ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ
ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

ПО ИСПОЛЬЗОВАНИЮ ГОСТ 28147-89, ГОСТ Р 34.11-2012 И ГОСТ Р 34.10-2012 В ПРОТОКОЛАХ ОБМЕНА КЛЮЧАМИ IKE И ISAKMP

Москва
2015

Содержание

1 Введение

Данный документ дополняет технические спецификации **ТК26IKE** определением способов использования алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

1.1 Текущий статус документа

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

Данный документ является открытым документом «Рабочей группы IPsec и IKE» и технического комитета по стандартизации «Криптографическая защита информации (ТК26)». Область распространения документа не ограничена.

2 Нормативные ссылки

Указанные в этом разделе спецификации ссылочные документы являются обязательными для их применения. Для датированных ссылок используют только указанное здесь издание. Для недатированных ссылок - последнее и актуальное издание со всеми изменениями и дополнениями:

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.

ТК26УЗ - Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет 026, «Системы обработки информации. Защита криптографическая. Методические рекомендации по заданию узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89», 2013.

ТК26АЛГ - Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет 026, «Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012», 2014.

ТК26IKE - Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет 026, «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 в протоколах обмена ключами IKE и ISAKMP», 2013.

2.1 Дополнительные ссылки

RFC2119 - С. Браднер, «Ключевые слова для использования в документах RFC, указывающие уровень требований», стандарт BCP 14, март 1997 г. (Bradner S., Key words for use in RFCs to Indicate Requirement Levels, BCP 14, IETF RFC 2119, March 1997).

RFC2407 - Д. Пайпер, «Область интерпретации IPsec для ISAKMP» (Piper D., The Internet IP Security Domain of Interpretation for ISAKMP, IETF RFC 2407, November 1998).

RFC2408 - Д. Шнейдер, М. Шертлер, «Протокол управления ключами и группами параметров сетевой безопасности (ISAKMP)» (Maughan D., Schneider M. and M. Schertler, Internet Security Association and Key Management Protocol (ISAKMP), IETF RFC 2408, November 1998).

RFC2409 - Д. Харкинс, Д. Каррел, «Протокол согласования ключей (IKE)» (Harkins, D. and D. Carrel, The Internet Key Exchange (IKE), IETF RFC 2409, November 1998).

2.2 Информативные ссылки

RFC6071 - С. Френкель, С. Кришнан, «Дорожная карта для протоколов IP Security (IPsec) и Internet Key Exchange (IKE) в документах» Frankel, S. and S. Krishnan, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, IETF RFC 6071, February 2011.

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 Основные понятия, термины и определения

В данном документе используются термины и определения стандартов IKE (**RFC2409**) и ISAKMP (**RFC2408**), далее приводятся только дополнительные определения.

3.1 Терминология требований

Термины "ДОЛЖНО", "ДОЛЖНА", "ДОЛЖНЫ", "ДОЛЖЕН" (MUST, REQUIRED, SHALL), "НЕ ДОЛЖЕН", "НЕ ДОЛЖНЫ" (MUST NOT, SHALL NOT), "РЕКОМЕНДУЕТСЯ" (SHOULD, RECOMMENDED), "НЕ РЕКОМЕНДУЕТСЯ" (SHOULD NOT, NOT RECOMMENDED), "МОГУТ", "МОЖЕТ" (MAY, OPTIONAL) в рамках этого документа ДОЛЖНЫ интерпретироваться в соответствии с положениями документа **RFC2119**

3.2 Определения

В настоящем документе определены следующие термины:

IPsec (сокращение от IP Security)	набор протоколов по обеспечению защиты данных, передаваемых по межсетевому протоколу IP, включает в себя протоколы согласования ключей и защиты сетевого трафика;
IKE (Internet Key Exchange)	протокол защищённого согласования ключей, используется для формирования сопоставлений безопасности (SA);
Сопоставление безопасности (Security Association, SA)	совокупность атрибутов безопасности и ключевой информации, ассоциируемая с безопасным соединением, представляющим собой виртуальный однонаправленный канал для передачи данных;

3.3 Условные обозначения

Для обозначения переменных, функций и их параметров в настоящей спецификации применяются нижеследующие обозначения:

HASH(D)	Расчёт хэш-функции с внутренним выравниванием по ГОСТ Р 34.11 (см. раздел 2.1 в **RFC4490**);
Cert_i u Cert_r	Сертификаты открытого ключа Инициатора и Респондента соответственно;
k_i u k_r:	Ключи подписи сертификата Инициатора и Респондента соответственно;
prf(K,D):	Соответствует HMAC_GOSTR3411(K,D) (см. раздел 3 в **RFC4357**) или PRF_IPSEC_KEYMAT_GOSTR3411_2012_512 (см. **ТК26АЛГ**);
Signature(d, h)	Вычисление электронной подписи ГОСТ Р 34.10 от аргумента h на ключе подписи d.

3.4 Аббревиатуры и сокращения

В тексте данного документа используются следующие сокращения и аббревиатуры:

ISAKMP	Internet Security Association and Key Management Protocol. Протокол управления ключами и группами параметров сетевой безопасности;
SA	Security Association. Набор параметров безопасности, формируемых протоколом управления ключами и группами параметров сетевой безопасности;
ЭЦП	Электронно-цифровая подпись (digital signature);
SPI	Security Parameter Index. Идентификатор IPsec SA;
HMAC	Hash-based message authentication code. Хэш-код аутентификации сообщений;
PFS	Perfect Forward Security (см. раздел 3.3 в **RFC2409**).

4 Хэш-функция ГОСТ Р 34.11-2012

В данном документе определяется использование идентификатора GOST_R_34_11_2012_512 для хэш-функции ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит в методах аутентификации IKE-GOST-PSK и IKE-GOST-SIGNATURE определённых в **ТК26IKE**.

Функция prf() строится на основе ГОСТ Р 34.11-2012 обычным образом согласно IKE (**RFC2409**), т.е. используется функция PRF_IPSEC_KEYMAT_GOSTR3411_2012_512 определённая **ТК26АЛГ**.

5 Алгоритм ЭЦП ГОСТ Р 34.11-2012

При реализации метода аутентификации IKE-GOST-SIGNATURE, определённого **ТК26IKE,** для ключей подписи ГОСТ Р 34.10-2012 функции Signature(k_i, HASH_I) и Signature(k_r, HASH_R) ДОЛЖНЫ вычислять подпись ГОСТ Р 34.10-2012 на результат вычисления хэш-функции ГОСТ Р 34.11-2012 от сетевых представлений HASH_I и HASH_R соответственно.

6 Дополнительные параметры и атрибуты ISAKMP SA

Для использования атрибутов методов аутентификации, описанных в данном документе, при согласовании параметров ISAKMP SA обе стороны ДОЛЖНЫ согласовать идентификатор приложения IKE_GOST_VENDOR_ID определённый в **ТК26IKE**.

Таблица 1: Параметры ISAKMP SA для методов расширения протокола IKE

Параметр	Атрибут	Формат	Умолчание
алгоритм шифрования	1	B	-
алгоритм хэширования	2	B	-
описание группы	4	B	-

6.1 Алгоритм хэширования ГОСТ Р 34.11-94 и параметры

Для атрибута «алгоритм хэширования» (2) используется идентификатор хэш-функции GOST_R_34_11_2012_512 <TBD+2>.

6.2 Алгоритм ГОСТ 28147-89 и параметры

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

Таблица 2: Параметры ГОСТ 28147-89 ISAKMP SA

Алгоритм	Режим	Узел замены	Значение
GOST-Z-CFB-IMIT	CFB	id-tc26-gost-28147-param-Z	<TBD+3>

6.3 Описания групп типа VKO GOST R 34.10-2012

Для атрибута «описание группы» (4) используется:

Таблица 3: Группы типа VKO GOST R 34.10-2012

Группа	Алгоритм и параметры	Значение
VKO GOST R 34.10-2012 256A_256	VKO_GOSTR3410_2012_256 id-GostR3410-2001-CryptoPro-XchA-ParamSet id-tc26-gost3411-12-256	<TBD+4>
VKO GOST R 34.10-2012 256B_256	VKO_GOSTR3410_2012_256 id-GostR3410-2001-CryptoPro-XchB-ParamSet id-tc26-gost3411-12-256	<TBD+5>
VKO GOST R 34.10-2012 512A_256	VKO_GOSTR3410_2012_256 id-tc26-gost-3410-12-512-paramSetA id-tc26-gost3411-12-256	<TBD+6>
VKO GOST R 34.10-2012 512B_256	VKO_GOSTR3410_2012_256 id-tc26-gost-3410-12-512-paramSetB id-tc26-gost3411-12-256	<TBD+7>

Реализации IPsec, соответствующие требованиям данного документа, ДОЛЖНЫ реализовать группу VKO GOST R 34.10-2012 256B_256, которая РЕКОМЕНДУЕТСЯ к использованию в сети Интернет. Алгоритм VKO_GOSTR3410_2012_256 определён в **ТК26АЛГ**.

7 Регистрация IANA

IANA выделяет два номера хэш-функции IKE для использования ГОСТ Р 34.11-2012:

<TBD+2> для GOST_R_34_11_2012_512.

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

<TBD+3> для GOST-Z-CFB-IMIT.

IANA выделяет четыре номера описания групп:

<TBD+4> для VKO GOST R 34.10-2012 256A;

<TBD+5> для VKO GOST R 34.10-2012 256B;

<TBD+6> для VKO GOST R 34.10-2012 512A;

<TBD+7> для VKO GOST R 34.10-2012 512B.

7.1 Приватные номера преобразований

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

65522 для GOST_R_34_11_2012_512;

65523 для GOST-Z-CFB-IMIT;

65524 для VKO GOST R 34.10-2012 256A;

65525 для VKO GOST R 34.10-2012 256B;

65526 для VKO GOST R 34.10-2012 512A;

65527 для VKO GOST R 34.10-2012 512B.

8 Рекомендации по совместимости

Стороны инициатора и ответчика предлагают и согласуют поддерживаемые ими алгоритмы с РЕКОМЕНДОВАННЫМ приоритетом хэш-функций и групп большего размера.

При использовании метода аутентификации GOST-IKE-SIGNATURE с ключами подписи ГОСТ Р 34.10-2012 любой длины необходимо хэшировать значение функции prf() алгоритмом хэш-функции, соответствующей сертификату (ключу подписи). Подписывается только этот хэш-код, в отличие от спецификаций **TK26IKE** и **RFC2409**, в которых предписывается подписывать само значение функции prf(). С учётом этого рекомендуется:

- В случае если у стороны есть ключ подписи ГОСТ Р 34.10-2001, предлагать и согласовывать только один вариант алгоритма хэш-функции: GOST_R_34_11_94;
- В случае если у стороны инициатора нет ключей подписи ГОСТ Р 34.10-2001, предлагать на согласование другой стороне все поддерживаемые алгоритмы.

Рекомендации по реализации алгоритмов и параметров:

- GOST_R_34_11_94 - рекомендовано;
- GOST_R_34_11_2012_512 - рекомендовано;
- GOST-B-CFB-IMIT - рекомендовано;
- GOST-Z-CFB-IMIT - рекомендовано;
- VKO GOST R 34.10-2001 XchB - рекомендовано;
- VKO GOST R 34.10-2012 256B - рекомендовано.

9 Примеры (информативные)

Форматы представление данных в примерах:

0xNNNN: Представление целого числа в шестнадцатеричной системе счисления, а также представление объектов в форме big-endian;

0xFFFFFFFF FF...: Представление объектов в форме *big-endian*;

BBBBBBBB BB: Представление объектов в сетевой нотации. Числа в *big-endian*. Сетевое представление сложных объектов согласно стандартам их определяющих, в частности, ключей и хэшей согласно **RFC4357**, **RFC4490** и **RFC4491**.

9.1 Пример GOST-IKE-PSK

В примерах используются параметры сопоставления безопасности, принятые по умолчанию:

- Шифрование обмена ISAKMP с узлом замены id-tc26-gost-28147-param-Z в режиме гаммирования с обратной связью и усложнением ключа (см. в RFC4357, пункт 3.2.3);
- Параметры алгоритма VKO - id-tc26-gost-3410-12-512-paramSetA+id-tc26-gost3411-12-256; PRF на основе ГОСТ Р 34.11-2012, 512.

```
IKE phase1 PSK Authentication Main Mode

Security Association
DH_OID=1.2.643.7.1.2.1.2.1
CIPHER_OID=1.2.643.7.1.2.5.1.1
HASH_OID=1.2.643.7.1.1.2.3

Initiator Internals:
CKY-I
```

```
   9F3F56E2 F256015E
SA
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFF2
   8004FFF6 8003FFE2 800B0001 000C0004 0028DE80

Initiator -> Responder

Initiator's Packet IKE phase 1 (1)
CKY-I
   9F3F56E2 F256015E
Flags
   01100200
Message ID
   00000000
Length
   00000054
Security Association
   00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFF2
   8004FFF6 8003FFE2 800B0001 000C0004 0028DE80
Initiator's Packet IKE phase 1 (1)
   9F3F56E2 F256015E 00000000 00000000 01100200 00000000 00000054 00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFF2
   8004FFF6 8003FFE2 800B0001 000C0004 0028DE80

Responder Internals:
CKY-R
   01D3BF55 08A31C87
SA
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFF2
   8004FFF6 8003FFE2 800B0001 000C0004 0028DE80

Initiator <- Responder

Responder's Packet IKE phase 1 (2)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   01100200
Message ID
   00000000
Length
   00000054
Security Association
   00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFF2
   8004FFF6 8003FFE2 800B0001 000C0004 0028DE80
Responder's Packet IKE phase 1 (2)
   9F3F56E2 F256015E 01D3BF55 08A31C87 01100200 00000000 00000054 00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFF2
```

```
   8004FFF6 8003FFE2 800B0001 000C0004 0028DE80

Initiator Internals:
Ni_b
   C51D5D4B 236952BC A6EEF7BD 18021798
x_i
   5CBD1702 68641A6E F47003E4 9E04BC5A A3146674 B70DAB3B D87F3CAF 8EB3CDE5
   A0A0FA99 8F92BC59 B8A119D3 508E16B3 AEA4760D D682F659 FB1C105F EED16596
gx_i
   357AC0CF 30683956 C5748EDA 910B85F9 E413C518 EE8B9A83 D89E5D26 4C07442C
   4802E803 4E4302C4 8E3A2AD2 D17305BD 8483006A 86E41876 1E0C45AA 5D2C54D3
   39648886 3EF766C1 F60DF71A 33CAA04D A844862E 1BA580B3 0C105FD6 D0B06706
   A31FF574 217DB0FD 5DCA7310 40F588E7 611C93E5 8FD44777 97819FC4 AC5FEFF2

Initiator -> Responder

Initiator's Packet IKE phase 1 (3)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   04100200
Message ID
   00000000
Length
   000000B4
Key exchange
   0A000084
   357AC0CF 30683956 C5748EDA 910B85F9 E413C518 EE8B9A83 D89E5D26 4C07442C
   4802E803 4E4302C4 8E3A2AD2 D17305BD 8483006A 86E41876 1E0C45AA 5D2C54D3
   39648886 3EF766C1 F60DF71A 33CAA04D A844862E 1BA580B3 0C105FD6 D0B06706
   A31FF574 217DB0FD 5DCA7310 40F588E7 611C93E5 8FD44777 97819FC4 AC5FEFF2
Nonce
   00000014
   C51D5D4B 236952BC A6EEF7BD 18021798
Initiator's Packet IKE phase 1 (3)
   9F3F56E2 F256015E 01D3BF55 08A31C87 04100200 00000000 000000B4 0A000084
   357AC0CF 30683956 C5748EDA 910B85F9 E413C518 EE8B9A83 D89E5D26 4C07442C
   4802E803 4E4302C4 8E3A2AD2 D17305BD 8483006A 86E41876 1E0C45AA 5D2C54D3
   39648886 3EF766C1 F60DF71A 33CAA04D A844862E 1BA580B3 0C105FD6 D0B06706
   A31FF574 217DB0FD 5DCA7310 40F588E7 611C93E5 8FD44777 97819FC4 AC5FEFF2
   00000014 C51D5D4B 236952BC A6EEF7BD 18021798

Responder Internals:
Nr_b
   CC53338C A5CD4FAB 6C388D7C CC7B6054
x_r
   6395F918 C27C9BB9 84F061DC 3D630462 BFC5E9A8 FEABEA28 137EFFA8 3B60938C
   B230BED7 1EC6C602 70B53995 CE27094D 9F76A507 9AD596FD C68A9A07 639CA489
gx_r
   71E4BB28 476F683C 43AC64E9 2B64470E 527AA8D9 9FD6F203 D38754B9 F9C8DA9B
```

```
   67492EA5 D1D1926E 9D7D9888 D23073FD F28B8E11 F73F522B 7F4D0214 1E6A46A8
   3959667B 7C39D2DB F9FAD346 9D2ACE3B 17A56BA1 CCF17458 99C0F358 3B0DA235
   1F899822 23A37FC8 E0BA4506 E0167D0F 1B81E8E5 70A32156 7920F33D 261E6BE6

Initiator <- Responder

Responder's Packet IKE phase 1 (4)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   04100200
Message ID
   00000000
Length
   000000B4
Key exchange
   0A000084
   71E4BB28 476F683C 43AC64E9 2B64470E 527AA8D9 9FD6F203 D38754B9 F9C8DA9B
   67492EA5 D1D1926E 9D7D9888 D23073FD F28B8E11 F73F522B 7F4D0214 1E6A46A8
   3959667B 7C39D2DB F9FAD346 9D2ACE3B 17A56BA1 CCF17458 99C0F358 3B0DA235
   1F899822 23A37FC8 E0BA4506 E0167D0F 1B81E8E5 70A32156 7920F33D 261E6BE6
Nonce
   00000014
   CC53338C A5CD4FAB 6C388D7C CC7B6054
Responder's Packet IKE phase 1 (4)
   9F3F56E2 F256015E 01D3BF55 08A31C87 04100200 00000000 000000B4 0A000084
   71E4BB28 476F683C 43AC64E9 2B64470E 527AA8D9 9FD6F203 D38754B9 F9C8DA9B
   67492EA5 D1D1926E 9D7D9888 D23073FD F28B8E11 F73F522B 7F4D0214 1E6A46A8
   3959667B 7C39D2DB F9FAD346 9D2ACE3B 17A56BA1 CCF17458 99C0F358 3B0DA235
   1F899822 23A37FC8 E0BA4506 E0167D0F 1B81E8E5 70A32156 7920F33D 261E6BE6
   00000014 CC53338C A5CD4FAB 6C388D7C CC7B6054

Initiator Internals:
Site ID
   11783
Net ID
   Net73
PSK IR
   D74RLXM4UE1FQC834G3EQBZAZ51WBXAF0VM9VG4RPCDKVEK83ZU9LZ1W
PSK Time Not After
   UTC Sat Oct 31 21:00:00 2009
PSK
   E7BCDC1B 0B7E8E97 B76B815A CB23E786 C25BC86F 68DE3073 3CBEF2A5 A5DA578C
ID_ii
   01000000 C0000201
akey
   C9FF3EAC 3F4A12A1 19B22445 42D56641 DE04AA5C 03FFFF49 460FF956 CA13284B
SKEYID
   98EBF9D3 D43B8A21 7B161E5C B8B753C8 169034F0 D3F958E1 57926969 C1693037
   223AEDDE 8CC71FB5 EEBEEC4D 2F81182E 21BE969B 5611FDD9 EC992471 635D608B
```

```
SKEYID_d
   86740720 C0FD04AF D2E424AE EA08B709 D7DD218F 1C7779A0 7814465F 9B621F47
   0228950F 1C302EC9 F2657E77 9D46F88F 0A351427 C3A58E40 9F4E1941 6399F48F
SKEYID_a
   FBAFF7F2 F1F52918 6B278D09 DBAAF6C7 B1458E3B 1CF37806 1A9BBB29 8D7B5F27
   8230A307 0B2C016B E5C18AC4 B33CFDBA 408E4904 6034033D 0688ED8E 2EB1681D
SKEYID_e
   B0BD5AE1 4FF08B05 781CE5D5 D7E56FB4 E39DB83C 8398C5D9 4450694F DFE7440B
   14953AE5 22835828 51AFDD2D 3B87FF14 743257F2 0461DAD7 0CF399FE 53D7AB2F
SK_e
   AA3F6B06 F2379D6C 67374935 19F036D4 5EF4CA00 A1C304AD 33E0447B C5EF497A
SK_a
   AA3F6B06 F2379D6C 67374935 19F036D4 5EF4CA00 A1C304AD 33E0447B C5EF497A
IV
   5C1B7F4E 0D3F2241
HASH_I
   22D2FE84 DF46BA51 737CDECA FEF13994 E05F2ABE A1B7671A E522B6E2 3DDB7773
   15096ADC E898F722 3CA6B271 B0A3991F 76BF10FF 4AE53585 C14A9D31 57D3E4F2
AUTH_I
   72197F20 F528F74F BC088189 EC8C7E7F 72821D9F 405CD8E2 357FC049 244DD95B
   FDBB4ADD 4FFDFF40 FD1AEE60 8AB3DB16 2AA5481C BFE42CE3 1945ABBE F7B8C0F7

Initiator -> Responder

Initiator's Packet IKE phase 1 (5)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   05100201
Message ID
   00000000
Length
   00000080
Identification
   0800000C
   01000000 C0000201
Hash
   00000044
   22D2FE84 DF46BA51 737CDECA FEF13994 E05F2ABE A1B7671A E522B6E2 3DDB7773
   15096ADC E898F722 3CA6B271 B0A3991F 76BF10FF 4AE53585 C14A9D31 57D3E4F2
Initiator's Packet IKE phase 1 (5)
   9F3F56E2 F256015E 01D3BF55 08A31C87 05100201 00000000 00000080 0800000C
   01000000 C0000201 00000044 22D2FE84 DF46BA51 737CDECA FEF13994 E05F2ABE
   A1B7671A E522B6E2 3DDB7773 15096ADC E898F722 3CA6B271 B0A3991F 76BF10FF
   4AE53585 C14A9D31 57D3E4F2
Encapsulated Initiator's Packet IKE phase 1 (5)
   9F3F56E2 F256015E 01D3BF55 08A31C87 05100201 00000000 00000080 00000000
   00000000 93D23DBB 8AE59F76 90EB16EA F82C7BB1 74276844 ABD158E4 DCCBD7FB
   8AA2AD18 03D65805 9AB011FC D59992AD 79582003 E8F3DAFF 879FE029 510A3A07
   4F94A6E9 2BA671A6 1B473E87 1DEDAD09 D6ED7925 4F6B7970 C83A3208 B04B2155
```

```
Responder Internals:
Site ID
   01:23:45:67:89:01:2345678901234567890123456780
Net ID
   Net73
PSK IR
   D74RLXM4UE1FQC834G3EQBZAZ51WBXAF0VM9VG4RPCDKVEK83ZU9LZ1W
PSK Time Not After
   UTC Sat Oct 31 21:00:00 2009
PSK
   E7BCDC1B 0B7E8E97 B76B815A CB23E786 C25BC86F 68DE3073 3CBEF2A5 A5DA578C
ID_ir
   01000000 C0000221
akey
   C9FF3EAC 3F4A12A1 19B22445 42D56641 DE04AA5C 03FFFF49 460FF956 CA13284B
SKEYID
   98EBF9D3 D43B8A21 7B161E5C B8B753C8 169034F0 D3F958E1 57926969 C1693037
   223AEDDE 8CC71FB5 EEBEEC4D 2F81182E 21BE969B 5611FDD9 EC992471 635D608B
SKEYID_d
   86740720 C0FD04AF D2E424AE EA08B709 D7DD218F 1C7779A0 7814465F 9B621F47
   0228950F 1C302EC9 F2657E77 9D46F88F 0A351427 C3A58E40 9F4E1941 6399F48F
SKEYID_a
   FBAFF7F2 F1F52918 6B278D09 DBAAF6C7 B1458E3B 1CF37806 1A9BBB29 8D7B5F27
   8230A307 0B2C016B E5C18AC4 B33CFDBA 408E4904 6034033D 0688ED8E 2EB1681D
SKEYID_e
   B0BD5AE1 4FF08B05 781CE5D5 D7E56FB4 E39DB83C 8398C5D9 4450694F DFE7440B
   14953AE5 22835828 51AFDD2D 3B87FF14 743257F2 0461DAD7 0CF399FE 53D7AB2F
SK_e
   AA3F6B06 F2379D6C 67374935 19F036D4 5EF4CA00 A1C304AD 33E0447B C5EF497A
SK_a
   AA3F6B06 F2379D6C 67374935 19F036D4 5EF4CA00 A1C304AD 33E0447B C5EF497A
IV
   5C1B7F4E 0D3F2241
HASH_R
   139FD79E C6AA3085 3CECDDC3 7018E6FE 5A3D7F8C A944C8B9 A7B392CB 4E24B47B
   5BF9B1CF E205A206 02CB8BA8 582026AA 9F52CFC0 A17F321C FB4CD289 4F370186
AUTH_R
   AF91AE9B 0B985048 F0EDF196 8FCD76A9 91D330A9 835B3715 675384FC 83843F6F
   1B64400E F8159CB6 45A2A143 A273AC6C 1CF1F388 9A0D2F80 6C78AC42 920CEE86

Initiator <- Responder

Responder's Packet IKE phase 1 (6)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   05100201
Message ID
   00000000
```

```
Length
   00000080
Identification
   0800000C
   01000000 C0000221
Hash
   00000044
   139FD79E C6AA3085 3CECDDC3 7018E6FE 5A3D7F8C A944C8B9 A7B392CB 4E24B47B
   5BF9B1CF E205A206 02CB8BA8 582026AA 9F52CFC0 A17F321C FB4CD289 4F370186
Responder's Packet IKE phase 1 (6)
   9F3F56E2 F256015E 01D3BF55 08A31C87 05100201 00000000 00000080 0800000C
   01000000 C0000221 00000044 139FD79E C6AA3085 3CECDDC3 7018E6FE 5A3D7F8C
   A944C8B9 A7B392CB 4E24B47B 5BF9B1CF E205A206 02CB8BA8 582026AA 9F52CFC0
   A17F321C FB4CD289 4F370186
Encapsulated Responder's Packet IKE phase 1 (6)
   9F3F56E2 F256015E 01D3BF55 08A31C87 05100201 00000000 00000080 00000000
   00000000 D5C67846 A7D5EF67 F90C9C93 652B2E89 C66BC14D 3C256B83 CA50776B
   5329379C 3DCA10B2 8B559EA1 FB327AE6 452A03A9 763A9F3C 5907E7D2 7EB02F3A
   93C99136 87A600F7 361F9F23 6CAA7F54 5893BB5D AA0ED417 A7047F5B 1F4EDB04

IKE phase2 Quick Mode PFS

Initiator Internals:
Message ID
   8EA17A5F
Message Nonce
   79119ECD 508B4EED
SPI
   0BDE051D
Transform ID
   FC000000
SA
   00000001 00000001 00000020 01030401 0BDE051D 00000014 01FC0000 80040002
   FE91FF7F 8003FFF6
Ni_b
   66DCE7DC CBCF602B BA75C499 28204D0A
ID_ci
   01010000 C0000201
x_i
   EA87B32A 3008FB73 EB45684F 3795DAAE F55C3A4A 7A7C42AB 149928FE 3DC87796
   AF823379 CC857CF2 9EF4004B 0F87A6B4 5EDE89F6 A580C752 7CC1F441 1A66E644
KE_i
   B12F05B4 83C780D4 A7B05734 36F000FC D0813D4D 90B44DC0 ACFDE365 03C556BB
   D5AFF6D3 5681A25A 7BEDA95C 287B4249 D420F6AC 096D0BBC DCA406FD B0C190AB
   15600B33 45664461 9A749143 443766B6 439B5124 613D7B29 2E7AE956 5517C516
   762F6897 5A991D4F C2F90230 28C447B3 CBA578CA 43254DB2 255463C8 2130B82B
gm_ir
   50003F29 91E03F0C 6367FF18 5B809C77 72C7D876 E9B68244 07CE746C 2D30CF93
SK_e
   027ED8C2 585702AF 23B5BEE3 35B46D6D F0086042 CF975BAB E8BF985D B9A32BA2
SK_a
   027ED8C2 585702AF 23B5BEE3 35B46D6D F0086042 CF975BAB E8BF985D B9A32BA2
```

```
IV
   3349F4AA F5FED26A
HASH(1)
   BB2F21B9 26290584 852507DE 96DCDCA2 0FB6295D AFF0E3D3 B222C5B5 D88638EA
   9201D91B 59CA1017 78894694 888EDC8A 29BB016A 180A0728 9BD57186 4A0D27EE

Initiator -> Responder

Initiator's Packet IKE phase 2 (1)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   08102001
Message ID
   8EA17A5F
Length
   00000150
Hash
   01000044
   BB2F21B9 26290584 852507DE 96DCDCA2 0FB6295D AFF0E3D3 B222C5B5 D88638EA
   9201D91B 59CA1017 78894694 888EDC8A 29BB016A 180A0728 9BD57186 4A0D27EE
Security Association
   0A00002C
   00000001 00000001 00000020 01030401 0BDE051D 00000014 01FC0000 80040002
   FE91FF7F 8003FFF6
Nonce
   04000014
   66DCE7DC CBCF602B BA75C499 28204D0A
Key exchange
   05000084
   B12F05B4 83C780D4 A7B05734 36F000FC D0813D4D 90B44DC0 ACFDE365 03C556BB
   D5AFF6D3 5681A25A 7BEDA95C 287B4249 D420F6AC 096D0BBC DCA406FD B0C190AB
   15600B33 45664461 9A749143 443766B6 439B5124 613D7B29 2E7AE956 5517C516
   762F6897 5A991D4F C2F90230 28C447B3 CBA578CA 43254DB2 255463C8 2130B82B
Identification
   0500000C
   01010000 C0000201
Identification
   0000000C
   01010000 C0000221
Initiator's Packet IKE phase 2 (1)
   9F3F56E2 F256015E 01D3BF55 08A31C87 08102001 8EA17A5F 00000150 01000044
   BB2F21B9 26290584 852507DE 96DCDCA2 0FB6295D AFF0E3D3 B222C5B5 D88638EA
   9201D91B 59CA1017 78894694 888EDC8A 29BB016A 180A0728 9BD57186 4A0D27EE
   0A00002C 00000001 00000001 00000020 01030401 0BDE051D 00000014 01FC0000
   80040002 FE91FF7F 8003FFF6 04000014 66DCE7DC CBCF602B BA75C499 28204D0A
   05000084 B12F05B4 83C780D4 A7B05734 36F000FC D0813D4D 90B44DC0 ACFDE365
   03C556BB D5AFF6D3 5681A25A 7BEDA95C 287B4249 D420F6AC 096D0BBC DCA406FD
   B0C190AB 15600B33 45664461 9A749143 443766B6 439B5124 613D7B29 2E7AE956
   5517C516 762F6897 5A991D4F C2F90230 28C447B3 CBA578CA 43254DB2 255463C8
```

```
   2130B82B 0500000C 01010000 C0000201 0000000C 01010000 C0000221
Encapsulated Initiator's Packet IKE phase 2 (1)
   9F3F56E2 F256015E 01D3BF55 08A31C87 08102001 8EA17A5F 00000150 79119ECD
   508B4EED 96113CAD 9D180BF1 EC89A330 951BF312 FF973167 5CA1F032 E7198E74
   44FA46B4 48BA527D 2E260CD7 D6CB6574 80F1C39F 6E01C70C 03D78B28 01ACD8F3
   B26D8DAD E46CEF1F 7CBE0618 43FBDFC9 D33DEB9E DAD1CD41 97D757C1 01A14423
   EE178341 770D8CA2 4264E549 8DE5CDFD A01B5406 C9159EA9 C95BAC2F FAEEA63F
   BAB6BAE0 CE2469B3 F4902E2F 96F10D13 E71ADB29 0E313793 39124DB8 E7F5DBFC
   67CDEECC 3523C52A 4BDF48E4 78125D69 E073C98D 8BDA9A9A 49040F12 921D62C7
   971FD1BA 008C849B 5E59759F 6424BA45 8A4EF8C4 51763872 E2F860F2 2A3F6819
   A999AAEB D11AF92A 8B4CFC2F 1F1FEDB5 2F0920FD 404CAB82 2E25B25F 0C609439
   D7578640 665B92A4 C6B9AD41 BFD94631 3F50890C 13C383EE CD430C0A 9C6E818D
   633FFA17 C44F6115 EEFF6E99 1C6D04CA

Responder Internals:
SPI
   A6395A7E
Transform ID
   FC000000
SA
   00000001 00000001 00000020 01030401 A6395A7E 00000014 01FC0000 80040002
   FE91FF7F 8003FFF6
Nr_b
   A5504B99 EE9C7D3C 4281A8EF 6A674769
ID_cr
   01010000 C0000221
x_r
   50A92AB9 F394A37C 0638429D 4F975CE3 845481FE 3E0EE4D8 CF6CA427 062579F8
   C6F1F4D7 53FDAD6B 47E8A7DB D1E121D8 6FCEB204 AEC3E8D6 BB5E630F A2AD1721
KE_r
   FBF5AFD3 F593C980 758F0A5D C3653607 F1DAA0B2 58E1FE1E 1C04990F 74B18CEA
   2E4C85CF D212AF09 56021B7B 9DEC301A 6B8C0F43 EFEBF72D 21D8E9D1 530E80F7
   C5E3E848 00BB2240 4EAD308F 4685550C F468A546 34B86CC4 141A8293 9224FA68
   2BF413BA ED099801 8F9AEFB7 9056779C 072DCF29 CBCD39FC BD0B228E B342B5AE
gm_ir
   50003F29 91E03F0C 6367FF18 5B809C77 72C7D876 E9B68244 07CE746C 2D30CF93
SK_e
   027ED8C2 585702AF 23B5BEE3 35B46D6D F0086042 CF975BAB E8BF985D B9A32BA2
SK_a
   027ED8C2 585702AF 23B5BEE3 35B46D6D F0086042 CF975BAB E8BF985D B9A32BA2
IV
   3349F4AA F5FED26A
HASH(2)
   0BEB7E92 362628FA FCBE6771 C88191AC 53F229A5 493DFC26 38BF3805 B7F13044
   49059997 7DFEA073 5B7094F5 BDF2E28C CAECECF6 A1974CC3 538D55F0 78B4B8D4

Initiator <- Responder

Responder's Packet IKE phase 2 (2)
CKY-I
   9F3F56E2 F256015E
CKY-R
```

```
   01D3BF55 08A31C87
Flags
   08102001
Message ID
   8EA17A5F
Length
   00000150
Hash
   01000044
   0BEB7E92 362628FA FCBE6771 C88191AC 53F229A5 493DFC26 38BF3805 B7F13044
   49059997 7DFEA073 5B7094F5 BDF2E28C CAECECF6 A1974CC3 538D55F0 78B4B8D4
Security Association
   0A00002C
   00000001 00000001 00000020 01030401 A6395A7E 00000014 01FC0000 80040002
   FE91FF7F 8003FFF6
Nonce
   04000014
   A5504B99 EE9C7D3C 4281A8EF 6A674769
Key exchange
   05000084
   FBF5AFD3 F593C980 758F0A5D C3653607 F1DAA0B2 58E1FE1E 1C04990F 74B18CEA
   2E4C85CF D212AF09 56021B7B 9DEC301A 6B8C0F43 EFEBF72D 21D8E9D1 530E80F7
   C5E3E848 00BB2240 4EAD308F 4685550C F468A546 34B86CC4 141A8293 9224FA68
   2BF413BA ED099801 8F9AEFB7 9056779C 072DCF29 CBCD39FC BD0B228E B342B5AE
Identification
   0500000C
   01010000 C0000201
Identification
   0000000C
   01010000 C0000221
Responder's Packet IKE phase 2 (2)
   9F3F56E2 F256015E 01D3BF55 08A31C87 08102001 8EA17A5F 00000150 01000044
   0BEB7E92 362628FA FCBE6771 C88191AC 53F229A5 493DFC26 38BF3805 B7F13044
   49059997 7DFEA073 5B7094F5 BDF2E28C CAECECF6 A1974CC3 538D55F0 78B4B8D4
   0A00002C 00000001 00000001 00000020 01030401 A6395A7E 00000014 01FC0000
   80040002 FE91FF7F 8003FFF6 04000014 A5504B99 EE9C7D3C 4281A8EF 6A674769
   05000084 FBF5AFD3 F593C980 758F0A5D C3653607 F1DAA0B2 58E1FE1E 1C04990F
   74B18CEA 2E4C85CF D212AF09 56021B7B 9DEC301A 6B8C0F43 EFEBF72D 21D8E9D1
   530E80F7 C5E3E848 00BB2240 4EAD308F 4685550C F468A546 34B86CC4 141A8293
   9224FA68 2BF413BA ED099801 8F9AEFB7 9056779C 072DCF29 CBCD39FC BD0B228E
   B342B5AE 0500000C 01010000 C0000201 0000000C 01010000 C0000221
Encapsulated Responder's Packet IKE phase 2 (2)
   9F3F56E2 F256015E 01D3BF55 08A31C87 08102001 8EA17A5F 00000150 79119ECD
   508B4EED 8AF71911 3A6B8F59 97761454 3C2C7778 4084D13D 1A7E07D1 705D19E0
   37544195 7E9F996C 404B0F16 E33775F3 57D002F5 895D9518 81B9F8BC F6018F11
   0E0832CC 4AEFF3CD B4D7EFFD EDBD4628 5C595479 991EF4A2 A5CE1A4C 74E217C2
   78875F10 DB63F8C8 E8DB1A74 648E72B4 A4F552C0 B72995F0 034F6BCD 3124A8CE
   AAD3CC88 493031D1 8DC6D5F9 4F27A264 804118B2 7EF9D54B 71D5C5FF 9145F4E1
   734388D2 0D4C5923 ED0DE321 345565A2 CCA7B7BB C06579F6 0861EA17 B1E24C9B
   D6CA0389 F0A1B6CE 31F037D5 608F6998 32480C64 0B15E4F1 60848F01 F60B48A8
   73B94989 A909D26D FD46EA9F 0FE2A943 27C96E42 2FD5E38F 59AC464C F3A1BEB7
   2ABA9FA3 9406AC69 5D75669D 30305DE6 15133977 5A2433AE 76BB953D 8EE9E073
```

```
   6211369F C2059D40 CFF6FFDA F764BB9F

Initiator Internals:
HASH(3)
   97ACECC5 049BE84A F1D2CC25 D09E9763 E07BBF0C ACF750E7 5C61756D 0BE9354E
   C0D77D1A 03EA3023 C4C6995A 96D4B300 4E4DD26B 7D04B55C 4FB56EC7 2C49F2BA

Initiator -> Responder

Initiator's Packet IKE phase 2 (3)
CKY-I
   9F3F56E2 F256015E
CKY-R
   01D3BF55 08A31C87
Flags
   08102001
Message ID
   8EA17A5F
Length
   00000070
Hash
   00000044
   97ACECC5 049BE84A F1D2CC25 D09E9763 E07BBF0C ACF750E7 5C61756D 0BE9354E
   C0D77D1A 03EA3023 C4C6995A 96D4B300 4E4DD26B 7D04B55C 4FB56EC7 2C49F2BA
Initiator's Packet IKE phase 2 (3)
   9F3F56E2 F256015E 01D3BF55 08A31C87 08102001 8EA17A5F 00000070 00000044
   97ACECC5 049BE84A F1D2CC25 D09E9763 E07BBF0C ACF750E7 5C61756D 0BE9354E
   C0D77D1A 03EA3023 C4C6995A 96D4B300 4E4DD26B 7D04B55C 4FB56EC7 2C49F2BA
Encapsulated Initiator's Packet IKE phase 2 (3)
   9F3F56E2 F256015E 01D3BF55 08A31C87 08102001 8EA17A5F 00000070 79119ECD
   508B4EED 2246E487 E5E932F7 D448B036 9F0AE54F B1BBF9C2 8BF00888 1EFCDD99
   C343ACA8 C03ED3AF ADF15767 636E7F61 8B0DD0B3 3F7020E2 AF77B4D1 F9E9FCE7
   1A90FCD7 B8735C74 7BE5E769 C834C3B5

TRANSFORM_ID=CPESP_GOST_1K_IMIT

Initiator's inbound SA
KEYMAT
   391A8602 6FB467F5 3715EED7 B59A06EE 52C8B55A DAE08AEB 8427C934 FD8FC09C
   25915BE9 251A1D11 6DA9BE2E 1F7949CD B352B6C8 77295540 AECB220D F9DAA507
   70A954C7

Initiator's outbound SA
KEYMAT
   4795099D 2D5596CA A847A428 502F5352 20C94797 B25C6593 35A1E5CF 355FCBA7
   A967A3FA D38A00FB 865F9450 BAEB759D FF6BE9D5 9A5CE54D 2B4CF6D3 39E8F108
   40435C12

Responder's inbound SA
KEYMAT
   4795099D 2D5596CA A847A428 502F5352 20C94797 B25C6593 35A1E5CF 355FCBA7
   A967A3FA D38A00FB 865F9450 BAEB759D FF6BE9D5 9A5CE54D 2B4CF6D3 39E8F108
```

```
   40435C12

Responder's outbound SA
KEYMAT
   391A8602 6FB467F5 3715EED7 B59A06EE 52C8B55A DAE08AEB 8427C934 FD8FC09C
   25915BE9 251A1D11 6DA9BE2E 1F7949CD B352B6C8 77295540 AECB220D F9DAA507
   70A954C7
```

9.2 Пример GOST-IKE-SIGNATURE

В примерах используются параметры сопоставления безопасности, принятые по умолчанию:

- Шифрование обмена ISAKMP с узлом замены id-tc26-gost-28147-param-Z в режиме гаммирования с обратной связью и усложнением ключа (см. п. 3.2.3 в **RFC4357**);
- Параметры алгоритма VKO - id-GostR3410-2001-CryptoPro-XchA-ParamSet+id-tc26-gost3411-12-256; PRF на основе ГОСТ Р 34.11-94.

```
IKE phase1 Signature Authentication Main Mode

Security Association
DH_OID=1.2.643.2.2.36.0
CIPHER_OID=1.2.643.7.1.2.5.1.1
HASH_OID=1.2.643.2.2.9

Initiator Internals:
CKY-I
   55D5D33D 9B0BC56C
SA
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFDD
   8004FFF4 8003FFE4 800B0001 000C0004 0028DE80

Initiator -> Responder

Initiator's Packet IKE phase 1 (1)
CKY-I
   55D5D33D 9B0BC56C
Flags
   01100200
Message ID
   00000000
Length
   00000054
Security Association
   00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFDD
   8004FFF4 8003FFE4 800B0001 000C0004 0028DE80
Initiator's Packet IKE phase 1 (1)
   55D5D33D 9B0BC56C 00000000 00000000 01100200 00000000 00000054 00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFDD
   8004FFF4 8003FFE4 800B0001 000C0004 0028DE80
```

```
Responder Internals:
CKY-R
   CFA1A8D3 D2AF5BEB
SA
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFDD
   8004FFF4 8003FFE4 800B0001 000C0004 0028DE80

Initiator <- Responder

Responder's Packet IKE phase 1 (2)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   01100200
Message ID
   00000000
Length
   00000054
Security Association
   00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFDD
   8004FFF4 8003FFE4 800B0001 000C0004 0028DE80
Responder's Packet IKE phase 1 (2)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 01100200 00000000 00000054 00000038
   00000001 00000001 0000002C 01010001 00000024 01010000 8001FFF3 8002FFDD
   8004FFF4 8003FFE4 800B0001 000C0004 0028DE80

Initiator Internals:
Ni_b
   727991D7 7D0F5F34 3E58AD39 4E2FFE5F
x_i
   732A1C7A D48CC42E ABA3CC38 4D6F4F2D 7699DBBD 1453E50F 078B506C 3C2B4084
gx_i
   F86621AC CE5953EC D5376531 2046C92A 6E57824A 91E19B0E 12A73BE4 7356120D
   A807FE20 75040578 23F05DD4 7E9AC92E 61A7C418 F2299A0C 7B555E89 04E9DA04

Initiator -> Responder

Initiator's Packet IKE phase 1 (3)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   04100200
Message ID
   00000000
Length
   00000074
Key exchange
```

```
   0A000044
   F86621AC CE5953EC D5376531 2046C92A 6E57824A 91E19B0E 12A73BE4 7356120D
   A807FE20 75040578 23F05DD4 7E9AC92E 61A7C418 F2299A0C 7B555E89 04E9DA04
Nonce
   00000014
   727991D7 7D0F5F34 3E58AD39 4E2FFE5F
Initiator's Packet IKE phase 1 (3)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 04100200 00000000 00000074 0A000044
   F86621AC CE5953EC D5376531 2046C92A 6E57824A 91E19B0E 12A73BE4 7356120D
   A807FE20 75040578 23F05DD4 7E9AC92E 61A7C418 F2299A0C 7B555E89 04E9DA04
   00000014 727991D7 7D0F5F34 3E58AD39 4E2FFE5F

Responder Internals:
Nr_b
   7CA3E945 E314B0AF 7A1D1B3D 915B78FD
x_r
   E225524F 67B63734 9D84C51A 85D9D05D D45199A7 D35013EA AB1EAFE0 1726B1F5
gx_r
   0879F31F FACF4960 59A47902 2139C076 E6C4E736 AB8845CD E8ADB468 7011F4BA
   2F53AA01 B881A66E 1165DBD4 E5036BE4 D6E76365 04272566 61D73156 31F552B8

Initiator <- Responder

Responder's Packet IKE phase 1 (4)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   04100200
Message ID
   00000000
Length
   00000079
Key exchange
   0A000044
   0879F31F FACF4960 59A47902 2139C076 E6C4E736 AB8845CD E8ADB468 7011F4BA
   2F53AA01 B881A66E 1165DBD4 E5036BE4 D6E76365 04272566 61D73156 31F552B8
Nonce
   07000014
   7CA3E945 E314B0AF 7A1D1B3D 915B78FD
Certificate Request
   00000005
   04
Responder's Packet IKE phase 1 (4)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 04100200 00000000 00000079 0A000044
   0879F31F FACF4960 59A47902 2139C076 E6C4E736 AB8845CD E8ADB468 7011F4BA
   2F53AA01 B881A66E 1165DBD4 E5036BE4 D6E76365 04272566 61D73156 31F552B8
   07000014 7CA3E945 E314B0AF 7A1D1B3D 915B78FD 00000005 04

Initiator Internals:
k_i
```

0E21F5D5 2692EB21 7FFAA47C 3A2681DE FBC2519A B2323E52 75D0FDA1 0F046AEA
Initiator's Signature Public Key Blob
06200000 492E0000 4D414731 00020000 30130607 2A850302 02240006 082A8503
07010102 020B6206 DE25E6CF 34331B24 A6061B45 E4E317DD 8E786FE5 FFEE1CEF
2CEF2512 31DC2925 74703FCF 38577F07 BDBD3413 FED40383 8C78987D 4DA9ACF4
CA58D6F6 33
CERT_I
04308202 B8308202 67A00302 0102020A 50CA968D 000000B0 A7FD3008 06062A85
03020203 303A3112 3010060A 09922689 93F22C64 01191602 72753112 3010060A
09922689 93F22C64 01191602 63703110 300E0603 55040313 07746573 742D6361
301E170D 31343037 32383033 32323134 5A170D32 34303732 38313030 3231345A
30293127 30250603 5504030C 1E544348 72705067 685F494E 49544941 544F525F
5F323536 5F323031 325F4130 66301F06 082A8503 07010101 01301306 072A8503
02022400 06082A85 03070101 02020343 0004400B 6206DE25 E6CF3433 1B24A606
1B45E4E3 17DD8E78 6FE5FFEE 1CEF2CEF 251231DC 29257470 3FCF3857 7F07BDBD
3413FED4 03838C78 987D4DA9 ACF4CA58 D6F633A3 82015930 82015530 13060355
1D25040C 300A0608 2B060105 05080202 300E0603 551D0F01 01FF0404 030204F0
301D0603 551D0E04 160414A2 9D725D92 133AFE85 FAFB9541 DF8E9940 E1108030
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 00C22CA9
0E8C38FD 487EE2DA 393495A1 6CC0B670 DBD63F61 F4E095F2 49859938 69095367
35FA4136 1FD1C401 255E1E26 10B993BB 4E39786D 17CF0926 A2FBBC6F F4
ID_ii
09000000 30293127 30250603 55040313 1E544348 72705067 685F494E 49544941
544F525F 5F323536 5F323031 325F41
akey
56CED698 2218C189 69757071 90671857 5229104C 12BA7D1D 9FC48552 D894916F
SKEYID
A56DFC7F F22A837E 6DB897FE 8718216C 4C18BE4A 6736F3EA 98908545 3AD61180
SKEYID_d
6DC370CE 1C367C10 CB9F07D5 D04F9985 7E38A6A8 0BCFBF27 870D2417 E8224B79
SKEYID_a
491374E5 0853B8AF 3938DEF1 18BB2476 04FE52BA 399A7284 11399CD3 A1F98CC7
SKEYID_e
17141F4E C23F5340 81481FCE 99304091 325FFDC9 8D6F286F 5E60ECE1 A131F480
SK_e
A9282E05 618D3F29 A8EFCDF8 C02F5C31 1D88F679 E72EA894 10C4E7BA 9D44B63A
SK_a
A9282E05 618D3F29 A8EFCDF8 C02F5C31 1D88F679 E72EA894 10C4E7BA 9D44B63A
IV
47A68CF4 F8830640
HASH_I
895C9AE7 F1780D2A 523C2428 D831C671 4E5226C7 2FD526BF A83CEBA1 05F2F0DC
SIG_I
700F56A6 C3812E70 BE3BC97F AA0CE371 58AF97B4 2D3F36B1 268F4C3D E7DD7265

```
   ACEF8391 D9EE8FB4 8083A675 C77BB8FF D167BDB5 B0898FB6 CE5B5A23 1A8103D4
AUTH_I
   AAFF3F8A ABDDD217 4A58A917 6194CF8B BBC15C4A E3B97592 D9524AE0 EA54A271

Initiator -> Responder

Initiator's Packet IKE phase 1 (5)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   05100201
Message ID
   00000000
Length
   00000368
Identification
   06000033
   09000000 30293127 30250603 55040313 1E544348 72705067 685F494E 49544941
   544F525F 5F323536 5F323031 325F41
Certificate
   090002C1
   04308202 B8308202 67A00302 0102020A 50CA968D 000000B0 A7FD3008 06062A85
   03020203 303A3112 3010060A 09922689 93F22C64 01191602 72753112 3010060A
   09922689 93F22C64 01191602 63703110 300E0603 55040313 07746573 742D6361
   301E170D 31343037 32383033 32323134 5A170D32 34303732 38313030 3231345A
   30293127 30250603 5504030C 1E544348 72705067 685F494E 49544941 544F525F
   5F323536 5F323031 325F4130 66301F06 082A8503 07010101 01301306 072A8503
   02022400 06082A85 03070101 02020343 0004400B 6206DE25 E6CF3433 1B24A606
   1B45E4E3 17DD8E78 6FE5FFEE 1CEF2CEF 251231DC 29257470 3FCF3857 7F07BDBD
   3413FED4 03838C78 987D4DA9 ACF4CA58 D6F633A3 82015930 82015530 13060355
   1D25040C 300A0608 2B060105 05080202 300E0603 551D0F01 01FF0404 030204F0
   301D0603 551D0E04 160414A2 9D725D92 133AFE85 FAFB9541 DF8E9940 E1108030
   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 00C22CA9
   0E8C38FD 487EE2DA 393495A1 6CC0B670 DBD63F61 F4E095F2 49859938 69095367
   35FA4136 1FD1C401 255E1E26 10B993BB 4E39786D 17CF0926 A2FBBC6F F4
Signature
   07000044
   700F56A6 C3812E70 BE3BC97F AA0CE371 58AF97B4 2D3F36B1 268F4C3D E7DD7265
   ACEF8391 D9EE8FB4 8083A675 C77BB8FF D167BDB5 B0898FB6 CE5B5A23 1A8103D4
Certificate Request
   00000005
   04
```

```
Initiator's Packet IKE phase 1 (5)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 05100201 00000000 00000368 06000033
   09000000 30293127 30250603 55040313 1E544348 72705067 685F494E 49544941
   544F525F 5F323536 5F323031 325F4109 0002C104 308202B8 30820267 A0030201
   02020A50 CA968D00 0000B0A7 FD300806 062A8503 02020330 3A311230 10060A09
   92268993 F22C6401 19160272 75311230 10060A09 92268993 F22C6401 19160263
   70311030 0E060355 04031307 74657374 2D636130 1E170D31 34303732 38303332
   3231345A 170D3234 30373238 31303032 31345A30 29312730 25060355 04030C1E
   54434872 70506768 5F494E49 54494154 4F525F5F 3235365F 32303132 5F413066
   301F0608 2A850307 01010101 30130607 2A850302 02240006 082A8503 07010102
   02034300 04400B62 06DE25E6 CF34331B 24A6061B 45E4E317 DD8E786F E5FFEE1C
   EF2CEF25 1231DC29 2574703F CF38577F 07BDBD34 13FED403 838C7898 7D4DA9AC
   F4CA58D6 F633A382 01593082 01553013 0603551D 25040C30 0A06082B 06010505
   08020230 0E060355 1D0F0101 FF040403 0204F030 1D060355 1D0E0416 0414A29D
   725D9213 3AFE85FA FB9541DF 8E9940E1 1080301F 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 C22CA90E 8C38FD48 7EE2DA39 3495A16C
   C0B670DB D63F61F4 E095F249 85993869 09536735 FA41361F D1C40125 5E1E2610
   B993BB4E 39786D17 CF0926A2 FBBC6FF4 07000044 700F56A6 C3812E70 BE3BC97F
   AA0CE371 58AF97B4 2D3F36B1 268F4C3D E7DD7265 ACEF8391 D9EE8FB4 8083A675
   C77BB8FF D167BDB5 B0898FB6 CE5B5A23 1A8103D4 00000005 04
Encapsulated Initiator's Packet IKE phase 1 (5)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 05100201 00000000 00000368 00000000
   00000000 E7C94712 DAD37A46 AC0C3F68 398EA619 0DA163A6 A262473C 579CB804
   E82AEB9C 8C4F93DE 5E6534B4 95DFECBF 7DE97082 1D0E5860 F1201939 ABB38C3C
   7DC3EFFE 7487BC9D D68CA2A3 D8E5D281 BF9534B6 817A23A5 893516C2 E0E78C99
   358DBB60 1D14BD3C BE16C3C2 8DA4529F 333D99EB AF6F1C9B 0E2C340E B30CC07A
   483D85E8 00DB47BC B71B3CEA 3571EDBE 449A5078 C23CE147 85333321 4C435073
   3720BE13 3FC57C9B 075A071E 80D62B11 00947107 96B2B299 8EC960E7 9F4C879F
   9DF39B29 EBF6BE4D 5AD7212C 12A0F0BC 4D2CD5DA C9D69221 3B68200D F95A9CE9
   C5FC0265 EB4431D6 0F0B3E6A E9FA212A 09E17C22 8D91AED3 F78EAA33 F3E56E16
   08A1C99C DB3F01AB 386FCBDA 6BA4100A F2770D4F EFC5D9F9 9BC3C0E8 2C515946
   07C1FCF2 892D7781 96D78BA1 7433818D 8C845EA8 86184A25 76162C02 40EA7A4C
   6E1918F6 37267408 08CF85EB 027355C8 68FD479C 0FE06554 B14CD403 255A778F
   1BD24136 AB268BA8 5EF67311 CBC46D83 AD9DD122 17475A43 65F9D82A 0246A9AC
   0F612B30 7BB8E056 8AB9C077 2833D322 D30C3E8C A0F49AF1 00509CF9 43DB1073
   5800B070 568B8A1B 6E540EE8 6B64E11C E46A9258 6E977174 8A4A2FB5 456F93F4
   38726902 69260CCA 719C9D3E 3BDFD9BB 0FE3DF67 279B8021 57E283CD 768F8023
   0ADB3FBA 93C6D54C 552B314E 912FDEBA F332BD4D 6540FB1F F8CCB1F1 A1CEBB60
   BFC4AA64 9BFC782B 63A8D2E7 D3AFED4C 24C4140E DDE6C3CC 66DCEDC7 1A7FF692
   6F473766 893213B7 1511EA05 58DECDBA 207FA25A 0E71E2E5 B8D861E4 CDC14CA0
   0B2D8497 58F3DDA8 742EB496 9E895330 9A66201F 6FBC54FB D38D81EE 723692ED
   245BC346 96280984 7C2263E3 AF22FEB5 E108C2C8 CE023CFB FD3CAA5E B02FFD8D
   8E811B53 1D350382 957105EA 883CF183 7217A512 BC954550 54C1FF43 567DA17D
   B00DAF7D 6E281E8C B69970E3 7D2837A2 8CC26BF4 5694B4EE DD24A30F 97C09860
```

```
   814FDE94 348F2EC1 2C47C37C FC5F1F4C E664ACB9 D358054F A85E75F2 BD03B7DD
   215BB04C 2A3A9595 78E32A77 1F051D7E 282745D6 099E0FE0 A6E65D0E A90DA2C7
   8C44EEA0 4402713D 7CA002EF C13DD578 B4193444 76234827 ED378F02 FAB338AC
   E8D76D74 AB7C1D4D 07DD7760 3AB1C5C4 5E23E46D 50972F8F 2773F9B0 C70A94F4
   83DE72A2 8C2CBE45

Responder Internals:
k_r
   775A60CB 946DC613 575169D6 D2515C12 80CAACAF 0744DAEE C6EBAA4C 3C2DD27C
Responder's Signature Public Key Blob
   06200000 492E0000 4D414731 00020000 30130607 2A850302 02240106 082A8503
   07010102 028AFA89 A2ED3EE5 D9D104AC D76DCF44 7FE54E2B 244B8176 D94C554E
   69D1EDFD 0BD2E222 C96C09E2 C1B2B35F 1008BC26 18750781 A787D4F5 19044064
   4ED16D3A 3B
CERT_R
   04308202 B8308202 67A00302 0102020A 50CAAC38 000000B0 A8063008 06062A85
   03020203 303A3112 3010060A 09922689 93F22C64 01191602 72753112 3010060A
   09922689 93F22C64 01191602 63703110 300E0603 55040313 07746573 742D6361
   301E170D 31343037 32383033 32323230 5A170D32 34303732 38313030 3232305A
   30293127 30250603 5504030C 1E544348 72705067 685F5245 53504F4E 4445525F
   5F323536 5F323031 325F4230 66301F06 082A8503 07010101 01301306 072A8503
   02022401 06082A85 03070101 02020343 0004408A FA89A2ED 3EE5D9D1 04ACD76D
   CF447FE5 4E2B244B 8176D94C 554E69D1 EDFD0BD2 E222C96C 09E2C1B2 B35F1008
   BC261875 0781A787 D4F51904 40644ED1 6D3A3BA3 82015930 82015530 13060355
   1D25040C 300A0608 2B060105 05080202 300E0603 551D0F01 01FF0404 030204F0
   301D0603 551D0E04 160414AC BF2A73B5 FCE5930F 1F8A9D58 AB215C13 2E37DC30
   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 00B2F68A
   6376D489 D49837BE 414BF4D9 0DD68BB9 956D821A B32C0344 5888860C 2F1C19B2
   363E7689 28F3CD99 6E43E30C 648981B3 9C94E11B 348B1285 20AAF237 10
ID_ir
   09000000 30293127 30250603 55040313 1E544348 72705067 685F5245 53504F4E
   4445525F 5F323536 5F323031 325F42
akey
   56CED698 2218C189 69757071 90671857 5229104C 12BA7D1D 9FC48552 D894916F
SKEYID
   A56DFC7F F22A837E 6DB897FE 8718216C 4C18BE4A 6736F3EA 98908545 3AD61180
SKEYID_d
   6DC370CE 1C367C10 CB9F07D5 D04F9985 7E38A6A8 0BCFBF27 870D2417 E8224B79
SKEYID_a
   491374E5 0853B8AF 3938DEF1 18BB2476 04FE52BA 399A7284 11399CD3 A1F98CC7
SKEYID_e
   17141F4E C23F5340 81481FCE 99304091 325FFDC9 8D6F286F 5E60ECE1 A131F480
SK_e
   A9282E05 618D3F29 A8EFCDF8 C02F5C31 1D88F679 E72EA894 10C4E7BA 9D44B63A
```

```
SK_a
   A9282E05 618D3F29 A8EFCDF8 C02F5C31 1D88F679 E72EA894 10C4E7BA 9D44B63A
IV
   47A68CF4 F8830640
HASH_R
   EF7146E8 F9AB4697 83C88050 9D5B886F E6BA28E4 E0DBDCDC 1B683F16 7B04E957
SIG_R
   19ADC242 3D1FCF1C 7BFDCFDB 799D3D3C FB178CB4 F8836C27 947DC984 6CC0F2D7
   41140A25 3335FF04 19787A65 023A4D3F 4A669287 A9F52A3A C5B2289A 502C250A
AUTH_R
   93DC145C 615F15A2 FEC9A769 8CD0DF97 93EB1DE8 C17D701E 473CDF59 C725CFFA

Initiator <- Responder

Responder's Packet IKE phase 1 (6)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   05100201
Message ID
   00000000
Length
   00000368
Identification
   06000033
   09000000 30293127 30250603 55040313 1E544348 72705067 685F5245 53504F4E
   4445525F 5F323536 5F323031 325F42
Certificate
   090002C1
   04308202 B8308202 67A00302 0102020A 50CAAC38 000000B0 A8063008 06062A85
   03020203 303A3112 3010060A 09922689 93F22C64 01191602 72753112 3010060A
   09922689 93F22C64 01191602 63703110 300E0603 55040313 07746573 742D6361
   301E170D 31343037 32383033 32323230 5A170D32 34303732 38313030 3232305A
   30293127 30250603 5504030C 1E544348 72705067 685F5245 53504F4E 4445525F
   5F323536 5F323031 325F4230 66301F06 082A8503 07010101 01301306 072A8503
   02022401 06082A85 03070101 02020343 0004408A FA89A2ED 3EE5D9D1 04ACD76D
   CF447FE5 4E2B244B 8176D94C 554E69D1 EDFD0BD2 E222C96C 09E2C1B2 B35F1008
   BC261875 0781A787 D4F51904 40644ED1 6D3A3BA3 82015930 82015530 13060355
   1D25040C 300A0608 2B060105 05080202 300E0603 551D0F01 01FF0404 030204F0
   301D0603 551D0E04 160414AC BF2A73B5 FCE5930F 1F8A9D58 AB215C13 2E37DC30
   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 00B2F68A
   6376D489 D49837BE 414BF4D9 0DD68BB9 956D821A B32C0344 5888860C 2F1C19B2
```

```
   363E7689 28F3CD99 6E43E30C 648981B3 9C94E11B 348B1285 20AAF237 10
Signature
   00000044
   19ADC242 3D1FCF1C 7BFDCFDB 799D3D3C FB178CB4 F8836C27 947DC984 6CC0F2D7
   41140A25 3335FF04 19787A65 023A4D3F 4A669287 A9F52A3A C5B2289A 502C250A
Responder's Packet IKE phase 1 (6)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 05100201 00000000 00000368 06000033
   09000000 30293127 30250603 55040313 1E544348 72705067 685F5245 53504F4E
   4445525F 5F323536 5F323031 325F4209 0002C104 308202B8 30820267 A0030201
   02020A50 CAAC3800 0000B0A8 06300806 062A8503 02020330 3A311230 10060A09
   92268993 F22C6401 19160272 75311230 10060A09 92268993 F22C6401 19160263
   70311030 0E060355 04031307 74657374 2D636130 1E170D31 34303732 38303332
   3232305A 170D3234 30373238 31303032 32305A30 29312730 25060355 04030C1E
   54434872 70506768 5F524553 504F4E44 45525F5F 3235365F 32303132 5F423066
   301F0608 2A850307 01010101 30130607 2A850302 02240106 082A8503 07010102
   02034300 04408AFA 89A2ED3E E5D9D104 ACD76DCF 447FE54E 2B244B81 76D94C55
   4E69D1ED FD0BD2E2 22C96C09 E2C1B2B3 5F1008BC 26187507 81A787D4 F5190440
   644ED16D 3A3BA382 01593082 01553013 0603551D 25040C30 0A06082B 06010505
   08020230 0E060355 1D0F0101 FF040403 0204F030 1D060355 1D0E0416 0414ACBF
   2A73B5FC E5930F1F 8A9D58AB 215C132E 37DC301F 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 B2F68A63 76D489D4 9837BE41 4BF4D90D
   D68BB995 6D821AB3 2C034458 88860C2F 1C19B236 3E768928 F3CD996E 43E30C64
   8981B39C 94E11B34 8B128520 AAF23710 00000044 19ADC242 3D1FCF1C 7BFDCFDB
   799D3D3C FB178CB4 F8836C27 947DC984 6CC0F2D7 41140A25 3335FF04 19787A65
   023A4D3F 4A669287 A9F52A3A C5B2289A 502C250A
Encapsulated Responder's Packet IKE phase 1 (6)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 05100201 00000000 00000368 00000000
   00000000 E95B9E7C BB229C7E 9775CA3A EB1302E4 F639C9A7 1FA04151 905CBDD0
   47E6712F 64D5CAA6 CBA4139A 5980F51F 033E9A98 B0755BE7 280FD731 B77301E5
   7EB5F8E5 78E27B75 27FE12F1 ED2A6AF3 62F32E20 2180BAEE 4A6D48CC 8BF35ED5
   39A3540C 5709CDE3 5351FEC9 9ADC1B80 B414B410 89D86311 C53DBAD7 6D492B5C
   4F5515F3 85BC7C5F 86DEF1DD 66718838 CAE5A13F 10E4733B 8815DD14 C764F7CB
   3D67B497 797157C2 18F4D461 5ABEB97B 40C5B536 DC642B47 7D3894EA 7D8AA9BB
   3E733B7E 8FA100F1 FB4B9582 162EBA78 3F2B81C3 4C0D33F2 218155FE 89F9BC0F
   4ED608D8 4EDC543F 570B0A6A 2020D9EE B8C04BBD 969AB2A5 14741EB2 ED1332A4
   648BBFB8 43B1B394 E6B459FB 7847E07E D0DF5F58 0F47335F B668C511 62E5BADF
   DBFA5518 F338DB27 62D32824 85068380 F54BC8BC B3254678 33F8D0FA 396EC67C
   C10635DF 3DE544BF AE33EF4F F97977E0 13813FFA E6F854F2 269154C8 C718490A
   E072B444 AFABF015 0AD3E800 2FA2031B E1862806 63C18657 993D384B 6758FEE4
   73FB1B9E 446A8AAF 95BA7136 044FEA86 A799354B F183741D F3C4B46E DF5C9E34
   8744D561 4BF85BBF 6F9BE6B7 F57E42F6 A527A773 E4E60864 8DAF9F23 FCB44280
   365A6104 BAC7CF8B E46862C0 C76C5795 7924041E 94D5B896 F3662540 7CB52608
   B41CDD14 3B3ADDAE EA30EA2B 5881B6E5 33513BB4 42053E48 BBBF771F 29F24882
   BAFE7D89 64C3A952 E4EDD266 5A839F29 CE03C05E 9A7D1CCF 34BEEA91 E4C8BF63
```

```
   3AD13BFF 0C7908D3 3EA4AB51 3647B7D5 51F23B9D 34F5F304 670BCC3D F9B44C2F
   C7859F7C 91BD47DD A8ECBD78 72318372 200F1C8D 21303F03 E7DD8F5A 277F4858
   CA5E5C1C 469ECE7A BD634704 515F049A F9A9F15C A2DC179D DDA2C703 486D4FBF
   8429BBAF 68D31408 C80ACAF9 B7769BBB 47054D63 C649C957 166115F3 9D6C81FF
   B3A249FB 40A156D9 53040979 EC693E43 0DABCC74 ADB50340 93C5A685 D06FDADC
   351B797A 1AF32378 18C280B5 E8757623 45592896 BE39E45E 9AC61E96 346210CA
   DE51F577 A1E1F4B2 8297C239 1ABB88EE C4AECFFB 0A852F77 5D1E240F 04A87E47
   95E4922B 27A1B4D3 82F81FCD FD0C5BC4 3AAC12A4 D54590D9 82EB006E B9AB9E48
   B67BD8CB 093A1EF1 85F26B10 AC297BE7 99119217 FDF04DA1 EA251799 16800B03
   AD4B1FBE D3C750A9

IKE phase2 Quick Mode PFS

Initiator Internals:
Message ID
   D365300E
Message Nonce
   E3025E8D 0E793B7E
SPI
   7BA7FFF9
Transform ID
   FC000000
SA
   00000001 00000001 00000020 01030401 7BA7FFF9 00000014 01FC0000 80040002
   FE91FF7F 8003FFF4
Ni_b
   7476FB2E 752035BD EA155FD7 5CAD9694
ID_ci
   01010000 C0000201
x_i
   8678FBC9 BCFE0B28 023B74F2 0D691D80 70E93056 CC062708 476BB70C 75C334BD
KE_i
   64B74E14 34343D57 FECACD45 DA6E7988 6D9944FB E9E64C3F 08AD0A64 0A9B4052
   138B34DC E296A2A2 1AECA5B6 1FB80E03 3457ECD6 8F591419 1D464E17 51D7907D
gm_ir
   9D1F90C1 084D37B1 0F92350C F7BEF6AD D7AFDE89 5F2B5560 FD5B2344 973EFFCF
SK_e
   2F3114D1 C7603A07 14241AEF 5414D8CB 212DCD07 BB67B366 579A5602 1D64A4F3
SK_a
   2F3114D1 C7603A07 14241AEF 5414D8CB 212DCD07 BB67B366 579A5602 1D64A4F3
IV
   1CAB3552 C0E16A57
HASH(1)
   8B056020 DF086AC9 591FE11C E07308BD 7F1A9045 9BDA6C0F DEA6B7E3 8A9FACBC

Initiator -> Responder

Initiator's Packet IKE phase 2 (1)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
```

```
Flags
   08102001
Message ID
   D365300E
Length
   000000F0
Hash
   01000024
   8B056020 DF086AC9 591FE11C E07308BD 7F1A9045 9BDA6C0F DEA6B7E3 8A9FACBC
Security Association
   0A00002C
   00000001 00000001 00000020 01030401 7BA7FFF9 00000014 01FC0000 80040002
   FE91FF7F 8003FFF4
Nonce
   04000014
   7476FB2E 752035BD EA155FD7 5CAD9694
Key exchange
   05000044
   64B74E14 34343D57 FECACD45 DA6E7988 6D9944FB E9E64C3F 08AD0A64 0A9B4052
   138B34DC E296A2A2 1AECA5B6 1FB80E03 3457ECD6 8F591419 1D464E17 51D7907D
Identification
   0500000C
   01010000 C0000201
Identification
   0000000C
   01010000 C0000221
Initiator's Packet IKE phase 2 (1)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 08102001 D365300E 000000F0 01000024
   8B056020 DF086AC9 591FE11C E07308BD 7F1A9045 9BDA6C0F DEA6B7E3 8A9FACBC
   0A00002C 00000001 00000001 00000020 01030401 7BA7FFF9 00000014 01FC0000
   80040002 FE91FF7F 8003FFF4 04000014 7476FB2E 752035BD EA155FD7 5CAD9694
   05000044 64B74E14 34343D57 FECACD45 DA6E7988 6D9944FB E9E64C3F 08AD0A64
   0A9B4052 138B34DC E296A2A2 1AECA5B6 1FB80E03 3457ECD6 8F591419 1D464E17
   51D7907D 0500000C 01010000 C0000201 0000000C 01010000 C0000221
Encapsulated Initiator's Packet IKE phase 2 (1)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 08102001 D365300E 000000F0 E3025E8D
   0E793B7E CA3719D7 B752B9D1 8D2D0858 BC439D70 FBCB8EAC 8F11A1F4 F4B3731A
   7DAA8944 8AD7B565 75BF7D86 4224F012 21351B60 1702F1A6 7610C13C 668056CA
   45D81B12 BD882369 4E242FEF 9F842DE6 2D016D1B 932FFAAA 9DF559FA DB0F921E
   021BEC58 BC2C2FC5 1EC20700 41AE1339 4D7929D8 E9914717 09FBF91E 62308EFF
   11F3AB81 887C9256 C35913E0 AC13E620 85BB02BC D9A5E266 A616C590 0023CAC2
   0EC0AA18 CF139583 527FEE43 DE2F6001 A5A8CC1F FFD2B3C8 A4EFAACE 10A3B654
   03535A9A 8FDBFCDE EEA80924 E450B24B

Responder Internals:
SPI
   8FC608BE
Transform ID
   FC000000
SA
   00000001 00000001 00000020 01030401 8FC608BE 00000014 01FC0000 80040002
   FE91FF7F 8003FFF4
```

```
Nr_b
   3BB6BA29 EAF2E524 04A59A03 2ACA322D
ID_cr
   01010000 C0000221
x_r
   46BA43F8 DF4D6EF4 9C0B3A7F C35772A8 45C95AE3 27C707FD A35A99DE 115E1A48
KE_r
   166BE737 CD8C246F 841A8868 EC192B04 EB8AF993 CB5C9CAF BA765A89 9B226C5A
   1D1A4953 1340D4C9 7EBB4E6C 782A26DD 269741CC 8739789D 58DC49F5 B622463D
gm_ir
   9D1F90C1 084D37B1 0F92350C F7BEF6AD D7AFDE89 5F2B5560 FD5B2344 973EFFCF
SK_e
   2F3114D1 C7603A07 14241AEF 5414D8CB 212DCD07 BB67B366 579A5602 1D64A4F3
SK_a
   2F3114D1 C7603A07 14241AEF 5414D8CB 212DCD07 BB67B366 579A5602 1D64A4F3
IV
   1CAB3552 C0E16A57
HASH(2)
   E950FA03 C7ED033B 8D13D6E4 DE38389F 9BEA3696 AC0EA35A 08B85CD7 0407A5E2

Initiator <- Responder

Responder's Packet IKE phase 2 (2)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   08102001
Message ID
   D365300E
Length
   000000F0
Hash
   01000024
   E950FA03 C7ED033B 8D13D6E4 DE38389F 9BEA3696 AC0EA35A 08B85CD7 0407A5E2
Security Association
   0A00002C
   00000001 00000001 00000020 01030401 8FC608BE 00000014 01FC0000 80040002
   FE91FF7F 8003FFF4
Nonce
   04000014
   3BB6BA29 EAF2E524 04A59A03 2ACA322D
Key exchange
   05000044
   166BE737 CD8C246F 841A8868 EC192B04 EB8AF993 CB5C9CAF BA765A89 9B226C5A
   1D1A4953 1340D4C9 7EBB4E6C 782A26DD 269741CC 8739789D 58DC49F5 B622463D
Identification
   0500000C
   01010000 C0000201
Identification
   0000000C
```

```
   01010000 C0000221
Responder's Packet IKE phase 2 (2)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 08102001 D365300E 000000F0 01000024
   E950FA03 C7ED033B 8D13D6E4 DE38389F 9BEA3696 AC0EA35A 08B85CD7 0407A5E2
   0A00002C 00000001 00000001 00000020 01030401 8FC608BE 00000014 01FC0000
   80040002 FE91FF7F 8003FFF4 04000014 3BB6BA29 EAF2E524 04A59A03 2ACA322D
   05000044 166BE737 CD8C246F 841A8868 EC192B04 EB8AF993 CB5C9CAF BA765A89
   9B226C5A 1D1A4953 1340D4C9 7EBB4E6C 782A26DD 269741CC 8739789D 58DC49F5
   B622463D 0500000C 01010000 C0000201 0000000C 01010000 C0000221
Encapsulated Responder's Packet IKE phase 2 (2)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 08102001 D365300E 000000F0 E3025E8D
   0E793B7E 878980B9 06242ECC 30B79255 0018D648 2D7CF5D8 47345DAE E0246B7C
   BCF2F42D EF140FD7 139407FC 4AD10D20 D9262348 1E5A976B A51E7654 253AA1F8
   350A66C3 5C0333D6 F76C2447 78928719 BF5CDAD7 666F844B 569BD5E3 91339E2B
   9332CDF6 38E4866D BFEAE92D 8CD2B695 17E7919E 8674F86D F194EE4D 74B9EFC5
   967109EE 983D35A4 29541C22 F7818D5E 33E504F1 FA712403 607CAA07 6F955969
   809BDCD1 AC203C4F C2F5666D 32AAE5E4 A7A21B53 17FDEBE0 C72ABE78 B02191FF
   18A03B66 37992414 F5F18AF6 B5F58D95

Initiator Internals:
HASH(3)
   4270A809 137396BF 6F438275 B659CF69 34011D9C AB871AB5 310673CD 2A3EAD40

Initiator -> Responder

Initiator's Packet IKE phase 2 (3)
CKY-I
   55D5D33D 9B0BC56C
CKY-R
   CFA1A8D3 D2AF5BEB
Flags
   08102001
Message ID
   D365300E
Length
   00000050
Hash
   00000024
   4270A809 137396BF 6F438275 B659CF69 34011D9C AB871AB5 310673CD 2A3EAD40
Initiator's Packet IKE phase 2 (3)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 08102001 D365300E 00000050 00000024
   4270A809 137396BF 6F438275 B659CF69 34011D9C AB871AB5 310673CD 2A3EAD40
Encapsulated Initiator's Packet IKE phase 2 (3)
   55D5D33D 9B0BC56C CFA1A8D3 D2AF5BEB 08102001 D365300E 00000050 E3025E8D
   0E793B7E 5A4B4A68 3DF4A173 A7440CA5 D7F44C4E 2FB6797B F8F92705 E7E2E390
   5F8491C5 52FD992A D1EFEADB 3452D24E

TRANSFORM_ID=CPESP_GOST_1K_IMIT

Initiator's inbound SA
KEYMAT
   97CCD843 E277A315 A203AA1D AB0C5FE8 49C7EEE3 50AD564D 214CDF8B DB1B58E2
```

```
   C46D2663 16889523 50232B88 4429162B D0974000 1D346FA3 C6F5884A 14DAFFF0
   CDDC284A

Initiator's outbound SA
KEYMAT
   211A76B0 662213FD 2A0C7C95 459CA430 5440A3DA 5406470A CD640FA0 15EA5AFA
   EF9DDE8E 4007ED8E 3A25E861 36DEECB5 BE39FFEE FBD42465 8982CDC1 234F4817
   7A8D34FF

Responder's inbound SA
KEYMAT
   211A76B0 662213FD 2A0C7C95 459CA430 5440A3DA 5406470A CD640FA0 15EA5AFA
   EF9DDE8E 4007ED8E 3A25E861 36DEECB5 BE39FFEE FBD42465 8982CDC1 234F4817
   7A8D34FF

Responder's outbound SA
KEYMAT
   97CCD843 E277A315 A203AA1D AB0C5FE8 49C7EEE3 50AD564D 214CDF8B DB1B58E2
   C46D2663 16889523 50232B88 4429162B D0974000 1D346FA3 C6F5884A 14DAFFF0
   CDDC284A
```