Экз. №1

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ (РОССТАНДАРТ)

Технический комитет 026
«Криптографическая защита информации»

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

СХЕМЫ ВЫРАБОТКИ ОБЩЕГО КЛЮЧА С АУТЕНТИФИКАЦИЕЙ НА ОСНОВЕ ОТКРЫТОГО КЛЮЧА

Проект первой редакции

Москва
2016

Содержание

Введение

В настоящее время в Российской Федерации отсутствует единое стандартизированное решение для задачи выработки общего ключа между двумя абонентами в открытой сети. При этом указанная процедура является важнейшей частью протоколов защищенного обмена информацией в сетях связи различного назначения.

Объединение протокола выработки общего ключа с протоколом аутентификации позволит повысить коммуникационную и вычислительную эффективность композиции указанных протоколов. Использование отечественных криптографических алгоритмов в предлагаемых схемах, созданных на основе международных стандартов, обеспечит повышение уровня защиты тайны переговоров и персональных данных граждан.

1. Описание криптографических задач, решаемых с помощью предлагаемого решения

Предлагаемые схемы обеспечивают выработку общего секретного ключа с одновременной двусторонней или односторонней аутентификацией между двумя сторонами, осуществляющими взаимодействие в открытой сети и, как правило, не имеющими заранее распределенной общей секретной информации.

Схемы задают общие алгоритмические решения для создания на их основе конкретных протоколов выработки общего ключа. Ввиду универсальности предлагаемых механизмов, они могут использоваться как составная часть протоколов защищенного обмена информацией в сетях связи различного назначения.

2. Описание предлагаемого решения

Документ определяет схемы протоколов выработки общего ключа с аутентификацией на основе открытого ключа. Описаны три схемы:

- **Эхинацея-3** (**Э-3**): схема выработки общего ключа с двусторонней аутентификацией при помощи ключа цифровой подписи.
- **Эхинацея-2** (**Э-2**): вариант схемы выработки общего ключа с односторонней аутентификацией при помощи ключа цифровой подписи.
- **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.

3. Ссылочные документы

3.1. 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 Р 34.10-2012 — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — Стандартинформ, Москва. 2013.

ГОСТ Р 34.11-2012 — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования. — Стандартинформ, Москва, 2013.

ГОСТ Р 34.12-2015 — Федеральное Агентство по техническому регулированию

и метрологии. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры. — Стандартинформ, Москва, 2015.

ГОСТ Р 34.13-2015 — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. — Стандартинформ, Москва, 2015.

ТК26ЭК — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет №26, Рекомендации по стандартизации. Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012. — Москва, 2013.

ТК26АЛГ — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет №26, Рекомендации по стандартизации. Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. — Москва, 2014.

ТК26ЭД — Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), Технический комитет №26, Методические рекомендации по заданию параметров скрученных эллиптических кривых Эдвардса в соответствии с ГОСТ Р 34.10-2012. — Москва, 2014.

3.2. Дополнительные ссылки

ISO/IEC11770-3 — ISO/IEC 11770-3: Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techinques.

4. Основные понятия, термины, определения

В протоколе участвуют две стороны A и B, между которыми осуществляется выработка общего ключа с аутентификацией.

4.1. Условные обозначения

В данном документе используются следующие обозначения:

V^*	множество всех двоичных строк конечной размерности, включая пустую строку
$A \Vert B$	конкатенация строк $A, B \in V^*$, т.е. строка из $V_{\lvert A\rvert+\lvert B\rvert}$, в которой левая подстрока из $V_{\lvert A\rvert}$ совпадает со строкой A, а правая подстрока из $V_{\lvert B\rvert}$ совпадает со строкой B
$[T]_{i,j}$	для битовой строки $T = (t_0, \ldots, t_n)$ подстрока $T' = (t_i, \ldots, t_j), 0 \leq i \leq j \leq n$
$\mathtt{SGN}_d(T)$	цифровая подпись, выработанная согласно **ГОСТ Р 34.10-2012** для сообщения T с использованием ключа подписи d
$\mathtt{VERIFY}_D(T, S)$	результат проверки цифровой подписи S согласно **ГОСТ Р 34.10-2012** для сообщения T с использованием ключа проверки подписи D
$\mathtt{MAC}_k(T)$	код аутентификации сообщения T с ключом k, способ вычисления кода аутентификации сообщения описан в разделе 4.3.
$\mathtt{KDF}_{512}(T)$	значение функции вычисления производного ключа $\mathtt{KDF}_{512} : V^* \to V^{512}$ на основе строки T, способ вычисления этой функции описан в разделе 4.3.
$\pi(Q)$	функция, отображающая точку на эллиптической кривой в битовую строку, способ вычисления этой функции описан в разделе 4.3.
$\langle \cdot \rangle$	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 секретный и открытый долговременные ключи стороны A
k_A, K_A	соответственно секретный и открытый сеансовые (эфемерные) ключи стороны A
$\mathtt{Id}_A$	идентификатор стороны A (байтовая строка)
$\mathtt{Cert}_A$	сертификат долговременного открытого ключа стороны A

4.2. Эллиптические кривые

В рамках документа предполагается использование операций в группе точек эллиптической кривой E над конечным простым полем характеристики p, заданной в одном из следующих представлений:

- (краткая) форма Вейерштрасса,

$$E_{W,a,b}(GF(p)) = \{(x,y) : y^2 \equiv x^3 + ax + b \pmod{p}\}, \tag{1}$$

- (скрученная) форма Эдвардса,

$$\overline{E}_{\mathrm{Edw},e,d}(GF(p)) = \{(u,v) : eu^2 + v^2 \equiv 1 + du^2v^2 \pmod{p}\}. \tag{2}$$

В документе используются обозначения параметров эллиптической кривой E в форме Вейерштрасса (p,a,b,m,q,x_P,y_P) согласно **ГОСТ Р 34.10-2012** и в скрученной форме Эдвардса $(p,a,b,m,q,x_P,y_P,e,d,u_P,v_P)$ согласно **ТК26ЭД**.

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 (краткой) форме Вейерштрасса должно удовлетворять требованиям **ГОСТ Р 34.10-2012** при $2^{508} < q < 2^{512}$.

4.3. Вспомогательные функции

Код аутентификации сообщения

Для вычисления кода аутентификации сообщения могут использоваться

- алгоритм шифрования «Кузнечик» согласно **ГОСТ Р 34.12-2015** в режиме выработки имитовставки согласно **ГОСТ Р 34.13-2015**;
- функция $HMAC\_GOSTR3411\_2012\_512$, определенная в **ТК26АЛГ**;
- другая функция, использование которой для вычисления кода аутентификации сообщения разрешается национальными стандартами либо методическими документами ТК26.

Вычисление производного ключа

В качестве функции вычисления производного ключа $\mathtt{KDF}_{512} : V^* \to V^{512}$ могут использоваться

- функция хэширования, определенная согласно **ГОСТ Р 34.10-2012** с длиной хэш-кода 512 бит;
- псевдослучайная функция $PRF\_TLS\_GOSTR3411\_2012\_512$ с длиной выхода 512 бит, определенная в **ТК26АЛГ**;
- другая функция, использование которой в качестве функции вычисления производного ключа разрешается национальными стандартами, рекомендациями по стандартизации либо методическими документами ТК26.

Способ вычисления функции $\pi(Q)$

В зависимости от выбранного представления кривой, функция $\pi(Q)$ вычисляется следующим образом.

- (краткая) форма Вейерштрасса: если $Q = (x_Q, y_Q)$, то

$$\pi(Q) = x_Q.$$

- (скрученная) форма Эдвардса: если $Q = (u_Q, v_Q)$, то

$$\pi(Q) = u_Q.$$

5. Схемы выработки общего ключа с аутентификацией

Если действие, предписанное схемой, связано с опциональным параметром, который не определен для конкретной версии протокола, то это действие следует проигнорировать.

При успешном завершении выполнения схемы стороны находятся в состоянии проведенной аутентификации (двусторонней или односторонней, как указано в описании схемы) с выработанным общим ключом.

Предусмотрены также следующие специфические ошибки:

- невалидность сертификата;
- некорректность параметров;
- невозможность аутентификации;
- невозможность подтверждения ключа.

5.1. Эхинацея-3

Долговременными ключами абонентов A и B в этой схеме являются ключи цифровой подписи s_A, S_A и s_B, S_B, определенные согласно разделу 5.2 **ГОСТ Р 34.10-2012** и удостоверенные сертификатами $\mathtt{Cert}_A, \mathtt{Cert}_B$.

5.1.1. Начальное состояние

Абонент A хранит:

- $\mathtt{Id}_A$ – идентификатор абонента A;
- ⟨опционально⟩ заранее распределенное общее секретное значение $\mathscr{K}$, $\mathscr{K} \in V^*$.

Абонент B хранит:

- $\mathtt{Id}_B$ – идентификатор абонента B;
- $\langle$опционально$\rangle$ заранее распределенное общее секретное значение $\mathscr{K}$, $\mathscr{K} \in V^*$.

Параметры эллиптической кривой E: $(p, a, b, m, q, x_P, y_P)$, если выбрана кривая в форме Вейерштрасса, и дополнительно d, e, u_P, v_P, если выбрана кривая в (скрученной) форме Эдвардса, считаются известными обоим абонентам и согласованными до начала выполнения схемы.

Предполагается, что выработка общего ключа и аутентификация осуществляются в рамках сеанса связи, с которым может быть ассоциирована доступная обоим абонентам открытая общая информация $\mathtt{OI}$.

5.1.2. Схема Э-3

1. A случайным образом выбирает значение k_A, $k_A \in \{1, \ldots, q-1\}$, вычисляет точку $K_A = k_A P$.
2. A посылает B $\mathtt{Id}_A, \mathtt{Cert}_A, K_A$.
3. B проверяет валидность сертификата $\mathtt{Cert}_A$. Если это условие не выполнено, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном сертификате.
4. B проверяет, что $K_A \in E$, а также, что $cK_A \neq \mathscr{O}$. Если эти условия не выполнены, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном выборе параметров.
5. B случайным образом выбирает значение k_B, $k_B \in \{1, \ldots, q-1\}$, вычисляет точку $K_B = k_B P$.
6. B вычисляет точку $Q_{AB} = k_B(cK_A)$.
7. B вычисляет значение $T_{AB} = \mathtt{KDF}(\pi(Q_{AB}) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B \langle\parallel \mathtt{OI}\rangle \langle\parallel \mathscr{K}\rangle)$.

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

9. B вычисляет тэг аутентификации $aut_B = \mathtt{SGN}_{s_B}(\pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_A)$ и тэг подтверждения ключа $tag_B = \mathtt{MAC}_{M_{AB}}(h_2 \parallel \pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_B \parallel \mathtt{Id}_A)$.

10. B посылает A $\mathtt{Id}_B, \mathtt{Cert}_B, K_B, aut_B, tag_B$.

11. A проверяет валидность сертификата $\mathtt{Cert}_B$. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о неверном сертификате.

12. A проверяет цифровую подпись B: $\mathtt{VERIFY}_{S_B}(\pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_A, aut_B) =$ “верно”. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о невозможности аутентификации.

13. A проверяет, что $K_B \in E$, а также, что $cK_B \neq \mathscr{O}$. Если эти условия не выполнены, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном выборе параметров.

14. A вычисляет точку $Q_{BA} = k_A(cK_B)$.

15. A вычисляет значение $T_{BA} = \mathtt{KDF}(\pi(Q_{BA}) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B \langle \parallel \mathtt{OI} \rangle \langle \parallel \mathscr{K} \rangle)$.

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

17. A вычисляет $tag'_B = \mathtt{MAC}_{M_{BA}}(h_2 \parallel \pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_B \parallel \mathtt{Id}_A)$ и проверяет, что $tag_B = tag'_B$. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о невозможности подтверждения ключа.

18. A вычисляет тэг аутентификации $aut_A = \mathtt{SGN}_{s_A}(\pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_B)$ и тэг подтверждения ключа $tag_A = \mathtt{MAC}_{M_{BA}}(h_3 \parallel \pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B)$.

19. A посылает B aut_A, tag_A.

20. B проверяет цифровую подпись A: $\mathtt{VERIFY}_{S_A}(\pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_B, aut_A) =$ “верно”. Если это условие не выполнено, то B завершает сеанс связи, возвращая ошибку, информирующую о невозможности аутентификации.

21. B вычисляет

$$tag'_A = \mathtt{MAC}_{M_{AB}}(h_3 \parallel \pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B)$$

и проверяет, что $tag_A = tag'_A$. Если это условие не выполнено, то B завершает сеанс связи, возвращая ошибку, информирующую о невозможности подтверждения ключа.

После завершения схемы абоненты A и B находятся в состоянии проведенной двусторонней аутентификации с выработанным общим ключом $K = K_{AB} = K_{BA}$. Ключи M_{AB}, M_{BA} более не используются и уничтожаются.

5.2. Эхинацея-2

В этой схеме только абонент B располагает долговременными ключами s_B, S_B, определенными согласно разделу 5.2 **ГОСТ Р 34.10-2012** и удостоверенными сертификатом $\mathtt{Cert}_B$.

5.2.1. Начальное состояние

Абонент A хранит:

- $\mathtt{Id}_A$ – идентификатор абонента A;
- ⟨опционально⟩ заранее распределенное общее секретное значение $\mathscr{K}$, $\mathscr{K} \in V^*$.

Абонент B хранит:

- $\mathtt{Id}_B$ – идентификатор абонента B;
- ⟨опционально⟩ заранее распределенное общее секретное значение $\mathscr{K}$, $\mathscr{K} \in V^*$.

Параметры эллиптической кривой E: $(p, a, b, m, q, x_P, y_P)$, если выбрана кривая в форме Вейерштрасса, и дополнительно d, e, u_P, v_P, если выбрана кривая в (скрученной) форме Эдвардса, считаются известными обоим абонентам и согласованными до начала выполнения схемы.

Предполагается, что выработка общего ключа и аутентификация осуществляются в рамках сеанса связи, с которым может быть ассоциирована доступная обоим абонентам открытая общая информация $\mathtt{OI}$.

5.2.2. Схема Э-2

1. A случайным образом выбирает значение k_A, $k_A \in \{1, \ldots, q-1\}$, вычисляет точку $K_A = k_A P$.

2. A посылает B $\mathtt{Id}_A, K_A$.

3. B проверяет, что $K_A \in E$, а также, что $cK_A \neq \mathscr{O}$. Если эти условия не выполнены, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном выборе параметров.

4. B случайным образом выбирает значение k_B, $k_B \in \{1, \ldots, q-1\}$, вычисляет точку $K_B = k_B P$.

5. B вычисляет точку $Q_{AB} = k_B(cK_A)$.

6. B вычисляет значение $T_{AB} = \mathtt{KDF}(\pi(Q_{AB}) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B \langle\parallel \mathtt{OI}\rangle \langle\parallel \mathscr{K}\rangle)$.

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

8. B вычисляет тэг аутентификации

$$aut_B = \mathtt{SGN}_{s_B}(\pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_A)$$

   и тэг подтверждения ключа

$$tag_B = \mathtt{MAC}_{M_{AB}}(h_2 \parallel K_B \parallel K_A \parallel \mathtt{Id}_B \parallel \mathtt{Id}_A).$$

9. B посылает A $\mathtt{Id}_B, \mathtt{Cert}_B, K_B, aut_B, tag_B$.

10. A проверяет валидность сертификата $\mathtt{Cert}_B$. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о неверном сертификате.

11. A проверяет цифровую подпись B: $\mathtt{VERIFY}_{S_B}(\pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_A, aut_B) =$ “верно”. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о невозможности аутентификации.

12. A проверяет, что $K_B \in E$, а также, что $cK_B \neq \mathscr{O}$. Если эти условия не выполнены, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном выборе параметров.

13. A вычисляет точку $Q_{BA} = k_A(cK_B)$.

14. A вычисляет значение $T_{BA} = \mathtt{KDF}(\pi(Q_{BA}) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B \langle \parallel \mathtt{OI} \rangle \langle \parallel \mathscr{K} \rangle)$.

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

16. A вычисляет

$$tag'_B = \mathtt{MAC}_{M_{BA}}(h_2 \parallel \pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_B \parallel \mathtt{Id}_A)$$

и проверяет, что $tag_B = tag'_B$. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о невозможности аутентификации.

17. A вычисляет тэг подтверждения ключа

$$tag_A = \mathtt{MAC}_{M_{BA}}(h_3 \parallel \pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B).$$

18. A посылает B tag_A.

19. B вычисляет $tag'_A = \mathtt{MAC}_{M_{AB}}(h_3 \parallel \pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B)$ и проверяет, что $tag_A = tag'_A$. Если это условие не выполнено, то B завершает сеанс связи, возвращая ошибку, информирующую о невозможности подтверждения ключа.

После завершения схемы абоненты A и B находятся в состоянии проведенной односторонней аутентификации (B перед A) с выработанным общим ключом $K = K_{AB} = K_{BA}$. Ключи M_{AB}, M_{BA} более не используются и уничтожаются.

5.3. Лимонник-3

В этой схеме допускается использование абонентами двух (возможно, различных) эллиптических кривых E_A и E_B. Если используются эллиптические кривые в форме Вейерштрасса, то эллиптическая кривая E_A задается параметрами $(p_A, a_A, b_A, m_A, q_A, x_{P_A}, y_{P_A})$, а эллиптическая кривая E_B задается параметрами $(p_B, a_B, b_B, m_B, q_B, x_{P_B}, y_{P_B})$. Если используются эллиптические кривые в скрученной форме Эдвардса, то эллиптическая кривая E_A задается параметрами $(p_A, a_A, b_A, m_A, q_A, x_{P_A}, y_{P_A}, e_A, d_A, u_{P_A}, v_{P_B})$, а эллиптическая кривая E_B задается параметрами $(p_B, a_B, b_B, m_B, q_B, x_{P_B}, y_{P_B}, e_B, d_B, u_{P_B}, v_{P_B})$. Соответствующие кофакторы равны $c_A = m_A/q_A$, $c_B = m_B/q_B$.

Долговременные ключи абонентов (s_A, S_A) и (s_B, S_B) определяются соотношениями $S_A = s_A P_A$, $S_B = s_B P_B$, где $0 < s_A < q_A$, $0 < s_B < q_B$, и удостоверяются сертификатами $\mathtt{Cert}_A, \mathtt{Cert}_B$.

5.3.1. Начальное состояние

Абонент A хранит:

- $\mathtt{Id}_A$ – идентификатор абонента A;
- ⟨опционально⟩ заранее распределенное общее секретное значение $\mathscr{K}$.

Абонент B хранит:

- $\mathtt{Id}_B$ – идентификатор абонента B;
- ⟨опционально⟩ заранее распределенное общее секретное значение $\mathscr{K}$.

Параметры эллиптических кривых E_A, E_B считаются известными обоим абонентам и согласованными до начала схемы.

Предполагается, что выработка общего ключа и аутентификация осуществляются в рамках сеанса связи, с которым может быть ассоциирована доступная обоим абонентам открытая общая информация $\mathtt{OI}$.

5.3.2. Схема Л-3

1. A случайным образом выбирает значение k_A, $k_A \in \{1, \ldots, q_B - 1\}$, вычисляет точку $K_A = k_A P_B$.

2. A посылает B $\mathtt{Id}_A, \mathtt{Cert}_A, K_A$.

3. B проверяет валидность сертификата $\mathtt{Cert}_A$. Если это условие не выполнено, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном сертификате.

4. B проверяет, что $K_A \in E_B$ и $c_B K_A \neq \mathscr{O}$. Если эти условия не выполнены, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном выборе параметров.

5. B случайным образом выбирает значение k_B, $k_B \in \{1, \ldots, q_A - 1\}$, вычисляет точку $K_B = k_B P_A$.

6. B вычисляет точки $Q_{AB} = c_A \cdot k_B S_A$ и $R_{AB} = s_B(c_B K_A)$.

7. B вычисляет значение $T_{AB} = \mathtt{KDF}(\pi(Q_{AB}) \parallel \pi(R_{AB}) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B \langle \parallel \mathtt{OI} \rangle \langle \parallel \mathscr{K} \rangle)$.

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

9. B вычисляет тэг подтверждения ключа

$$tag_B = \mathtt{MAC}_{M_{AB}}(h_2 \parallel \pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_B \parallel \mathtt{Id}_A).$$

10. B посылает A $\mathtt{Id}_B, \mathtt{Cert}_B, K_B, tag_B$.

11. A проверяет валидность сертификата B. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о неверном сертификате.

12. A проверяет, что $K_B \in E_A$ и $c_A K_B \neq \mathscr{O}$. Если эти условия не выполнены, то B завершает сеанс связи, возвращая ошибку, информирующую о неверном выборе параметров.

13. A вычисляет точки $Q_{BA} = s_A(c_A K_B)$ и $R_{BA} = c_B \cdot k_A S_B$.

14. A вычисляет значение $T_{BA} = \mathtt{KDF}(\pi(Q_{BA}) \parallel \pi(R_{BA})\mathtt{Id}_A \parallel \mathtt{Id}_B\langle\parallel \mathtt{OI}\rangle\langle\parallel \mathscr{K}\rangle)$.

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

16. A вычисляет $tag'_B = \mathtt{MAC}_{M_{BA}}(h_2 \parallel \pi(K_B) \parallel \pi(K_A) \parallel \mathtt{Id}_B \parallel \mathtt{Id}_A)$ и проверяет, что $tag_B = tag'_B$. Если это условие не выполнено, то A завершает сеанс связи, возвращая ошибку, информирующую о невозможности аутентификации.

17. A вычисляет тэг подтверждения ключа

$$tag_A = \mathtt{MAC}_{M_{BA}}(h_3 \parallel \pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B).$$

18. A посылает B tag_A.

19. B вычисляет

$$tag'_A = \mathtt{MAC}_{M_{AB}}(h_3 \parallel \pi(K_A) \parallel \pi(K_B) \parallel \mathtt{Id}_A \parallel \mathtt{Id}_B)$$

и проверяет, что $tag_A = tag'_A$. Если это условие не выполнено, то B завершает сеанс связи, возвращая ошибку, информирующую о невозможности аутентификации.

После завершения схемы абоненты A и B находятся в состоянии проведенной двусторонней аутентификации с выработанным общим ключом $K = K_{AB} = K_{BA}$. Ключи M_{AB}, M_{BA} более не используются и уничтожаются.

6. Авторы проекта документа

С.В. Гребнев (ТК 26)

grebnev_sv@tc26.ru