ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.015— 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платежных систем

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «Системы практической безопасности» (ООО «СПБ») совместно с Открытым акционерным обществом «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС») и Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)

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 2 марта 2018 г. № 116-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «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 (*gost.e-ecolog.ru

© Стандартинформ, 2018

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и обозначения 2
3.1 Термины и определения 2
3.2 Обозначения 2
4 Описание параметров 2
4.1 Инфраструктура открытых ключей приложения 3

Введение

В настоящих рекомендациях описан формат сертификатов открытых ключей платежной системы «Мир».

В данной системе использованы три уровня сертификатов открытых ключей: уровень центра сертификации карт платежной системы «Мир», уровень банка — эмитента карты, уровень приложения.

В платежной системе используется схема выпуска сертификатов открытых ключей, в соответствии с которой сертификат удостоверяющего центра платежной системы является корневым сертификатом. Данный удостоверяющий центр выдает сертификаты банкам эмитентам, которые в свою очередь выдают сертификаты для платежных карт.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платежных систем

Information technology. Cryptographic data security. Setting parameters of digital signature algorithm and hash function in the template of EMV public key certificates of the payment systems

Дата введения — 2018—08—01

1 Область применения

Настоящие рекомендации предназначены для описания сертификатов открытых ключей, используемых при аутентификации: при проверке цепочки сертификатов открытых ключей терминал с помощью открытого ключа удостоверяющего центра проверяет сертификат открытого ключа банка-эмитента, после чего с помощью открытого ключа этого банка проверяет подлинность сертификата открытого ключа карты. Кроме того, в настоящих рекомендациях описан формат сертификата открытого ключа карты для оффлайновой проверки PIN.

Сертификаты открытых ключей удостоверяющего центра платежной системы, банка-эмитента и карты содержат поля, которые позволяют связать открытый ключ с конкретным удостоверяющим центром, банком-эмитентом или картой.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

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

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов 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 документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

3.1.1 **банк-эмитент**: Банк, выпустивший платежную карту.

3.1.2 **терминал**: Аппаратно-программный комплекс, обеспечивающий прием платежей от физических лиц в режиме самообслуживания.

3.1.3 **цепочка сертификатов**: Структура, позволяющая проверить валидность сертификата банка-эмитента.

3.2 Обозначения

В настоящих рекомендациях используют следующие обозначения:

b	— бинарный формат данных;
$C_{icc-iss}$	— Issuer Public Key Certificate. Сертификат открытого ключа банка-эмитента;
C_{icc}	— ICC Public Key Certificate. Сертификат открытого ключа карты;
cn	— сжатый цифровой формат данных. Данные указанного формата всегда должны быть дополнены справа до нужного количества байт символами ‘0xf’;
ICC	— Integrated Circuit Card. Карта с интегральной микросхемой;
id-tc26-gost3410-2012-256	— функция формирования/проверки электронной подписи в соответствии с ГОСТ Р 34.10—2012;
id-tc26-gost3411-2012-256	— функция хэширования в соответствии с ГОСТ Р 34.11—2012;
id-GostR3410-2001-CryptoPro-A-ParamSet	— набор параметров алгоритма формирования/проверки электронной подписи в соответствии с ГОСТ Р 34.10—2012;
n	— цифровой формат данных. Данные указанного формата всегда должны быть дополнены справа до нужного количества байт символами ‘0x0’;
P_{icc}	— открытый ключ карты;
P_{icc-ca}	— открытый ключ удостоверяющего центра;
$P_{icc-iss}$	— открытый ключ банка-эмитента;
PAN	— номер карты (Primary Account Number). Длина значения равна от 12 до 20 десятичных цифр;
S_{icc}	— закрытый ключ карты;
S_{icc-ca}	— закрытый ключ удостоверяющего центра;
$S_{icc-iss}$	— закрытый ключ банка-эмитента.

4 Описание параметров

Схема инфраструктуры открытых ключей приложения изображена на рисунке 1.

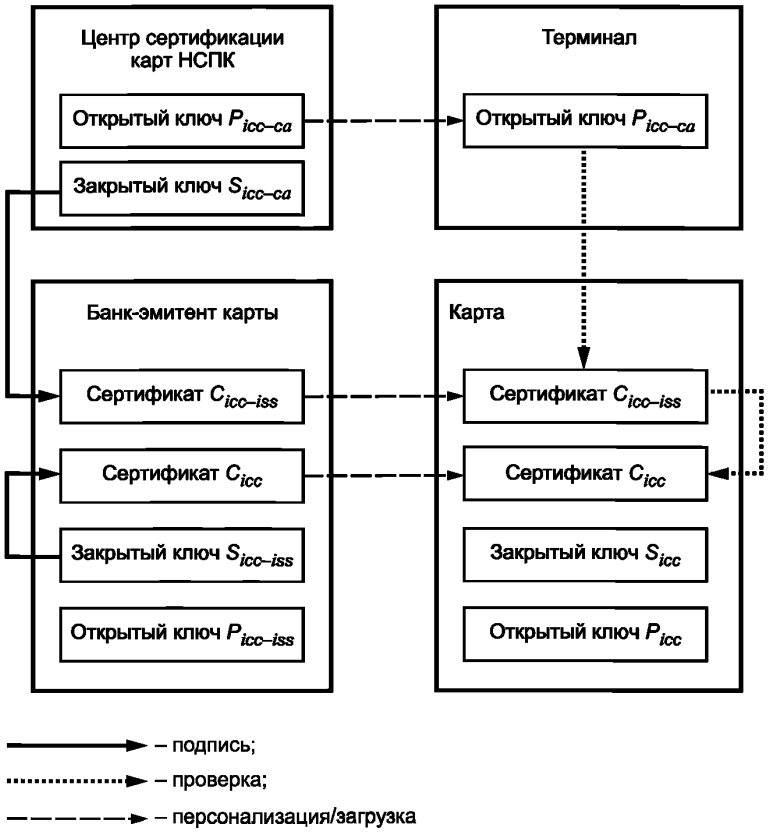

Рисунок 1

4.1 Инфраструктура открытых ключей приложения

Для формирования и проверки электронной цифровой подписи должны быть использованы алгоритмы, описанные в ГОСТ Р 34.10—2012, с длиной ключа порядка 256 бит (длина подписи — 256 бит) и параметрами id-GostR3410-2001-CryptoPro-A-ParamSet.

Форматы сертификатов открытых ключей банка-эмитента, карты и удостоверяющего центра, в роли которого выступает центр сертификации Национальной системы платежных карт (НСПК), представлены в таблицах 1—5.

Таблица 1 — Формат сертификата открытого ключа удостоверяющего центра

Имя поля	Длина, байт	Описание/значение	Формат
Header (заголовок)	1	'0x31'	b
Service Identificator (идентификатор приложения)	4	Например, '10100000' — для корневых ключей	cn8
RID — Registered Application ID (зарегистрированный идентификатор приложения)	5	'0xa000000658'	b
CA Public Key Index (индекс открытого ключа удостоверяющего центра)	1	Номер ключа проверки подписи удостоверяющего центра, в роли которого выступает НСПК	b
Certificate Expiration Date (дата истечения срока действия сертификата)	2	Дата (месяц и год), после которой сертификат открытого ключа недействителен	n4

Окончание таблицы 1

Имя поля	Длина, байт	Описание/значение	Формат
CA Public Key Algorithm Indicator (индикатор алгоритма формирования/проверки электронной подписи удостоверяющего центра)	1	'0x11' — определяет алгоритм id-tc26-gost3410-2012-256	b
CA Public Key Parameters Indicator (индикатор параметров для алгоритма формирования/проверки электронной подписи удостоверяющего центра)	1	'0x01' — определяет набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet	b
CA Public Key (открытый ключ удостоверяющего центра)	64	Поле содержит открытый ключ удостоверяющего центра	b
Hash Algorithm Indicator (индикатор алгоритма вычисления хэш-функции)	1	'0x11' — определяет алгоритм id-tc26-gost3411-2012-256	b
Signature (подпись)	64	Подпись от предыдущих полей сертификата открытого ключа	b

Таблица 2 — Формат запроса на сертификацию банка-эмитента

Имя поля	Длина, байт	Описание/значение	Формат
Header (заголовок)	1	'0x33'	b
Service Identificator (идентификатор приложения)	4	Например: '2010 0000' — продукт «Дебетовая»	cn8
Certificate Format (формат сертификата открытого ключа)	1	'0x13'	b
Issuer Identification Number (идентификационный номер банка-эмитента)	4	Крайние левые с 3 по 8 цифры из PAN	b
Certificate Expiration Date (дата истечения срока действия сертификата)	2	Дата (месяц и год), после которой сертификат открытого ключа недействителен	n4
Tracking Number (номер отслеживания)	3	Уникальный номер запроса сертификата открытого ключа в системе банка-эмитента	b
Hash Algorithm Indicator (индикатор алгоритма вычисления хэш-функции)	1	'0x11' — определяет алгоритм id-tc26-gost3411-2012-256	b
Issuer Public Key Algorithm Indicator (индикатор алгоритма формирования/проверки электронной подписи банка-эмитента)	1	'0x11' — определяет алгоритм id-tc26-gost3410-2012-256	b
Issuer Public Key Parameters Indicator (индикатор параметров для алгоритма формирования/проверки электронной подписи банка-эмитента)	1	'0x01' — определяет набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet	b
Issuer Public Key Length [длина открытого ключа банка-эмитента (в битах)]	2	'0x200'	b
Issuer Public Key (открытый ключ банка-эмитента)	64	Поле содержит открытый ключ банка-эмитента	b
Signature (подпись)	64	Подпись от предыдущих полей сертификата открытого ключа	b

Таблица 3 — Формат сертификата открытого ключа банка-эмитента

Имя поля	Длина, байт	Описание/значение	Формат
Header (заголовок)	1	'0x7A'	b
Certificate Format (формат сертификата открытого ключа)	1	'0x12'	b
Issuer Identification Number (идентификационный номер банка-эмитента)	4	Крайние левые с 3-й по 8-ю цифры из PAN	b
Certificate Expiration Date (дата истечения срока действия сертификата)	2	Дата (месяц и год), после которой сертификат открытого ключа недействителен	n4
Certificate Serial Number (серийный номер сертификата)	3	Двоичный номер, уникальный для данного сертификата открытого ключа, присвоенный банком-эмитентом	b
Hash Algorithm Indicator (индикатор алгоритма вычисления хэш-функции)	1	'0x11' — определяет алгоритм id-tc26-gost3411-2012-256	b
Issuer Public Key Algorithm Indicator (индикатор алгоритма формирования/проверки электронной подписи банка-эмитента)	1	'0x11' — определяет алгоритм id-tc26-gost3410-2012-256	b
Issuer Public Key Parameters Indicator (индикатор параметров для алгоритма формирования/проверки электронной подписи банка-эмитента)	1	'0x01' — определяет набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet	b
Issuer Public Key (открытый ключ банка-эмитента)	64	Поле содержит открытый ключ банка-эмитента	b
Signature (подпись)	64	Подпись от предыдущих полей сертификата открытого ключа	b
Data Trailer (завершающие данные)	1	'0xBC'	

Таблица 4 — Формат сертификата открытого ключа карты для аутентификации

Имя поля	Длина, байт	Описание	Формат
Header (Заголовок)	1	'0x7B'	b
Certificate Format (формат сертификата открытого ключа)	1	'0x14'	b
PAN	10	Номер карты	cn20
Certificate Expiration Date (дата истечения срока действия сертификата)	2	Дата (месяц и год), после которой сертификат открытого ключа недействителен	n4
Certificate Serial Number (серийный номер сертификата)	3	Двоичный номер, уникальный для данного сертификата открытого ключа, присвоенный банком-эмитентом	b
Hash Algorithm Indicator (индикатор алгоритма вычисления хэш-функции)	1	'0x11' — определяет алгоритм id-tc26-gost3411-2012-256	b
ICC Public Key Algorithm Indicator (индикатор алгоритма формирования/проверки электронной подписи карты)	1	'0x11' — определяет алгоритм id-tc26-gost3410-2012-256	b

Окончание таблицы 4

Имя поля	Длина, байт	Описание	Формат
ICC Public Key Parameters Indicator (индикатор параметров для алгоритма формирования/проверки электронной подписи карты)	1	'0x01' — определяет набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet	b
ICC Public Key (открытый ключ карты)	64	Поле содержит открытый ключ карты	b
Static Data to be Authenticated (статические данные, подлинность которых проверяется)	Переменная	Данные, целостность которых гарантируется. Определяются непосредственно банком-эмитентом	b
Signature (подпись)	64	Подпись от предыдущих полей сертификата открытого ключа	b

Таблица 5 — Формат сертификата открытого ключа карты для оффлайновой проверки PIN

Имя поля	Длина, байт	Описание	Формат
Header (заголовок)	1	'0x7B'	b
Certificate Format (формат сертификата открытого ключа)	1	'0x15'	b
PAN	10	Номер карты	cn20
Certificate Expiration Date (дата истечения срока действия сертификата)	2	Дата (месяц и год), после которой сертификат открытого ключа недействителен	n4
Certificate Serial Number (серийный номер сертификата)	3	Двоичный номер, уникальный для данного сертификата открытого ключа, присвоенный банком-эмитентом	b
Hash Algorithm Indicator (индикатор алгоритма вычисления хэш-функции)	1	'0x11' — определяет алгоритм id-tc26-gost3411-2012-256	b
ICC PIN Encryption Public Key Algorithm Indicator (индикатор алгоритма формирования/проверки электронной подписи карты для оффлайного шифрования PIN)	1	'0x11' — определяет алгоритм id-tc26-gost3410-2012-256	b
ICC PIN Encryption Public Key Parameters Indicator (индикатор параметров для алгоритма формирования/проверки электронной подписи карты для оффлайного шифрования PIN)	1	'0x01' — определяет набор параметров id-GostR3410-2001-CryptoPro-A-ParamSet	b
ICC PIN Encryption Public Key (открытый ключ карты для оффлайного шифрования PIN)	64	Поле содержит открытый ключ карты	b
Signature (подпись)	64	Подпись от предыдущих полей сертификата открытых ключей	b

УДК 681.3.06:006.354 ОКС 35. 040

Ключевые слова: информационная технология, криптографическая защита информации, сертификаты открытых ключей, электронная подпись, платежная карта, банк-эмитент, удостоверяющий центр

БЗ 3—2018/47

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 02.03.2018. Подписано в печать 06.03.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 19 экз. Зак. 410.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru