ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.004 – 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Схемы выработки общего ключа с аутентификацией на основе открытого ключа

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 РАЗРАБОТАНЫ Центром защиты информации и специальной связи ФСБ России с участием ОАО «Информационные технологии и коммуникационные системы»

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2017 г. № 1505-ст

3 ВВЕДЕНЫ ВПЕРВЫЕ

Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru).

Содержание

Введение

Средства защиты информации, в ряде случаев, реализуют протоколы аутентификации и выработки общего ключа для выполнения своих целевых функций. Реализация таких протоколов может базироваться на безопасных схемах выработки общего ключа с аутентификацией на основе открытого ключа.

Настоящие рекомендации определяют схемы выработки общего ключа с аутентификацией на основе открытого ключа с использованием криптографических алгоритмов, определенных национальными стандартами в области криптографической защиты информации.

Необходимость разработки настоящих рекомендаций вызвана потребностью в формировании единого подхода к реализации используемых в разрабатываемых и модернизируемых средствах защиты информации схем выработки общего ключа с аутентификацией на основе открытого ключа с использованием криптографических алгоритмов, определенных национальными стандартами.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Схемы выработки общего ключа с аутентификацией на основе открытого ключа

Дата введения 2018 — 04 — 01

1 Область применения

Настоящие рекомендации определяют схемы выработки общего ключа с аутентификацией на основе открытого ключа с использованием криптографических алгоритмов, определенных национальными стандартами, и могут быть использованы при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты и рекомендации по стандартизации:

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11–2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

Р 50.1.113-2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Примечание – При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов (рекомендаций) в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт (рекомендации), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (рекомендаций) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (рекомендации), на который дана датированная ссылка, то рекомендуется использовать версию

этого стандарта (рекомендаций) с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт (рекомендации), на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт (рекомендации) отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящих рекомендациях применены следующие термины в соответствии со следующими определениями:

3.1.1 **ключ:** Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

3.1.2 **ключ подписи:** Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи.

3.1.3 **ключ проверки подписи:** Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

3.1.4 **сертификат ключа проверки:** Элемент данных, подтверждающий принадлежность ключа проверки владельцу сертификата ключа проверки.

3.1.5 **код аутентификации сообщения:** Строка бит фиксированной длины, добавляемая к сообщению для обеспечения его целостности и аутентификации источника данных.

3.2 Обозначения

В настоящих рекомендациях используют следующие обозначения:

V^* — множество всех двоичных строк конечной длины, включая пустую строку;

$A||B$ — конкатенация строк A, $B \in V^*$, т.е. строка из $V_{|A|+|B|}$, в которой подстрока с большими номерами компонент из $V_{|A|}$ совпадает со строкой A, а подстрока с меньшими номерами компонент из $V_{|B|}$ совпадает со строкой B;

$[T]_{i,j}$ — для битовой строки $T=(t_0, \dots, t_n)$ подстрока $T`=(t_i, \dots, t_j), 0 \le i \le j \le n$;

$H_{512}(T)$ — значение функции хэширования с длинной хэш-кода 512 бит, определенной ГОСТ Р 34.11-2012, для сообщения T;

$SGN_d(T)$ — цифровая подпись, сформированная в соответствии с ГОСТ Р 34.10-2012, для сообщения T с использованием ключа подписи d;

$VERIFY_D(T,S)$ — результат проверки цифровой подписи S согласно ГОСТ Р 34.10-2012 для сообщения T с использованием ключа проверки подписи D;

$MAC_k(T)$ — результат вычисления кода аутентификации для сообщения *T* с использованием ключа k;

$KDF_{512}(T)$: $V^* \to V_{512}$ — функция вычисления производного ключа длины 512 на основе входного значения *T*;

$\pi(Q)$ — функция, отображающая точку эллиптической кривой в битовую строку;

$\langle\cdot\rangle$ — опциональный параметр схемы (может являться строкой нулевой длины);

h_2, h_3 — фиксированные различные строки ненулевой длины, определяемые для каждой реализации протокола;

s_A, S_A — соответственно долговременные ключ подписи и ключ проверки подписи стороны *A*;

k_A, K_A — соответственно сеансовые (эфемерные) ключ подписи и ключ проверки подписи стороны *A*;

Id_A — идентификатор стороны *A*;

$Cert_A$ — сертификат долговременного ключа проверки подписи стороны *A*;

$\mathcal{O}$ — нулевая точка эллиптической кривой.

4 Общие положения

Настоящие рекомендации определяют три схемы выработки общего ключа с аутентификацией на основе открытого ключа:

1 Эхинацея-3 (Э-3) - схема выработки общего ключа с двусторонней аутентификацией при помощи ключа подписи.

2 Эхинацея-2 (Э-2) - схемы выработки общего ключа с односторонней аутентификацией при помощи ключа подписи.

3 Лимонник-3 (Л-3) - схема выработки общего ключа с возможностью использования двух различных эллиптических кривых и с двусторонней аутентификацией при помощи ключа схемы Диффи-Хеллмана.

4.1 Эллиптические кривые

Предполагается использование операций в группе точек эллиптической кривой E над конечным простым полем характеристики p, заданной в форме Вейерштрасса - $\mathrm{E_{W,a,b}}\big(\mathrm{GF(p)}\big) = \{(\mathrm{x,y}): \mathrm{x^2} \equiv \mathrm{x^3 + ax + b (mod\ p)}\}$ или в форме Эдвардса $\overline{\mathrm{E}}_{\mathrm{Edw,e,d}}\big(\mathrm{GF(p)}\big) = \{(\mathrm{u,v}): \mathrm{eu^2 + v^2} \equiv 1 + \mathrm{du^2v^2 (mod\ p)}\}$. Для обозначения параметров эллиптической кривой E в форме Вейерштрасса будет использоваться обозначение $\big(\mathrm{p, a, b, m, q, x_p, y_p}\big)$ согласно ГОСТ Р 34.10-2012, а для эллиптической кривой в форме Эдвардса - обозначение $\big(\mathrm{p, a, b, m, q, x_p, y_p, e, d, u_p, v_p}\big)$ согласно [1].

Используемые эллиптические кривые должны удовлетворять требованиям ГОСТ Р 34.10-2012 при $2^{508} < q < 2^{512}$. Допускается использование эллиптических кривых и в других представлениях, при этом, эквивалентное представление кривой в форме Вейерштрасса должно удовлетворять требованиям ГОСТ Р 34.10-2012 при $2^{508} < q < 2^{512}$.

4.2 Код аутентификации сообщения

Для вычисления кода аутентификации сообщения могут использоваться:

1 Алгоритм блочного шифрования с длиной блока 128 бит («Кузнечик») согласно ГОСТ Р 34.12-2015 в режиме выработки имитовставки согласно ГОСТ Р 34.13-2015.

2 Функция $\mathrm{HMAC\_GOSTR3411\_2012\_512}$, определенная в Р 50.1.113-2016.

4.2 Вычисление производного ключа

В качестве функции вычисления производного ключа $\mathrm{KDF}_{512}(\mathrm{T}):\mathrm{V}^{*}\rightarrow\mathrm{V}_{512}$ могут использоваться:

1 Функция хэширования, определенная согласно ГОСТ Р 34.10-2012 с длиной хэш-кода 512 бит.

2 Псевдослучайная функция $\mathrm{PRF\_TLS\_GOSTR3411\_2012\_512}$ с длиной выхода 512 бит, определенная в Р 50.1.113-2016.

4.3 Способ вычисления функции $\pi(Q)$

В случае использования кривой в форме Вейерштрасса для $Q=(\mathrm{x}_Q,\mathrm{y}_Q)$ выполняется $\pi(Q)=\mathrm{x}_Q$.

В случае использования кривой в форме Эдвардса для $Q=(\mathrm{u}_Q,\mathrm{v}_Q)$ выполняется $\pi(Q)=\mathrm{u}_Q$.

5 Схема выработки общего ключа с аутентификацией «Эхинацея-3»

Долговременными ключами сторон A и B являются ключи цифровой подписи $\mathrm{s_A},\mathrm{S_A}$ и $\mathrm{s_B},\mathrm{S_B}$ соответственно, определенные согласно разделу 5.2 ГОСТ Р 34.10-2012, и удостоверенные сертификатами ключа проверки $\mathrm{Cert_A}$ и $\mathrm{Cert_B}$.

Сторона A имеет $(\mathrm{Id_A},\langle\mathrm{K}\rangle)$, сторона B имеет $(\mathrm{Id_B},\langle\mathrm{K}\rangle)$, где $\mathrm{K}\in\mathrm{V}^{*}$ - заранее распределенное общее секретное значение.

Параметры эллиптической кривой считаются известными обеим сторонам и согласованными до начала протокола.

Предполагается, что выработка общего ключа и аутентификация осуществляются в рамках сеанса связи, с которым может быть ассоциирована доступная обеим сторонам открытая общая информация OI.

Схема выработки общего ключа с аутентификацией «Эхинацея-3» состоит из следующей последовательности действий.

1 Сторона A случайным образом выбирает $\mathrm{k_A}$, где $\mathrm{k_A}\in\{1,\dots,\mathrm{q}-1\}$, и вычисляет точку эллиптической кривой $\mathrm{K_A}=\mathrm{k_A}\mathrm{P}$.

2 Сторона A посылает стороне B - $(\mathrm{Id_A},\mathrm{Cert_A},\mathrm{K_A})$.

3 Сторона B проверяет валидность сертификата ключа проверки $\mathrm{Cert_A}$. Если это условие не выполнено, то сторона B завершает протокол, возвращая ошибку стороне A, информирующую о невалидности сертификата ключа проверки $\mathrm{Cert_A}$.

4 Сторона B проверяет, что $K_A \in E$ и $\frac{m}{q}K_A \neq \mathcal{O}$. Если это условие не выполнено, то сторона B завершает протокол, возвращая ошибку стороне A, информирующую о неверном выборе параметров.

5 Сторона B случайным образом выбирает k_B, где $k_B \in \{1, \dots, q-1\}$, и вычисляет точку эллиптической кривой $K_B = k_B P$.

6 Сторона B вычисляет точку $Q_{AB} = (m/q) \cdot k_B K_A$.

7 Сторона B вычисляет значение $T_{AB} = KDF(\pi(Q_{AB})||Id_A||Id_B\langle||OI\rangle\langle||K\rangle)$.

8 Сторона B вычисляет общие сеансовые ключи $K_{AB} = [T_{AB}]_{0,255}$ и $M_{AB} = [T_{AB}]_{256,511}$.

9 Сторона B вычисляет метку аутентификации $aut_B = SGN_{s_B}(\pi(K_B)||\pi(K_A)||Id_A)$ и метку подтверждения ключа $tag_B = MAC_{M_{AB}}(h_2||\pi(K_B)||\pi(K_A)||Id_B||Id_A)$.

10 Сторона B посылает стороне A - $(Id_B, Cert_B, K_B, aut_B, tag_B)$.

11 Сторона A проверяет валидность сертификата ключа проверки $Cert_B$. Если это условие не выполнено, то сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невалидности сертификата ключа проверки $Cert_B$.

12 Сторона A проверяет цифровую подпись $VERIFY_{S_B}(\pi(K_B)||\pi(K_A)||Id_A, aut_B)$= «верно». Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невозможности аутентификации.

13 Сторона A проверяет, что $K_B \in E$ и $\frac{m}{q}K_B \neq \mathcal{O}$. Если это условие не выполнено, то сторона A завершает протокол, возвращая ошибку стороне B, информирующую о неверном выборе параметров.

14 Сторона A вычисляет точку $Q_{BA} = (m/q) \cdot k_A K_B$.

15 Сторона A вычисляет значение $T_{BA} = KDF(\pi(Q_{BA})||Id_A||Id_B\langle||OI\rangle\langle||K\rangle)$.

16 Сторона A вычисляет общие сеансовые ключи $K_{BA} = [T_{BA}]_{0,255}$ и $M_{BA} = [T_{BA}]_{256,511}$.

17 Сторона A вычисляет метку подтверждения ключа $tag`_B = MAC_{M_{BA}}(h_2||\pi(K_B)||\pi(K_A)||Id_B||Id_A)$ и проверяет $tag_B = tag`_B$. Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невозможности аутентификации.

18 Сторона A вычисляет метку аутентификации $aut_A = SGN_{s_A}(\pi(K_A)||\pi(K_B)||Id_B)$ и метку подтверждения ключа $tag_A = MAC_{M_{BA}}(h_3||\pi(K_A)||\pi(K_B)||Id_A||Id_B)$.

19 Сторона A посылает стороне B - (aut_A, tag_A).

20 Сторона B проверяет цифровую подпись $VERIFY_{S_A}(\pi(K_A)||\pi(K_B)||Id_B, aut_A)$= «верно». Если это условие не выполнено, сторона B завершает протокол, возвращая ошибку стороне A, информирующую о невозможности аутентификации.

21 Сторона B вычисляет метку подтверждения ключа $tag`_A = MAC_{M_{AB}}(h_3||\pi(K_A)||\pi(K_B)||Id_A||Id_B)$ и проверяет $tag_A = tag`_A$. Если это условие не выполнено, сторона B завершает протокол, возвращая ошибку стороне A, информирующую о невозможности аутентификации.

22 Стороны A и B уничтожают ключи M_{BA} и M_{AB} соответственно.

Стороны A и B находятся в состоянии проведенной аутентификации с выработанным общим ключом $\overline{K} = K_{BA} = K_{AB}$.

6 Схема выработки общего ключа с аутентификацией «Эхинацея-2»

Сторона B обладает долговременными ключами цифровой подписи s_B, S_B, определенными согласно ГОСТ Р 34.10-2012 (пункт 5.2), и удостоверенными сертификатом ключа проверки $Cert_B$.

Сторона A имеет $(Id_A, \langle K \rangle)$, сторона B имеет $(Id_B, \langle K \rangle)$, где $K \in V^*$ - заранее распределенное общее секретное значение.

Параметры эллиптической кривой считаются известными обеим сторонам и согласованными до начала протокола.

Предполагается, что выработка общего ключа и аутентификация осуществляются в рамках сеанса связи, с которым может быть ассоциирована доступная обеим сторонам открытая общая информация OI.

Схема выработки общего ключа с односторонней аутентификацией «Эхинацея-2» состоит из следующей последовательности действий.

1 Сторона A случайным образом выбирает k_A, где $k_A \in \{1, \dots, q-1\}$, и вычисляет точку эллиптической кривой $K_A = k_A P$.

2 Сторона A посылает стороне B - (Id_A, K_A).

3 Сторона B проверяет, что $K_A \in E$ и $\frac{m}{q} K_A \neq \mathcal{O}$. Если это условие не выполнено, то сторона B завершает протокол, возвращая ошибку стороне A, информирующую о неверном выборе параметров.

4 Сторона B случайным образом выбирает k_B, где $k_B \in \{1, \dots, q-1\}$, и вычисляет точку эллиптической кривой $K_B = k_B P$.

5 Сторона B вычисляет точку $Q_{AB} = (m/q) \cdot k_B K_A$.

6 Сторона B вычисляет значение $T_{AB} = KDF(\pi(Q_{AB}) || Id_A || Id_B \langle || OI \rangle \langle || K \rangle)$.

7 Сторона B вычисляет общие сеансовые ключи $K_{AB} = [T_{AB}]_{0,255}$ и $M_{AB} = [T_{AB}]_{256,511}$.

8 Сторона B вычисляет метку аутентификации $aut_B = SGN_{s_B}(\pi(K_B) || \pi(K_A) || Id_A)$ и метку подтверждения ключа $tag_B = MAC_{M_{AB}}(h_2 || \pi(K_B) || \pi(K_A) || Id_B || Id_A)$.

9 Сторона B посылает стороне A - $(Id_B, Cert_B, K_B, aut_B, tag_B)$.

10 Сторона A проверяет валидность сертификата ключа проверки $Cert_B$. Если это условие не выполнено, то сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невалидности сертификата ключа проверки $Cert_B$.

11 Сторона A проверяет цифровую подпись $VERIFY_{S_B}(\pi(K_B) || \pi(K_A) || Id_A, aut_B)$= «верно». Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невозможности аутентификации.

12 Сторона A проверяет, что $K_B \in E$ и $\frac{m}{q} K_B \neq \mathcal{O}$. Если это условие не выполнено, то сторона A завершает протокол, возвращая ошибку стороне B, информирующую о неверном выборе параметров.

14 Сторона A вычисляет точку $Q_{BA} = (m/q) \cdot k_A K_B$.

14 Сторона A вычисляет значение $T_{BA} = KDF(\pi(Q_{BA}) || Id_A || Id_B \langle || OI \rangle \langle || K \rangle)$.

15 Сторона A вычисляет общие сеансовые ключи $K_{BA} = [T_{BA}]_{0,255}$ и $M_{BA} = [T_{BA}]_{256,511}$.

16 Сторона A вычисляет метку подтверждения ключа $\mathrm{tag`_B} = \mathrm{MAC_{M_{BA}}}(\mathrm{h_2}||\pi(\mathrm{K_B})||\pi(\mathrm{K_A})||\mathrm{Id_B}||\mathrm{Id_A})$ и проверяет $\mathrm{tag_B} = \mathrm{tag`_B}$. Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невозможности аутентификации.

17 Сторона A вычисляет метку подтверждения ключа $\mathrm{tag_A} = \mathrm{MAC_{M_{BA}}}(\mathrm{h_3}||\pi(\mathrm{K_A})||\pi(\mathrm{K_B})||\mathrm{Id_A}||\mathrm{Id_B})$.

18 Сторона A посылает стороне B - $(\mathrm{tag_A})$.

19 Сторона B вычисляет метку подтверждения ключа $\mathrm{tag`_A} = \mathrm{MAC_{M_{AB}}}(\mathrm{h_3}||\pi(\mathrm{K_A})||\pi(\mathrm{K_B})||\mathrm{Id_A}||\mathrm{Id_B})$ и проверяет $\mathrm{tag_A} = \mathrm{tag`_A}$. Если это условие не выполнено, сторона B завершает протокол, возвращая ошибку стороне A, информирующую о невозможности аутентификации.

20 Стороны A и B уничтожают ключи $\mathrm{M_{BA}}$ и $\mathrm{M_{AB}}$ соответственно.

Стороны A и B находятся в состоянии проведенной односторонней аутентификации (B перед A) с выработанным общим ключом $\overline{\mathrm{K}} = \mathrm{K_{BA}} = \mathrm{K_{AB}}$.

7 Схема выработки общего ключа с аутентификацией «Лимонник-3»

В данной схеме допускается использование двух (возможно, различных) эллиптических кривых $\mathrm{E_A}$ и $\mathrm{E_B}$.

Долговременными ключами сторон A и B являются ключи цифровой подписи $\mathrm{s_A}, \mathrm{S_A}$ и $\mathrm{s_B}, \mathrm{S_B}$ соответственно, которые определяются соотношениями $\mathrm{S_A} = \mathrm{s_A P_A}$, $\mathrm{S_B} = \mathrm{s_B P_B}$, где $0 < \mathrm{s_A} < \mathrm{q_A}$, $0 < \mathrm{s_B} < \mathrm{q_B}$, и удостоверенные сертификатами ключей проверки $\mathrm{Cert_A}$ и $\mathrm{Cert_B}$.

Сторона A имеет $(\mathrm{Id_A}, \langle \mathrm{K} \rangle)$, сторона B имеет $(\mathrm{Id_B}, \langle \mathrm{K} \rangle)$, где $\mathrm{K} \in \mathrm{V}^*$ - заранее распределенное общее секретное значение.

Параметры эллиптических кривых $\mathrm{E_A}$ и $\mathrm{E_B}$ считаются известными обеим сторонам и согласованными до начала протокола.

Предполагается, что выработка общего ключа и аутентификация осуществляются в рамках сеанса связи, с которым может быть ассоциирована доступная обеим сторонам открытая общая информация OI.

Схема выработки общего ключа с аутентификацией «Лимонник-3» состоит из следующей последовательности действий.

1 Сторона A случайным образом выбирает $\mathrm{k_A}$, где $\mathrm{k_A} \in \{1, \dots, \mathrm{q_B} - 1\}$, и вычисляет точку эллиптической кривой $\mathrm{K_A} = \mathrm{k_A P_B}$.

2 Сторона A посылает стороне B - $(\mathrm{Id_A}, \mathrm{Cert_A}, \mathrm{K_A})$.

3 Сторона B проверяет валидность сертификата ключа проверки $\mathrm{Cert_A}$. Если это условие не выполнено, сторона B завершает протокол, возвращая ошибку стороне A, информирующую о невалидности сертификата ключа проверки $\mathrm{Cert_A}$.

4 Сторона B проверяет, что $\mathrm{K_A} \in \mathrm{E_B}$ и $\frac{\mathrm{m}}{\mathrm{q}}\mathrm{K_A} \neq \mathit{0}$. Если это условие не выполнено, сторона B завершает протокол, возвращая ошибку стороне A, информирующую о неверном выборе параметров.

5 Сторона B извлекает из сертификата $\mathrm{Cert_A}$ долговременный ключ проверки подписи $\mathrm{S_A}$.

6 Сторона B случайным образом выбирает k_B, где $k_B \in \{1, \dots, q_B - 1\}$, и вычисляет точку эллиптической кривой $K_B = k_B P_A$.

7 Сторона B вычисляет точки $Q_{AB} = (m_A/q_A) \cdot k_B S_A$ и $R_{AB} = (m_B/q_B) \cdot s_B K_A$.

8 Сторона B вычисляет значение $T_{AB} = KDF(\pi(Q_{AB})||\pi(R_{AB})||Id_A||Id_B\langle||OI\rangle\langle||K\rangle)$.

9 Сторона B вычисляет общие сеансовые ключи $K_{AB} = [T_{AB}]_{0,255}$ и $M_{AB} = [T_{AB}]_{256,511}$.

10 Сторона B вычисляет метку подтверждения ключа $tag_B = MAC_{M_{AB}}(h_2||\pi(K_B)||\pi(K_A)||Id_B||Id_A)$.

11 Сторона B посылает стороне A - $(Id_B, Cert_B, K_B, tag_B)$.

12 Сторона A проверяет валидность сертификата ключа проверки $Cert_B$. Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невалидности сертификата ключа проверки $Cert_B$.

13 Сторона A проверяет, что $K_B \in E_A$ и $\frac{m}{q} K_B \neq \mathcal{O}$. Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о неверном выборе параметров.

14 Сторона A извлекает из сертификата $Cert_B$ долговременный ключ проверки подписи S_B.

15 Сторона A вычисляет точки $Q_{BA} = (m_A/q_A) \cdot s_A K_B$ и $R_{BA} = (m_B/q_B) \cdot k_B S_A$.

16 Сторона A вычисляет значение $T_{BA} = KDF(\pi(Q_{BA})||\pi(R_{BA})||Id_A||Id_B\langle||OI\rangle\langle||K\rangle)$.

17 Сторона A вычисляет общие сеансовые ключи $K_{BA} = [T_{BA}]_{0,255}$ и $M_{BA} = [T_{BA}]_{256,511}$.

18 Сторона A вычисляет метку подтверждения ключа $tag`_B = MAC_{M_{BA}}(h_2||\pi(K_B)||\pi(K_A)||Id_B||Id_A)$ и проверяет $tag_B = tag`_B$. Если это условие не выполнено, сторона A завершает протокол, возвращая ошибку стороне B, информирующую о невозможности аутентификации.

19 Сторона A вычисляет метку подтверждения ключа $tag_A = MAC_{M_{BA}}(h_3||\pi(K_A)||\pi(K_B)||Id_A||Id_B)$.

20 Сторона A посылает стороне B - (tag_A).

21 Сторона B вычисляет метку подтверждения ключа $tag`_A = MAC_{M_{AB}}(h_3||\pi(K_A)||\pi(K_B)||Id_A||Id_B)$ и проверяет $tag_A = tag`_A$. Если это условие не выполнено, сторона B завершает протокол, возвращая ошибку стороне A, информирующую о невозможности аутентификации.

22 Стороны A и B уничтожают ключи M_{BA} и M_{AB} соответственно.

Стороны A и B находятся в состоянии проведенной аутентификации с выработанным общим ключом $\overline{K} = K_{BA} = K_{AB}$.

Библиография

[1] Методические рекомендации по заданию параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012. Технический комитет по стандартизации «Криптографическая защиты информации».

УДК 681.3.06:006.354 ОКС 35. 040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификации, ключ, открытый ключ