шифрование обмена ISAKMP с узлом замены id-Gost28147-89-CryptoPro-B-ParamSet
в режиме CRYPT_MODE_CFB, CRYPT_PROMIX_MODE;
параметры алгоритма VKO - id-GostR3410-2001-CryptoPro-XchB-ParamSet+id-GostR3411-94.
Время использования PSK:  UTC Mon Oct 02 09:11:55 2009.

|>Example-GOST-IKE-PSK.bin
IKE ph1   Main Mode   PSK Authentication
время использования psk:   UTC Mon Oct 02 09:11:55 2009

 Initiator PSK
 SiteID   11783
 SiteNetID  Net73
 PSK_a  D74RLXM4UE1FQC834G3EQBZAZ51W
 PSK 0x
8c57daa5 a5f2be3c 7330de68 6fc85bc2 86e723cb 5a816bb7 978e7e0b 1bdcbce7
 Responder PSK
 SiteID   01:23:45:67:89:01:23456789012345678901234567890
 SiteNetID  Net73
 PSK_a  BXAF0VM9VG4RPCDKVEK83ZU9LZ1W
 PSK 0x
8c57daa5 a5f2be3c 7330de68 6fc85bc2 86e723cb 5a816bb7 978e7e0b 1bdcbce7

 Diffi-Hellman keys
 Initiator
 CKY-I 0x
04000000 03000000
 Nonce 0x
00000000 00000065 63696f4e 74696e49
 x_i 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 74696e49
 gx_i
 x=0x
683846aa c920d1af 0b835b8e a1697496 d2068eea 5504edcc 472796e2 0c8a6520
 y=0x
895776c7 866895f6 c0316dac 96545690 61919b47 9dfae57a 984fabb0 1005c337
 Responder
 CKY-R 0x
04000000 04000000
 Nonce 0x
00000000 00000065 63696f4e 70736552
 x_r 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 70736552
 gx_r
 x=0x
0e8e5776 73d9d92c ffad302b cfa2c141 85727e6f 377630bb a4b013b7 d0e64d59
 y=0x
24a72040 eb72567a bae92700 b75a4826 c3ebb58e 3e976cef 7caaa6e8 08e78633
 akey 0x
cfcec605 92510824 4035636e c37cba10 98dfbfc7 efd22d5d c9fb22df 6f4d0cf7

 SKEYID keys
 SKEYID 0x
b7c19dd9 37939ea6 a521439d bf5ce13e 534160e5 69cffab1 36c7d302 64d5ec59
 SKEYID_d 0x
7a0b2a9f cdedaf4a 03e61694 1ba77362 05a6efd9 c73759c3 e0143815 8c6b7f3d
```

```
 SKEYID_a 0x
c007a797 9eaa9ac2 7a198a11 31b08508 7474d70c b41b7a7c a949b665 55313444
 SKEYID_e 0x
e7c112a8 8dbfe62e cca5f02e 30e29d90 5fc7f7b2 7ebb9e74 47a1bd6e bc26ed85
 SK_a 0x
ee60bcb0 83b5f9ad a7b19261 d8d02252 ea877ca1 7109b2c9 65a7a85e e7f3d09d
 SK_e 0x
ee60bcb0 83b5f9ad a7b19261 d8d02252 ea877ca1 7109b2c9 65a7a85e e7f3d09d
 IV 0x
fec9200a b45c110b

 Authentkaton
 HASH_I 0x
8dd30326 066c9f2f 73b32be5 c1a0b644 2258c143 bb7eeebf 10655309 3b419c97
 HASH_R 0x
9c6e644c 3069489c 55742653 8f8fe00d 3b95a406 d9c5358f 5b867555 cb5cd2cc
 AUTH_I 0x
3f6cca0c f5b9558c 6d847e38 2250b2c4 8ed421c8 4bcb59c7 3d70a25b 31964997
 AUTH_R 0x
26b41754 14863665 bdc63546 961a2604 7a216a31 87b13c83 144d7bd4 b9a7f9db

 Ph 1 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 05010001
Messege ID
 00000000
Lenght
 00000060
Messege-Nonce
 00000000 00000000
 PL
Identification
 08001000
  00000000
  00000001 00000001
Hash
 00002400
  979c413b 09536510 bfee7ebb 43c15822 44b6a0c1 e52bb373 2f9f6c06 2603d38d
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 08001000 00000000 00000001 00000001 00002400 979c413b 09536510
 bfee7ebb 43c15822 44b6a0c1 e52bb373 2f9f6c06 2603d38d 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 48870189 867183aa e7540fc9 4dd3bbb4 1e08195f fd42ce48 514ca0d7
 2f3427bd 3dfd69ed 8b179611 abce17c4 58c07c71 e90dffdf f382d655 a7f7ca31

 Ph 1 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
```

```
 00000004 00000004
Flags
 05010001
Messege ID
 00000000
Lenght
 00000060
Messege-Nonce
 00000000 00000000
 PL
Identification
 08001000
  00000000
  00000002 00000002
Hash
 00002400
  ccd25ccb 5575865b 8f35c5d9 06a4953b 0de08f8f 53267455 9c486930 4c646e9c
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 08001000 00000000 00000002 00000002 00002400 ccd25ccb 5575865b
 8f35c5d9 06a4953b 0de08f8f 53267455 9c486930 4c646e9c 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000060 00000000
 00000000 d3146e1b 28ffca53 a42acd12 afcd55fb 8a00e051 18b51888 90e2b7c5
 9519f417 57deb9bc 8e63ea07 2dc44169 d586c199 5cbb4c17 56ef79a0 7b7e8ee8
LastICV



 IKE ph2   Non PFS

 Quick Mode keys
 Initiator
 Nonce 0x
63696f4e 726f7461 6974696e 495f3270
 Messege Nonce 0x
005f4e5f 4d5f3270
 Responder
 Nonce 0x
63696f4e 7265646e 6f707365 525f3270
 Messege Nonce 0x
005f4e5f 4d5f3270
 SK_a 0x
089966a8 870e10d1 5cce810f 374a5f28 7e2a65c3 23dddb8e 0ad4b9c3 cc595da2
 SK_e 0x
089966a8 870e10d1 5cce810f 374a5f28 7e2a65c3 23dddb8e 0ad4b9c3 cc595da2
 IV 0x
93170a6a fd019360

 spi Initiator -> Responder 0x
34333231
 K1 0x
93384606 364ac23f 8cbc31e3 740a735c 9d1bf663 355c91cd c70dac7a 6f153db6
 K2 0x
c00341ab 7f7fcbf1 65685590 76d601ce de8443ad 3c4264f2 0d71612d 7f1a4ecb

 spi Responder -> Initiator 0x
```

```
31323334
 K1 0x
09567ecf a73a2d97 86f71948 19c574ad 5312f515 4e4d00bf ba34edfc 2d7b7124
 K2 0x
246c00eb c04770b7 f14bc569 e7477f11 4f6475e8 24ada4e6 1874c694 80833421

 Ph 2 Packet 1

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000b0
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 01002400
  918828f7 e54fa536 cb40d539 f6cc3821 52e25380 c597d123 bb51967e beb884d2
Security Association
 0a003000
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
  03000c00
  01fc0000
  00000000
Nonce
 05001400
  70325f49 6e697469 61746f72 4e6f6963
Identification
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 08080808 08080808
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000b0 70325f4d
 5f4e5f00 01002400 918828f7 e54fa536 cb40d539 f6cc3821 52e25380 c597d123
 bb51967e beb884d2 0a003000 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 03000c00 01fc0000 00000000 05001400 70325f49
 6e697469 61746f72 4e6f6963 05000c00 00000000 01020301 00000c00 00000000
 03027d02 08080808 08080808
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000b0 70325f4d
```

```
 5f4e5f00 02238667 aab03043 5b1a4bb7 884e60c5 2941b9c5 15ff7a1d f2608d14
 c807c066 457b3b5e 9b6669d7 a7f1b5f8 32a38267 dc7ef414 d06ca59d 98a465be
 5687fc54 86eb6144 1013fe4c c47a82c5 3257d24d 37271cb6 afe3b9be 6a79310f
 e3fdacbc 1602b5a8 a130baec af8ae4f4 de3b2518 4b9db52a 3c61c482 d0dce5da
 a8edcba3 857a2cff 2a0051a8 f1d42208

 Ph 2 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000a0
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 01002400
  61bc0c15 d1690439 0b53bea5 3222597b daa5a75f aaf387a1 c0368ea2 beb8ce1f
Security Association
 0a002400
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
Nonce
 05001400
  70325f52 6573706f 6e646572 4e6f6963
Identification
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000a0 70325f4d
 5f4e5f00 01002400 61bc0c15 d1690439 0b53bea5 3222597b daa5a75f aaf387a1
 c0368ea2 beb8ce1f 0a002400 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 05001400 70325f52 6573706f 6e646572 4e6f6963
 05000c00 00000000 01020301 00000c00 00000000 03027d02 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000a0 70325f4d
 5f4e5f00 fb1bab8b ac46efc7 a81c8bca b35afc19 07b4a7b0 c79a91eb 6840a860
 0c90257d 09f6ed37 07dcb089 98625051 8762671a a8be5a02 b27eed4c 90c55cf4
 534cbcff 286f2923 ee9ada8d 3e272b24 8ad8e24f 3d3c4c69 253f8beb e0da0d37
 b0907b7e 6dd978d3 10594bbe c24c3e62 6aa5d694 cec75d2e f8a66dfb 147d2969
```

```
 Ph 2 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 00000050
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 00002400
  c61dfce7 db4220ca ea65be60 02f36a0f 32d226ee faa298ed 79621161 e94acce0
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f00 00002400 c61dfce7 db4220ca ea65be60 02f36a0f 32d226ee faa298ed
 79621161 e94acce0 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f00 db8106d1 2349fb88 407a692e 772c769e 5e0dcb9a 20ec1f2f 3590a1de
 638850e0 c640348d 3c8b5397 8cc393d8


 IKE ph2   PFS

 Quick Mode keys
 Initiator
 Nonce 0x
00534650 6563696f 4e74696e 495f3270
 Messege Nonce 0x
505f4e5f 4d5f3270
 x_i 0x
00000000 00000000 00000000 00000000 00000053 46507965 4b74696e 495f3270
 gx_i
 x=0x
96567f88 5edcf177 26b5e9df 64a4aa87 f52db551 a60d241b 6bdc9a82 14b60d63
 y=0x
298bc55b e33916e3 02f10ea1 46cb857b cd6a3dad 40300494 f3e0c983 90b0c61f
 Responder
 Nonce 0x
00534650 6563696f 4e707365 525f3270
 Messege Nonce 0x
505f4e5f 4d5f3270
 x_r 0x
00000000 00000000 00000000 00000000 00000053 46507965 4b707365 525f3270
 gx_r
 x=0x
517fbbc8 ddb119d7 cb54cea0 38fda66f b2ae9fef 5e71d7b5 79961b8e 17fe6c80
 y=0x
2965c2de 8c82ba2a 65fb6455 c2cb08cd 76a06649 2988aa80 330b9ca9 8d72b638
```

```
 gm_ir 0x
692818f6 39b36364 8d4f9bbc 73e9b044 43d86e51 8788acba d89e3169 16465221
 SK_a 0x
073f0f59 75815f47 f0954460 cb26a1cb 30fa6a56 d44a2791 73a688b5 a7c33720
 SK_e 0x
073f0f59 75815f47 f0954460 cb26a1cb 30fa6a56 d44a2791 73a688b5 a7c33720
 IV 0x
b17037eb 7bd91648

 spi Initiator -> Responder 0x
34333231
 K1 0x
9b6a7fda 8d484a43 f9e6ca9b b5a4acc5 be4015a2 c3c8c63d 88c9180b 911e3416
 K2 0x
df487f8a 11492b09 01f27236 a9f17100 164f2ee3 c3ab4798 e0b4eeea cc38f0af

 spi Responder -> Initiator 0x
31323334
 K1 0x
3c86f5e1 28b560ea df2b57bd a0872675 31f79677 b1ef22c4 8f2f329b 01055ec2
 K2 0x
12a86b1d a2cc1d2c 05492e06 94f2724b 848b3f54 d42b7a80 b19d8273 61e42414

 Ph 2 Packet 1

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000f0
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 01002400
  3322ec58 58132288 bb0a486a d0fdfcf0 0e9ec9e7 8de3ad82 cf6a6c45 363876fe
Security Association
 0a003000
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
  03000c00
  01fc0000
  00000000
Nonce
 04001400
  70325f49 6e69744e 6f696365 50465300
Key Exchange
 05004400
```

```
  630db614 829adc6b 1b240da6 51b52df5 87aaa464 dfe9b526 77f1dc5e 887f5696
 1fc6b090 83c9e0f3 94043040 ad3d6acd 7b85cb46 a10ef102 e31639e3 5bc58b29
Identification
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000f0 70325f4d
 5f4e5f50 01002400 3322ec58 58132288 bb0a486a d0fdfcf0 0e9ec9e7 8de3ad82
 cf6a6c45 363876fe 0a003000 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 03000c00 01fc0000 00000000 04001400 70325f49
 6e69744e 6f696365 50465300 05004400 630db614 829adc6b 1b240da6 51b52df5
 87aaa464 dfe9b526 77f1dc5e 887f5696 1fc6b090 83c9e0f3 94043040 ad3d6acd
 7b85cb46 a10ef102 e31639e3 5bc58b29 05000c00 00000000 01020301 00000c00
 00000000 03027d02 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000f0 70325f4d
 5f4e5f50 0046c03b 18d704ad c8bc98d4 db97d881 4c5d37bf 1ede3efa 29ef3528
 f717c5bd ee654aaa dca116bc 56d45870 42b74089 6f6be52e 88ca2620 d45015f0
 e8a0c268 f1563549 a685ca9b 519ee653 92422332 46793cf9 0316a412 48ca56fd
 6ac41aa0 73f5a9b4 1f72298d a91e1256 872f1230 5bdfd456 c43c2138 4a79582d
 5a0266f5 366afbe1 a01c40ca db25ba31 7f0ef36f ef5c5b8f 4c5e02db 90659495
 76ac9051 d4530f3f baa37019 f91e616c 4a4f19d1 d57a353d 73f0b30c f6a64b02
 51103632 b245711f 40b28aea f8a76b2e

 Ph 2 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000e8
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 01002400
  ccbb7089 4fec2da3 ceea2261 ea7ab502 1270326c cee79dd8 64255dcc 0bf2f8f3
Security Association
 0a002400
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
```

```
Nonce
 04001400
  70325f52 6573704e 6f696365 50465300
Key Exchange
 05004400
  806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd c8bb7f51
 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c dec26529
Identification
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 08080808 08080808
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000e8 70325f4d
 5f4e5f50 01002400 ccbb7089 4fec2da3 ceea2261 ea7ab502 1270326c cee79dd8
 64255dcc 0bf2f8f3 0a002400 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 04001400 70325f52 6573704e 6f696365 50465300
 05004400 806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd
 c8bb7f51 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c
 dec26529 05000c00 00000000 01020301 00000c00 00000000 03027d02 08080808
 08080808
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000e8 70325f4d
 5f4e5f50 a6befdfa 421f86bf 1c2a8a26 367dbf89 3c8e7469 9bc2bb73 e137b9b1
 301122b8 1a71738a 2810d890 5440de25 08a71dda 8afbf36e 3d5d4fe5 bdf76b60
 3474eeed 97ee24c3 a6115f2b 06dd8ee4 a7046037 cc609707 346df445 4f47ed29
 e5999dd9 fc16b1a4 2b0faa82 5550a705 0d055f0a 365a4d30 d53c2061 2590cc21
 a4188d88 2d8fce76 81ad46b6 2233d7df 53071e26 7e5e498f a7a8979e 11fed6ac
 8a958040 53a8589b b473ca7e d660b89c 8ce15ffd 56e8ca4b b95711ad a20bd92c
 532450f1 6b144751

 Ph 2 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 00000050
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 00002400
  0e82958c c21148d7 a02199a2 25cdc557 b5bbb354 45039b18 36cba097 6f5909b3
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f50 00002400 0e82958c c21148d7 a02199a2 25cdc557 b5bbb354 45039b18
```

```
 36cba097 6f5909b3 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f50 2ce28a01 ea93a87d 3d332b33 615f47b1 729e761f 34e71412 feb66ece
 4711778c 38717663 831e40ac 7bdeed6a

|<Example-GOST-IKE-PSK.bin
```

12.3 Тестовые пакеты GOST-IKE-SIGNATURE

TODOXX: предварительная версия примера

```
|>Example-GOST-IKE-SIGNATURE.bin
 IKE ph1   Main Mode   Signature Authentication

 Initiator Signature key
 Signature key K_i 0x
feeed8da 176776d4 8bc20bc2 e3fd8847 a34e8339 b8d3428c f1c06fb1 d424b9e7
 KE_i
 x=0x
683846aa 895776c7 866895f6 c0316dac 96545690 61919b47 9dfae57a 984fabb0
 y=0x
895776c7 866895f6 c0316dac 96545690 61919b47 9dfae57a 984fabb0 1005c337
 Cert i 0x
8d381956 96b28a21 aa624128 f66ea1cf dd2c029a 857d1c96 5480f130 acf00676
  081bf2e4 dafd8192 7eb59426 4ef36b42 b961bea4 15fd3fab 3bb551a0 43b2e8d2
  00410303 02020385 2a060608 3005930a 8ee8c975 a5e6420e 72d96b7b 9567c374
  c8140416 040e1d55 03061d30 6dc01929 86fcb409 cff922ce 9dddd3be 71dd5f91
  14801630 1804231d 5503061f 30020208 05050106 2b08060a 300c0425 1d550306
  133080ff 07030305 04ff0101 0f1d5503 060f3066 3068a3b4 d5bfc6be c7d3fc08
  7577f770 6c01f1f6 3c15fe4e e82da53b 8e49ee72 5739c4e9 ad6d75e9 342ea644
  b9d8e613 f83cdf5f 148ab0e2 82aa4fca d7678c33 9405a040 04004303 011e0202
  03852a07 06002402 0203852a 07061230 13020203 852a0606 1c306330 3220746f
  6f52206d 6f726620 74726543 20646e45 20797469 6d726f66 6e6f4320 63655350
  49250c03 04550306 2c302e31 6f72502d 6f747079 7243204f 4f4f0e0c 0a045503
  06153017 31555202 13060455 03060930 0b315630 5a303030 30303031 30313038
  340d175a 31303433 39303231 31313930 0d171e30 3220746f 6f522079 74696d72
  6f666e6f 43206365 53504917 13030455 03061e30 20312230 03020203 852a0606
  08300201 02020102 03a07d01 8230ce01 8230

 Responder Signature key
 Signature key K_r 0x
8ee932fc f8a46163 0dc0a08a c691e20e 7fc40d0e 2881abfe e974ca9a b124cdbf
 KE_r
 x=0x
0e8e5776 24a72040 eb72567a bae92700 b75a4826 c3ebb58e 3e976cef 7caaa6e8
 y=0x
24a72040 eb72567a bae92700 b75a4826 c3ebb58e 3e976cef 7caaa6e8 08e78633
 Cert r 0x
0c47e371 07e8cacd 78961426 7d2e4e8d ce752efb 5f1623f5 0891b7be 30cdaeff
  b3e6d646 f22aeb59 73ad1b44 eb627a04 3a80e3f3 ed64f50c 2bd5d60a bdc8cf0f
  00410303 02020385 2a060608 30a9956c 4c2a9c05 b5bfd98b bcbddddf f7c80d24
  d2140416 040e1d55 03061d30 73f87edb d71444c8 1d71d4fc 855d5e18 dd18c2bb
  14801630 1804231d 5503061f 30020208 05050106 2b08060a 300c0425 1d550306
  133080ff 07030305 04ff0101 0f1d5503 060f3066 3068a3ba 3e69b330 02cf2981
  e9c7be66 5e0dd1c7 0fbac454 1607d71d 201fac2f 71c57fbc 8dc96376 596cead5
  b61765a4 f8565ebc df2be162 baa3c04a c735d437 05c3b140 04004303 011e0202
  03852a07 06002402 0203852a 07061230 13020203 852a0606 1c306330 3320746f
  6f52206d 6f726620 74726543 20646e45 20797469 6d726f66 6e6f4320 63655350
  49250c03 04550306 2c302e31 6f72502d 6f747079 7243204f 4f4f0e0c 0a045503
  06153017 31555202 13060455 03060930 0b315630 5a303030 30303031 30313038
  340d175a 33303433 39303231 31313930 0d171e30 3320746f 6f522079 74696d72
  6f666e6f 43206365 53504917 13030455 03061e30 20312230 03020203 852a0606
  08300301 02020102 03a07d01 8230ce01 8230

 Diffi-Hellman keys
 Initiator
 CKY-I 0x
```

```
04000000 03000000
 Nonce 0x
00000000 00000065 63696f4e 74696e49
 x_i 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 74696e49
 gx_i
 x=0x
683846aa c920d1af 0b835b8e a1697496 d2068eea 5504edcc 472796e2 0c8a6520
 y=0x
895776c7 866895f6 c0316dac 96545690 61919b47 9dfae57a 984fabb0 1005c337
 Responder
 CKY-R 0x
04000000 04000000
 Nonce 0x
00000000 00000065 63696f4e 70736552
 x_r 0x
00000000 00000000 00000000 00000000 00000000 00000000 0079654b 70736552
 gx_r
 x=0x
0e8e5776 73d9d92c ffad302b cfa2c141 85727e6f 377630bb a4b013b7 d0e64d59
 y=0x
24a72040 eb72567a bae92700 b75a4826 c3ebb58e 3e976cef 7caaa6e8 08e78633
 akey 0x
cfcec605 92510824 4035636e c37cba10 98dfbfc7 efd22d5d c9fb22df 6f4d0cf7

 SKEYID keys
 SKEYID 0x
f2d2fead c51ef5c4 b48e8a70 ee99058a c9a06aa9 63862e2f 624abc8b 949d68c6
 SKEYID_d 0x
5d03ddfb 5907a6b7 e6b8a1c7 78b3cef4 7011b7b8 e40c7f8b ce07175b 6ff30a9c
 SKEYID_a 0x
00d882f3 7d854ebd 9a3ea9f9 1f853748 857d7dbf 07fa5273 abad160d 4b8d455f
 SKEYID_e 0x
6a16b087 68bd0ad9 43a96046 5f9a0963 15d5c6ba 73b70dc6 fb623ff6 73752aa7
 SK_a 0x
d1f869e3 9358e7ca 97b2e5d9 6d10a84f b3543487 24eca24b ec692dc9 322c72a7
 SK_e 0x
d1f869e3 9358e7ca 97b2e5d9 6d10a84f b3543487 24eca24b ec692dc9 322c72a7
 IV 0x
fec9200a b45c110b

 Authentkaton
 HASH_I 0x
fb4993d4 51950a2f 45ffe884 70c460b4 edadd356 4f622fb9 d91d4e0e 514e6847
 HASH_R 0x
6b1a18d9 67f7f11b de434db5 f1a66693 7334c908 89b3af74 d096f269 204d9073
 AUTH_I 0x
81050919 1a5b8f4c ec3fd327 5ba1aecc 06604a6b ff3c4c3c 036b91bc 1433a4c0
 AUTH_R 0x
09a77b07 c582401a c404f0a9 d5851ff4 903c4b5f 91f0b6f0 eb44990d 2939bd28

 Ph 1 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 05010001
```

```
Messege ID
 00000000
Lenght
 00000258
Messege-Nonce
 00000000 00000000
 PL
Identification
 06001000
  00000000
  00000001 00000001
Certificate
 0900d701
Certificate type
 04
  308201ce 3082017d a0030201 02020102 30080606 2a850302 02033022 3120301e
 06035504 03131749 50536563 20436f6e 666f726d 69747920 526f6f74 2032301e
 170d3039 31313132 30393334 30315a17 0d343830 31303130 30303030 305a3056
 310b3009 06035504 06130252 55311730 15060355 040a0c0e 4f4f4f20 43727970
 746f2d50 726f312e 302c0603 5504030c 25495053 65632043 6f6e666f 726d6974
 7920456e 64204365 72742066 726f6d20 526f6f74 20323063 301c0606 2a850302
 02133012 06072a85 03020224 0006072a 85030202 1e010343 000440a0 0594338c
 67d7ca4f aa82e2b0 8a145fdf 3cf813e6 d8b944a6 2e34e975 6dade9c4 395772ee
 498e3ba5 2de84efe 153cf6f1 016c70f7 777508fc d3c7bec6 bfd5b4a3 68306630
 0f060355 1d0f0101 ff040503 0307ff80 30130603 551d2504 0c300a06 082b0601
 05050802 02301f06 03551d23 04183016 8014915f dd71bed3 dd9dce22 f9cf09b4
 fc862919 c06d301d 0603551d 0e041604 14c874c3 67957b6b d9720e42 e6a575c9
 e88e0a93 05300806 062a8503 02020303 4100d2e8 b243a051 b53bab3f fd15a4be
 61b9426b f34e2694 b57e9281 fddae4f2 1b087606 f0ac30f1 8054961c 7d859a02
 2cddcfa1 6ef62841 62aa218a b2965619 388d
  00
Signature
 00004400
  34aafbd4 f5332d65 00c46f7a 78d0eeb7 095f8d23 d9d70720 6f05492b 9a4775ec
 83e30750 5a2c78f0 3df29851 946bc241 b0a2a71f 36c9cd5d 031e89fb a928196c
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000258 00000000
 00000000 06001000 00000000 00000001 00000001 0900d701 04308201 ce308201
 7da00302 01020201 02300806 062a8503 02020330 22312030 1e060355 04031317
 49505365 6320436f 6e666f72 6d697479 20526f6f 74203230 1e170d30 39313131
 32303933 3430315a 170d3438 30313031 30303030 30305a30 56310b30 09060355
 04061302 52553117 30150603 55040a0c 0e4f4f4f 20437279 70746f2d 50726f31
 2e302c06 03550403 0c254950 53656320 436f6e66 6f726d69 74792045 6e642043
 65727420 66726f6d 20526f6f 74203230 63301c06 062a8503 02021330 1206072a
 85030202 24000607 2a850302 021e0103 43000440 a0059433 8c67d7ca 4faa82e2
 b08a145f df3cf813 e6d8b944 a62e34e9 756dade9 c4395772 ee498e3b a52de84e
 fe153cf6 f1016c70 f7777508 fcd3c7be c6bfd5b4 a3683066 300f0603 551d0f01
 01ff0405 030307ff 80301306 03551d25 040c300a 06082b06 01050508 0202301f
 0603551d 23041830 16801491 5fdd71be d3dd9dce 22f9cf09 b4fc8629 19c06d30
 1d060355 1d0e0416 0414c874 c367957b 6bd9720e 42e6a575 c9e88e0a 93053008
 06062a85 03020203 034100d2 e8b243a0 51b53bab 3ffd15a4 be61b942 6bf34e26
 94b57e92 81fddae4 f21b0876 06f0ac30 f1805496 1c7d859a 022cddcf a16ef628
 4162aa21 8ab29656 19388d00 00004400 34aafbd4 f5332d65 00c46f7a 78d0eeb7
 095f8d23 d9d70720 6f05492b 9a4775ec 83e30750 5a2c78f0 3df29851 946bc241
 b0a2a71f 36c9cd5d 031e89fb a928196c 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000258 00000000
```

```
 00000000 f0b02f0d fa3f999a f09f833f f465f09f 02b9924a a9dac76d 6dc830c0
 f42f7054 e1006f8c e6dc52b6 31cea21b 2420c3cf 6c05a305 8ff164bf be5d5b6c
 0f2a7703 674b13b8 a937c024 09cc6956 bce0b3ac 44a16771 d3eabb90 16c69473
 3068583e 0b4bfce0 1d48fb4a 4c80a101 bd9884ac daef1849 6a2640a7 d2a6fdb9
 324dd071 880c9b19 721fea17 0c800f05 01fd66fb dfadd392 e8a195fc d210b5d6
 702236f6 6d396ba3 aec96658 1a9f234e 273e24d2 f0cf9f41 17229bd6 b8b37e4e
 9c867943 518e819c 0754c506 e873e02e 7b0491b3 814220d2 9a610882 c283d71a
 1a658ded 7746f368 f7926020 ae50e01d fedb7025 5404871f 5f0c1c73 53e728e9
 0a707677 a8cb3f37 2686b8ed 173cea11 3d4ec375 c14b6e1f 23a3b853 bd1f8213
 dc63f7f4 10b8724f 0b2e4dff a4fc4f68 d1ed4cb9 f2c5a87a cd78d37b 4addb113
 a33e4c02 a3273747 2e0ddf65 e953d19a 9279591b 474b4ba1 f9c0accb 49563bdf
 2d05d6bc 862d8a62 a8787d49 d45c2e75 abd9fc3a 48fa6229 8f225eeb b17c04d3
 04ce71aa dc165f71 28fbe31b 7099c642 fcb2ab75 fc61eb16 9029cbd1 2e0fe446
 d2d42882 ae8a3daf 1d19e607 94934fbc 6e76c69a f510a8c0 ff5aefe7 d9054127
 eb0bbcec 9c82757c 0159fd70 679cb684 afe79569 34a58e6f 385150d7 5b092785
 68852993 6b979152 edf48782 380de0da 105249a2 3279f96c 33c20a65 228024b3
 904040e8 fada5a81 1c34be98 98bf58f4 3d80c811 371e9683 34409d9f 306db275
 0472d8c2 d69606d5 81fd925f 87be3cd1 8a5fb690 7ce97dcd

 Ph 1 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 05010001
Messege ID
 00000000
Lenght
 00000258
Messege-Nonce
 00000000 00000000
 PL
Identification
 06001000
  00000000
  00000002 00000002
Certificate
 0900d701
Certificate type
 04
  308201ce 3082017d a0030201 02020103 30080606 2a850302 02033022 3120301e
 06035504 03131749 50536563 20436f6e 666f726d 69747920 526f6f74 2033301e
 170d3039 31313132 30393334 30335a17 0d343830 31303130 30303030 305a3056
 310b3009 06035504 06130252 55311730 15060355 040a0c0e 4f4f4f20 43727970
 746f2d50 726f312e 302c0603 5504030c 25495053 65632043 6f6e666f 726d6974
 7920456e 64204365 72742066 726f6d20 526f6f74 20333063 301c0606 2a850302
 02133012 06072a85 03020224 0006072a 85030202 1e010343 000440b1 c30537d4
 35c74ac0 a3ba62e1 2bdfbc5e 56f8a465 17b6d5ea 6c597663 c98dbc7f c5712fac
 1f201dd7 071654c4 ba0fc7d1 0d5e66be c7e98129 cf0230b3 693ebaa3 68306630
 0f060355 1d0f0101 ff040503 0307ff80 30130603 551d2504 0c300a06 082b0601
 05050802 02301f06 03551d23 04183016 8014bbc2 18dd185e 5d85fcd4 711dc844
 14d7db7e f873301d 0603551d 0e041604 14d2240d c8f7dfdd bdbc8bd9 bfb5059c
 2a4c6c95 a9300806 062a8503 02020303 41000fcf c8bd0ad6 d52b0cf5 64edf3e3
 803a047a 62eb441b ad7359eb 2af246d6 e6b3ffae cd30beb7 9108f523 165ffb2e
 75ce8d4e 2e7d2614 9678cdca e80771e3 470c
  00
Signature
```

```
 00004400
  4ab1e222 84ccafd3 74d7c746 5aa28854 1e046e9f fe2b9d92 e3ba5251 81df1c80
 119500b7 7986548d 31ee95c2 1fe0c407 8c6b8978 3d7cd9f7 69b03414 374ab5e9
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000258 00000000
 00000000 06001000 00000000 00000002 00000002 0900d701 04308201 ce308201
 7da00302 01020201 03300806 062a8503 02020330 22312030 1e060355 04031317
 49505365 6320436f 6e666f72 6d697479 20526f6f 74203330 1e170d30 39313131
 32303933 3430335a 170d3438 30313031 30303030 30305a30 56310b30 09060355
 04061302 52553117 30150603 55040a0c 0e4f4f4f 20437279 70746f2d 50726f31
 2e302c06 03550403 0c254950 53656320 436f6e66 6f726d69 74792045 6e642043
 65727420 66726f6d 20526f6f 74203330 63301c06 062a8503 02021330 1206072a
 85030202 24000607 2a850302 021e0103 43000440 b1c30537 d435c74a c0a3ba62
 e12bdfbc 5e56f8a4 6517b6d5 ea6c5976 63c98dbc 7fc5712f ac1f201d d7071654
 c4ba0fc7 d10d5e66 bec7e981 29cf0230 b3693eba a3683066 300f0603 551d0f01
 01ff0405 030307ff 80301306 03551d25 040c300a 06082b06 01050508 0202301f
 0603551d 23041830 168014bb c218dd18 5e5d85fc d4711dc8 4414d7db 7ef87330
 1d060355 1d0e0416 0414d224 0dc8f7df ddbdbc8b d9bfb505 9c2a4c6c 95a93008
 06062a85 03020203 0341000f cfc8bd0a d6d52b0c f564edf3 e3803a04 7a62eb44
 1bad7359 eb2af246 d6e6b3ff aecd30be b79108f5 23165ffb 2e75ce8d 4e2e7d26
 149678cd cae80771 e3470c00 00004400 4ab1e222 84ccafd3 74d7c746 5aa28854
 1e046e9f fe2b9d92 e3ba5251 81df1c80 119500b7 7986548d 31ee95c2 1fe0c407
 8c6b8978 3d7cd9f7 69b03414 374ab5e9 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 05010001 00000000 00000258 00000000
 00000000 efcee728 e0ed5140 f54a8a2c cd44f0eb da7c010d d2ce3fb6 d95ca1b5
 48f0df84 4449578b 76f8b0a2 2b083ac8 d5f5d285 8200596d e360df28 8fa269dc
 20c5e1f2 fd9957e7 40a75b1e 7e099244 8ce2eef1 07233a0c 6152f6d0 125a77de
 15e8a2ce 82fd6665 57da1d89 25586a92 e866ec04 02f98f27 bcf6882c f1c1f757
 1fb19e63 d2519b89 1a1cad59 84d64683 5b5b9857 5a387dcd 79c09f2f d0cb8f24
 7862e84c c2ad1fa6 676ffd82 54b461dd d24f438d 0a73bfc6 6d10ab61 84f8ca03
 1b4d41a9 fc168c85 afe90629 ea41cfd3 a4544e8a 384bd600 1f8001ef 3297a20f
 1dfd3f5e 2bd05c6e 685de8eb a96a6cfa 42e60b09 e1cf2cff 0643d40f 4e9e9882
 722f525a 57c2886b 928ad274 82ab8235 31446501 2fe8663b 25b41d3c 44a6b152
 c18febd1 38b12437 5401643f 8a647b92 af516c45 3385d036 ffa3fe19 69b68ee8
 c1cba57c a9928267 9326fd6d db64601b 7cff7d5a fc0ee6a4 26a53303 4568019e
 51e8729e 08d28488 e307bc9e 9fec0e6a 74026cef d1cb2e39 ed7735ae 5bb0ac35
 a63dd6e8 b8776cfc 6e8f4b55 489195d0 61eff0df 5a5449fc 1d84b180 94bf69bd
 c043802d cbe6e8a4 8bedaf04 6c0357d1 d7b70992 f88117ec 2342fe4e 408c88e7
 84f8a409 fa0fb950 c60a0c58 d4f70d06 88511ff4 0b3cd313 baf2a1ea 5b25810f
 4700ed9d 85dbaf14 0548b375 7b54f9d2 554f6ccd 5c28e0fc 1e6fee70 49f3ce26
 9af9ec4a 16961655 9bc71115 961d6652 78e7cdf0 823d6597 85a8bd9c 2c905856
 02c1fd0c ee064791 add74023 d64af483 3e2ba0e5 2ccd7aaa
LastICV



 IKE ph2   Non PFS

 Quick Mode keys
 Initiator
 Nonce 0x
63696f4e 726f7461 6974696e 495f3270
 Messege Nonce 0x
005f4e5f 4d5f3270
 Responder
 Nonce 0x
```

```
63696f4e 7265646e 6f707365 525f3270
 Messege Nonce 0x
005f4e5f 4d5f3270
 SK_a 0x
da5d3920 72dcabd0 4b35ab3d 95ca1b51 3ec4bb81 188e15b7 6b909311 9667c395
 SK_e 0x
da5d3920 72dcabd0 4b35ab3d 95ca1b51 3ec4bb81 188e15b7 6b909311 9667c395
 IV 0x
ab739111 d633524d

 spi Initiator -> Responder 0x
34333231
 K1 0x
b4ae0927 ba789b7c 57b87bdc 943be136 54559c56 ab3d5393 ec6f6e10 2224ac11
 K2 0x
cef4f13b 7f238be6 3f0989c7 ad6584dd 777e02ed 7a45ae86 b780a7d3 b73c364f

 spi Responder -> Initiator 0x
31323334
 K1 0x
3a0558c4 e8c445bd dd96aec9 d58818d3 23ab2e18 38b22d9d 054667f8 0ab26492
 K2 0x
e61f5437 6b6d7450 2eb01a23 e369dbcb 59dc6472 1c3f3ee1 ca952ecc 5e3c3bd0

 Ph 2 Packet 1

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000b0
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 01002400
  ae66fcd8 38c54166 77863955 4db856c4 e1f3e9e6 23f49307 13a771dc 8c0ed74d
Security Association
 0a003000
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
  03000c00
  01fc0000
  00000000
Nonce
 05001400
  70325f49 6e697469 61746f72 4e6f6963
Identification
```

```
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 08080808 08080808
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000b0 70325f4d
 5f4e5f00 01002400 ae66fcd8 38c54166 77863955 4db856c4 e1f3e9e6 23f49307
 13a771dc 8c0ed74d 0a003000 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 03000c00 01fc0000 00000000 05001400 70325f49
 6e697469 61746f72 4e6f6963 05000c00 00000000 01020301 00000c00 00000000
 03027d02 08080808 08080808
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000b0 70325f4d
 5f4e5f00 465b3ba8 087b04aa cab958c1 e5202a8a b00c47e4 a3fc8bcf 86c35266
 f8398038 65d83501 b525c953 8a59f8d7 4110969f 874394fa 86ace068 66f96cd0
 5332caa4 ea21f6a3 f679eeef 809a64da 8909f894 2fa39f6d 6deb4f35 a3b78b5f
 d195bbec 2fb36a9f 0c058b88 0f51f833 9188a23d c5cb0829 9bbab2b8 e847659a
 1d42057d 396eb675 2df9b097 736936a7

 Ph 2 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000a0
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 01002400
  b1e32e89 c1eec5ab e8a61640 1734f63a a9fd8376 6c56d1c6 1dad9283 c6bdfbb9
Security Association
 0a002400
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
Nonce
 05001400
  70325f52 6573706f 6e646572 4e6f6963
Identification
 05000c00
  00000000
  01020301
```

```
Identification
 00000c00
  00000000
  03027d02
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000a0 70325f4d
 5f4e5f00 01002400 b1e32e89 c1eec5ab e8a61640 1734f63a a9fd8376 6c56d1c6
 1dad9283 c6bdfbb9 0a002400 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 05001400 70325f52 6573706f 6e646572 4e6f6963
 05000c00 00000000 01020301 00000c00 00000000 03027d02 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000a0 70325f4d
 5f4e5f00 13020109 6e293b50 1892f435 9001a918 9cf3f147 c66817ba 092a5c41
 a960df5e 4a956b01 6809b4fb 00bd7537 fbb52749 8878c305 cbbc7755 43e24cbe
 13fe8f20 23c2c024 e2aed5e5 4ebf268b 86acbc6c 64d9ddd7 bc4c7e4e 81f2cf53
 462100b3 342ee7e7 da71af7d 22066a92 80b47582 00f52ac0 15a86e9f 1de19c92

 Ph 2 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 00000050
Messege-Nonce
 70325f4d 5f4e5f00
 PL
Hash
 00002400
  9054025b 0f9a05d4 8f95a847 31224184 ef74fb93 826d6a4a c40c197e a6865b13
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f00 00002400 9054025b 0f9a05d4 8f95a847 31224184 ef74fb93 826d6a4a
 c40c197e a6865b13 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f00 510961d5 4a8bcc1d 046b22c0 e3431153 07310aaf b5eaf3e2 99f451b4
 01404668 a97ca119 05e056fc c79f89a2


 IKE ph2   PFS

 Quick Mode keys
 Initiator
 Nonce 0x
00534650 6563696f 4e74696e 495f3270
 Messege Nonce 0x
505f4e5f 4d5f3270
 x_i 0x
00000000 00000000 00000000 00000000 00000053 46507965 4b74696e 495f3270
```

```
 gx_i
 x=0x
96567f88 5edcf177 26b5e9df 64a4aa87 f52db551 a60d241b 6bdc9a82 14b60d63
 y=0x
298bc55b e33916e3 02f10ea1 46cb857b cd6a3dad 40300494 f3e0c983 90b0c61f
 Responder
 Nonce 0x
00534650 6563696f 4e707365 525f3270
 Messege Nonce 0x
505f4e5f 4d5f3270
 x_r 0x
00000000 00000000 00000000 00000000 00000053 46507965 4b707365 525f3270
 gx_r
 x=0x
517fbbc8 ddb119d7 cb54cea0 38fda66f b2ae9fef 5e71d7b5 79961b8e 17fe6c80
 y=0x
2965c2de 8c82ba2a 65fb6455 c2cb08cd 76a06649 2988aa80 330b9ca9 8d72b638

 gm_ir 0x
692818f6 39b36364 8d4f9bbc 73e9b044 43d86e51 8788acba d89e3169 16465221
 SK_a 0x
1230bcbc 1f651e57 2a866f84 b7df33d5 9e502aa3 6e1038d9 7a52ed5f e6cfd5a3
 SK_e 0x
1230bcbc 1f651e57 2a866f84 b7df33d5 9e502aa3 6e1038d9 7a52ed5f e6cfd5a3
 IV 0x
39983837 0e4fb872

 spi Initiator -> Responder 0x
34333231
 K1 0x
3448fbad fe40c7f9 b053fd7c 1d6bb1d9 e9222268 64c6df43 2561010c 9c9df29d
 K2 0x
bd32bdeb 9c0f46b5 0ebd9bb6 5f15a4ba 432e9c64 816e14f4 fa495550 24c513c6

 spi Responder -> Initiator 0x
31323334
 K1 0x
92f9fd4f c812aa97 4522aec1 460d904a 32c59109 79306695 b5bd1280 dcdc2d4b
 K2 0x
66fe5ed8 df6ed41a adb32a0c 64b746f4 5fcf23f9 69d187fb 8922934f d1f8e9c8

 Ph 2 Packet 1

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 000000f0
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 01002400
  8e1df1c8 01709834 ed4c316c 94f27ccc 65c0eaeb ac8bd5f9 cc15ca3c 381e8c40
```

```
Security Association
 0a003000
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
  03000c00
  01fc0000
  00000000
Nonce
 04001400
  70325f49 6e69744e 6f696365 50465300
Key Exchange
 05004400
  630db614 829adc6b 1b240da6 51b52df5 87aaa464 dfe9b526 77f1dc5e 887f5696
 1fc6b090 83c9e0f3 94043040 ad3d6acd 7b85cb46 a10ef102 e31639e3 5bc58b29
Identification
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000f0 70325f4d
 5f4e5f50 01002400 8e1df1c8 01709834 ed4c316c 94f27ccc 65c0eaeb ac8bd5f9
 cc15ca3c 381e8c40 0a003000 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 03000c00 01fc0000 00000000 04001400 70325f49
 6e69744e 6f696365 50465300 05004400 630db614 829adc6b 1b240da6 51b52df5
 87aaa464 dfe9b526 77f1dc5e 887f5696 1fc6b090 83c9e0f3 94043040 ad3d6acd
 7b85cb46 a10ef102 e31639e3 5bc58b29 05000c00 00000000 01020301 00000c00
 00000000 03027d02 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000f0 70325f4d
 5f4e5f50 c43b13ca ea81fba0 5c32cd78 57ecb60a d57ee749 358cfd8c f53bfcb8
 9ce4a35d 6feb2e6c 3aa869fc d4ddf351 741f1051 eb03af98 c24e4a0a bd7c10be
 5cc22deb 946041c7 01b6ff2c 7cdb9efa d3136e87 c653b60a e022ca28 b19af227
 e57c4327 f9fcf6f3 ae7a4d20 a4632e90 cd05ff61 d4bdee21 0827272b 1e198d18
 85b798af 82c02a7c 0f46ebf8 fe6f5a52 cdedec1d 6be8186b a26a306a 83f1ed41
 d7de678b 591ea380 f8c63124 cab8a798 f5338690 a3303a5e 82617e46 78e88c87
 c9a264b4 dd609905 982afc59 e7ef805e

 Ph 2 Packet 2

Initiator Cookie
 00000003 00000004
Responder Cookie
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
```

```
Lenght
 000000e8
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 01002400
  484cd087 f70cc1e2 40caf531 780eec2a 165da91d 8da643d9 803e2647 a8102018
Security Association
 0a002400
  00000000
  00000000
  00000c00
  01030402
  00000000
  03000c00
  01fd0000
  00000000
Nonce
 04001400
  70325f52 6573704e 6f696365 50465300
Key Exchange
 05004400
  806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd c8bb7f51
 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c dec26529
Identification
 05000c00
  00000000
  01020301
Identification
 00000c00
  00000000
  03027d02
padding
 08080808 08080808
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000e8 70325f4d
 5f4e5f50 01002400 484cd087 f70cc1e2 40caf531 780eec2a 165da91d 8da643d9
 803e2647 a8102018 0a002400 00000000 00000000 00000c00 01030402 00000000
 03000c00 01fd0000 00000000 04001400 70325f52 6573704e 6f696365 50465300
 05004400 806cfe17 8e1b9679 b5d7715e ef9faeb2 6fa6fd38 a0ce54cb d719b1dd
 c8bb7f51 38b6728d a99c0b33 80aa8829 4966a076 cd08cbc2 5564fb65 2aba828c
 dec26529 05000c00 00000000 01020301 00000c00 00000000 03027d02 08080808
 08080808
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 000000e8 70325f4d
 5f4e5f50 e3af029d 98716050 7dfa29e3 00c30e3e 755b72a8 e4778239 c6867b09
 c739c82b f9db3c53 5e328fac e4a1d494 a451c7db 9a25d8c5 0c064e81 06390d1b
 ffe8c4c6 940dfb9e dcb32df2 7f8b5a4e dc5fb995 c09afcbe 84958a45 a5450525
 b15e8c16 0166b1af 39aaad9f a4006fa0 33396064 e31392da aa34ba19 9a2b53ac
 895ecb65 415717a9 d5f5b369 bdbecc8f e7c3757f d5af2ade dbff6a2c f9b51246
 8c52716c 34bdf467 66095e27 e5ae67a3 cf8c8e20 f812cf3a 80272e0a 1756a77d
 f300d735 3510b356

 Ph 2 Packet 3

Initiator Cookie
 00000003 00000004
Responder Cookie
```

```
 00000004 00000004
Flags
 08010001
Messege ID
 61626364
Lenght
 00000050
Messege-Nonce
 70325f4d 5f4e5f50
 PL
Hash
 00002400
  1c12e52a 0a40adb1 7780cd16 2b7130b1 46649e71 3e785af9 ef7c8188 8a9f3ac7
padding
 04040404
Cipher input packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f50 00002400 1c12e52a 0a40adb1 7780cd16 2b7130b1 46649e71 3e785af9
 ef7c8188 8a9f3ac7 04040404
Encrypted packet
 00000003 00000004 00000004 00000004 08010001 61626364 00000050 70325f4d
 5f4e5f50 7f166301 0fb9c7e5 cd93a6db d1cbd272 cde795f1 47f21190 6c440fe3
 e05b38b6 66f6fb00 8303fd98 62359040

|<Example-GOST-IKE-SIGNATURE.bin
```

13. Библиография

13.1 Нормативные ссылки

[ARCH] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[CPALGS] Popov, V., Kurepkin, I., and S. Leontiev, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms", RFC 4357, January 2006.

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[ESN] Kent, S., "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", RFC 4304, December 2005.

[ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

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

[GOST3431004] Council for Standardization, Metrology and Certification of the Commonwealth of Independence States (EASC), Minsk , "Information technology. Cryptographic Data Security. Formation and verification processes of (electronic) digital signature based on Asymmetric Cryptographic Algorithm (In Russian)", GOST 34.310-2004, 2004.

[GOST3431195] Council for Standardization, Metrology and Certification of the Commonwealth of Independence States (EASC), Minsk , "Information technology. Cryptographic Data Security. Cashing function (In Russian)", GOST 34.311-95, 1995.

[GOSTR341001] Government Committee of the Russia for Standards , "Information technology. Cryptographic Data Security.Signature and verification processes of [electronic] digital signature, Gosudarstvennyi Standard of Russian Federation (In Russian)", GOST R 34.10-2001, 2001.

[GOSTR341194] Government Committee of the Russia for Standards , "Information technology. Cryptographic Data Security. Hashing function, Gosudarstvennyi Standard of Russian Federation (In Russian)", GOST R 34.11-94, 1994.

[IKE] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[ISAKMP] Maughan, D., Schneider, M., and M. Schertler, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[JUMBO] Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4134] Hoffman, P., "Examples of S/MIME Messages", RFC 4134, July 2005.

13.2 Информативные ссылки

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

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

[CRYPTOLIC] "Russian Federal Government Regulation on Licensing of Selected Activity Categories in Cryptography Area, 23 Sep 2002 N 691", September 2002.

[draft.CPAH] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Алгоритм обеспечения целостности IPsec (ESP, AH) на основе ГОСТ Р 34.11-94", December 2009.

[draft.CPESP] Леонтьев, С.Е., Ed., Павлов, М.В., Ed., and А.А. Федченко, Ed., "Комбинированый алгоритм шифрования вложений IPsec (ESP) на основе ГОСТ 28147-89", December 2009.

[RFLLIC] "Russian Federal Law on Licensing of Selected Activity Categories, 08 Aug 2001 N 128-FZ", August 2001.

[Schneier95] Schnier, B., "Applied cryptography, second edition", John Wiley, 1995.

13.3 Библиотека ссылок

[AH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

[GOST3431095] Council for Standardization, Metrology and Certification of the Commonwealth of Independence States (EASC), Minsk , "Information technology. Cryptographic Data Security. Produce and check procedures of Electronic Digital Signature based on Asymmetric Cryptographic Algorithm (In Russian)", GOST 34.310-95, 1995.

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

[HMAC] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

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

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

[RFEDSL] "Russian Federal Electronic Digital Signature Law, 10 Jan 2002 N 1-FZ", January 2002.

[X.208-88] International International Telephone and Telegraph Consultative Committee , "Specification of Abstract Syntax Notation One (ASN.1)", CCITT Recommendation X.208, November 1988.

[X.209-88] International Telephone and Telegraph Consultative Committee, "Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)", CCITT Recommendation X.209, 1988.

[X.509-00] International Telecommunications Union , "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO Standard 9594-8, March 2000.

[X.680-02] International International Telephone and Telegraph Consultative Committee, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", CCITT Recommendation X.680, July 2002.

[X.690-02] International International Telephone and Telegraph Consultative Committee, "ASN.1 encoding rules: Specification of basic encoding Rules (BER), Canonical encoding rules (CER) and Distinguished encoding rules (DER)", CCITT Recommendation X.690, July 2002.

13.4 Ссылки на примеры и методы редактирования

[draft.rfc2434bis] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", Internet-Draft draft-narten-iana-considerations-rfc2434bis-09 (work in progress), March 2008.

[draft.RFC2629bis] Rose, M.T., "Writing I-Ds and RFCs using XML (revised)", February 2009, <http://xml.resource.org/authoring/draft-mrose-writing-rfcs.html>.

[ID-Checklist] Wijnen, B., "Checklist for Internet-Drafts (IDs) submitted for RFC publication", October 2006, <http://www.ietf.org/ID-Checklist.html>.

[ipsec-registry] IANA, "Internet Key Exchange (IKE) Attributes - per RFC 2409 (IKE)", January 2009, <http://www.iana.org/assignments/ipsec-registry>.

[isakmp-registry] IANA, "FROM RFC 2407 and RFC 2408 "Magic Numbers" for ISAKMP Protocol", October 2006, <http://www.iana.org/assignments/isakmp-registry>.

[RFC2629] Rose, M.T., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[XML2RFC] Rose, M.T., Fenner, B., and C. Levert, "xml2rfc v1.33", February 2009, <http://xml.resource.org/authoring/README.html>.

[xml2rfc-validator] Fenner, , "xml2rfc validator", January 2007, <http://www.fenron.com/~fenner/ietf/xml2rfc-valid/>.

Адреса авторов

Сергей Е. Леонтьев (editor)
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (916) 686 10 81
Fax: +7 (495) 780 48 20
EMail: lse@cryptopro.ru
URI: http://www.CryptoPro.ru

Михаил В. Павлов (editor)
ООО Крипто-Про
Сущёвский вал., д. 16, стр. 5
Москва, 127018
Россия
Phone: +7 (495) 780 48 20
Fax: +7 (495) 780 48 20
EMail: pav@cryptopro.ru
URI: http://www.CryptoPro.ru

Андрей А. Федченко (editor)
S-Terra
Зеленоград, МГИЭТ, корпус 10, офис 110
Москва, 124498
Россия
Phone: +7 (495) 726 98 91
Fax: +7 (495) 531 9789
EMail: hell@s-terra.com
URI: http://www.s-terra.ru

A. Приложение: Применение

Выбор алгоритма аутентификации:

IKE-GOST-PSK: Очень высокая производительность, но высокие требования к управлению ключами. Некрупные сети равноправных шлюзов;

IKE-GOST-SIGNATURE: Низкая производительность, но несколько более высокая устойчивость к DoS атакам ложных соединений в основном (main) режиме.

Выбор режима алгоритма аутентификации:

Основной (Main): Низкая производительность, но высокая устойчивость к DoS аткам в Интернет. Для алгоритма IKE-GOST-PSK обеспечивается конфиденциальность идентификационной информации;

Быстрый (Aggressive): Высокая производительность, устойчивость к DoS атакам при использовании радиоканалов (при достаточной производительности процессора).

Пояснение к DoS атакам:

в Интернет: Нарушитель не имеет возможности перехватывать траффик, не имеет достаточных вычислительных мощностей, но имеет возможность посылать большое количество пакетов (первых пакетов). Блокируется механизмом контроля CKI-I/R протокола ISAKMP;

ложных соединений: Нарушитель не имеет возможности перехватывать трафик, но имеет возможность устанавливать большое количество соединений (первый, второй и третий пакет). Блокируется механизмом непосредственно механизмом аутентификации (распределённые DoS атаки);

при использовании радиоканалов: Нарушитель имеет возможность, как перехватывать трафик, так и посылать пакеты, но не имеет возможности искажать пакеты в канале. Блокируется механизмом имитозащиты при условии достаточной производительности процессора;

B. Приложение: Описание текстового представления PSK

При использовании PSK следует предусмотреть его периодическую смену и обеспечить контроль сроков действия PSK.

Срок действия НЕ ДОЛЖЕН превышать 8 лет. НЕ РЕКОМЕНДОВАНО, что бы срок действия PSK превышал 6 месяцев.

При текстовом представлении PSK (PSK_a) для последующего ручного ввода, РЕКОМЕНДОВАНО снабжать PSK следующими атрибутами:

- Идентификатор канала связи (опционально);
- Идентификатор узла;
- Версия PSK;
- Срок действия PSK;

B.1 Текстовое представление PSK

PSK_a является конкатенацией двух частей: A1,...,A14 и B1,...,B14.

Каждая из частей PSK состоит из 14 символов из набора 32, легко различимых символов:

[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F]

[G, H, K, L, M, N, P, Q, R, T, U, V, W, X, Y, Z]

Ввод PSK_a в аппаратуру требует ввода имени узла и, опционально, имени канала связи. РЕКОМЕНДОВАНО реализовать раздельный ввод и хранение всех компонент PSK. Компоненты PSK_a могут вводится в произвольном порядке.

B.2 Алгоритм выработки текстового PSK

Знакам [0,1, ... ,Y,Z] ставятся в соответствие 5-битовые комбинации [00000,00001, ... ,11110,11111]. PSK состоит из двух блоков по 70 бит, D1 и D2.

Содержание первого блока:

биты 0-58:	случайные;
бит 59:	равен 0 (признак первого блока);
биты 60-63:	месяц окончания срока действия PSK по модулю 16;
биты 64-67:	имитовставка, биты 0-3;
биты 68-69:	версия PSK, биты 0-1.

Биты 0-64 первого блока участвуют в расчёте имитовставки и шифруются.

Содержание второго блока:

биты 0-58:	случайные;
бит 59:	равен 1 (признак второго блока);
биты 60-63:	год окончания срока действия PSK по модулю 16 [rfc.comment.3];
биты 64-67:	имитовставка, биты 4-7;
биты 68-69:	версия PSK, биты 2-3.

Биты 0-64 второго блока участвуют в расчёте имитовставки и шифруются.

Ключ имитозащиты:

Kpi = HASH([<ид. канала>|]"IKE_SA_ IMITAKEYGost28147-89CryptoPro-B-ParamSet")

Ключ шифрования:

[rfc.comment.3] Вставить формулу сравнения, она простая, т.к. срок действия PSK НЕ ДОЛЖЕН превышать 8 лет

Kpe = HASH([<ид. канала>|]<ид.
узла>|"IKE_SA_ENCRYPTIONKEYECBGost28147-89CryptoPro-B-ParamSet")

Шифрование и имитозащита вычисляются с параметрами id-Gost28147-89-CryptoPro-B-ParamSet, хэш-функция вычисляется согласно Section 3 of [draft.CPAH]

Порядок вычислений:

1. Заполнить версию PSK в E1[68..69] и E2[68..69];
2. Заполнить срок окончания действия PSK (год и месяц) в D1[59..63] и D2[59..63];
3. Выработать 118 случайных бит в D1[0..58] и D2[0..58];
4. Рассчитать имитовставку на биты 0-63 первого и второго блока:

   ICVp = gost28147IMIT(0, Kpi, D1[0..63]|D2[0..63]);
   E1[64..67] = ICVp[4..7];
   E2[64..67] = ICVp[0..3];

5. Зашифровать биты 0-63 первого и второго блока:

   E1[0..63] = encryptECB(Kpe, D1[0..63]);
   E2[0..63] = encryptECB(Kpe, D2[0..63]);

6. Преобразуем зашифрованные первый и второй блоки E1,E2 в A1,...,A14 и B1,...,B14.
7. Порядок использования PSK в аппаратуре:
   1. Ввод частей E1,E2 в произвольном порядке.
   2. Расшифрование, контроль целостности и контроль срока действия PSK. В результате получаются блоки бит F1 = (D1[0..63], E1[64..67)) и F2 = (D2[0..63], E2[64..67]);
   3. Блоки F1, F2 разбиваются на 4-битовые фрагменты, превращаемые в байты дополнением старшими нулями, в результате получается последовательность B1 ... B34.
   4. Байтовая последовательность хэшируется по алгоритму ГОСТ Р 34.11-94, значение хеш-функции является ключом PSK.

B.3 Пример текстового PSK

TODO: предварительная версия примера

```
 Responder PSK
  tm_year 0x0000006d
  tm_mon 0x00000009
  NetID
  4e 65 74 37 33 00 00 00 00 00 00     Net73..........
  StationName
  30 31 3a 32 33 3a 34 35 3a 36 37 3a 38 39 3a 30  01:23:45:67:89:0
  31 3a 32 33 34 35 36 37 38 39 30 31 32 33 34 35  1:23456789012345
  36 37 38 39 30 31 32 33 34 35 36 37 38 30    67890123456780..
  Текстовое представление PSK
  42 58 41 46 30 56 4d 39 56 47 34 52 50 43 44 4b  BXAF0VM9VG4RPCDK
  56 45 4b 38 33 5a 55 39 4c 5a 31 57 00 00 00 00  VEK83ZU9LZ1W....
Представление в Hex
  42 41 42 41 37 30 36 33 44 34 42 31 32 31 43 36  BABA7063D4B121C6
  39 44 34 45 36 37 32 31 44 38 46 41 33 44 43 46  9D4E6721D8FA3DCF
  31 38         18
  Перед расшифрованием
  ab ab 07 36 4d 1b 12 6c 4d 6e 27 d1 f8 3a cd 1f
  Рассшифрованные знаки
  f4 9a 29 9f 60 53 71 a4 18 42 4d 10 97 ba 84 d7

  ChSm 0x89

 хешируемая последовательность
  34 46 41 39 39 32 46 39 30 36 33 35 31 37 34 41  4FA992F90635174A
  39 38 31 32 34 44 34 30 31 37 39 41 42 34 38 37  98124D40179AB487
  44 38         D8

  PSK  0x
 8c57daa5 a5f2be3c 7330de68 6fc85bc2 86e723cb 5a816bb7 978e7e0b 1bdcbce7
```

Copyright

[TODO: пока секции прав полностью неопределены стоят все возможные Copyright]

Права на интеллектуальную собственность

[TODO: Описать позицию ТК26 относительно прав на интеллектуальную собственность, возможность для российских потребителей использовать результаты ТК26, а так же на потенциальные конфликты интересов]

Всё согласно IETF BCP 78 and BCP 79.