ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.016—2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре оффлайновой аутентификации платежного приложения

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 5 марта 2018 г. № 117-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 Обозначения 2
4 Описание алгоритмов 3
4.1 Алгоритм формирования объекта ICC Dynamic Number (IDN) 3
4.2 Динамическая аутентификация платежного приложения (DDA) 3
4.3 Комбинированная аутентификация платежного приложения (CDA) 4
Приложение А (справочное) Контрольные примеры 7

Введение

В настоящих рекомендациях представлен алгоритм оффлайновой аутентификации платежного приложения. Данная процедура является ключевым элементом безопасности операций, выполняемых с помощью механизмов платежных карт.

В настоящих рекомендациях рассматриваются криптографические механизмы двух видов оффлайновой аутентификации: динамической и комбинированной. Динамическая аутентификация обеспечивает проверку целостности критичных данных приложения и проверку подлинности карты и производится до выполнения команды GENERATE AC. Комбинированная аутентификация обеспечивает еще и целостность критичных данных, циркулирующих между картой и терминалом, и проводится в рамках процедуры обработки команды GENERATE AC.

Команда GENERATE AC отправляет связанные с транзакцией данные на карту, которая вычисляет и возвращает криптограмму приложения.

Разработка настоящих рекомендаций вызвана необходимостью внедрения процедур для оффлайновой аутентификации платежных приложений.

Примечание — Настоящие рекомендации дополнены приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре оффлайновой аутентификации платежного приложения

Information technology. Cryptographic data security.
Using block encryption algorithm modes, digital signature algorithm and hash function in offline authentication of the payment application

Дата введения — 2018—08—01

1 Область применения

Настоящие рекомендации предназначены для описания алгоритмов, используемых в процессе оффлайновой аутентификации в платежной системе «МИР».

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие документы:

ГОСТ 28147—89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

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

Р 1323565.1.010—2017 Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения

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

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 Обозначения

В настоящих рекомендациях используют следующие обозначения:

V_n — конечномерное векторное пространство размерности *n;*

$A||B$ — конкатенация строк, т. е. если $A \in V_{n_1}$, $B \in V_{n_2}$, $A = (a_{n1-1}, a_{n1-2}, \ldots, a_0)$, $B = (b_{n2-1}, b_{n2-2}, \ldots, b_0)$, то $A||B = (a_{n1-1}, a_{n1-2}, \ldots, a_0, b_{n2-1}, b_{n2-2}, \ldots, b_0) \in V_{n1+n2}$;

ATC — Application Transaction Counter. Номер текущей транзакции. Длина значения равна 2 байтам;

C_{icc} — ICC Public Key Certificate. Сертификат открытого ключа карты;

$C_{icc-iss}$ — Issuer Public Key Certificate. Сертификат открытого ключа эмитента;

CDA — Combined Dynamic Data Authentication/Application Cryptogram Generation. Комбинированная оффлайновая аутентификация приложения карты;

CDOL1 — Combined Dynamic Data Authentication Data Object List. Перечень тегов и длин объектов данных, значения которых должны быть переданы карте во время первой команды GENERATE AC;

CDOL2 — Combined Dynamic Data Authentication Data Object List. Перечень тегов и длин объектов данных, значения которых должны быть переданы карте во время второй команды GENERATE AC;

CID — Cryptogram Information Data. Тип используемой криптограммы. Длина значения равна 1 байту. Возможные значения: ‘00’ — криптограмма AAC, ‘40’ — криптограмма TC, ‘80’ — криптограмма ARQC;

DDA — Dynamic Data Authentication. Оффлайновая динамическая аутентификация приложения карты;

DDOL — Dynamic Data Authentication Data Object List. Список (теги и длины) объектов данных, необходимых карте для формирования данных, подписываемых картой;

$E_K(M)$ — функция зашифрования;

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 с длиной ключа порядка 256 бит;

id-tc26-gost3411-2012-256 — функция хэширования в соответствии с ГОСТ Р 34.11—2012 с длиной ключа порядка 256 бит;

id-Gost28147-89 — функция шифрования в режиме простой замены в соответствии с алгоритмом ГОСТ 28147—89 с узлом замены id-tc26-gost-28147-param-Z;

id-GostR3410-2001-CryptoPro-A-ParamSet — набор параметров алгоритма формирования/проверки электронной подписи в соответствии с ГОСТ Р 34.10—2012;

IDN — ICC Dynamic Number. Используется для подтверждения факта выполнения терминалом процедуры аутентификации карты. Длина значения равна от 2 до 8 байт;

IDN Length — длина значения объекта IDN;

MK_{IDN} — мастер-ключ карты для вычисления IDN; формируется в соответствии с Р 1323565.1.010—2017. Длина значения равна 32 байтам;

P_{icc} — ICC Public Key. Открытый ключ карты;

$P_{icc-iss}$ — Issuer Public Key. Открытый ключ эмитента;

PDOL — Processing Options Data Object List (Tag ‘9F38’). Определяет данные о транзакции и терминале, необходимые карте, для принятия решения о наилучшем с точки зрения эмитента карты способе обработки операции;

S_{icc} — ICC Secret Key. Секретный ключ карты;

Unpredictable Number — случайное число, генерируемое терминалом. Длина значения равна 4 байтам.

4 Описание алгоритмов

Суть методов состоит в том, что терминал генерирует случайное число, передаваемое карте вместе с некоторыми другими данными для подписи.

Карта возвращает терминалу подписанные данные терминала, и в том случае, если терминал устанавливает, что подпись полученных от карты данных, а также сертификаты ключа эмитента и ключа карты оказываются правильными, следует вывод о том, что карта подлинная.

Оффлайновая аутентификация карты выполняется при каждой транзакции. Выбор метода аутентификации осуществляется терминалом на основе возможностей терминала и профиля обмена приложениями.

Для оффлайновой аутентификации карты используются специальные сертификаты, формат которых представлен в Рекомендации «Задание параметров алгоритмов электронной подписи и функции хэширования в профиле сертификатов открытых ключей платежных систем».

Возможные значения аргументов функций в представленных алгоритмах ограничены допустимостью их использования в качестве входных параметров преобразований.

4.1 Алгоритм формирования объекта ICC Dynamic Number (IDN)

Объект данных IDN представляет собой результат зашифрования $(ATC||'0x00'||'0x00'||'0x00'||'0x00'||'0x00'||'0x00')$ на ключе MK_{IDN} в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z:

$$IDN = E_{MK_{IDN}}(ATC||'0x00'||'0x00'||'0x00'||'0x00'||'0x00'||'0x00').$$

В качестве IDN выбираются *n* левых (старших) байтов результата зашифрования, где *n* = IDN Length (принимает значение от 2 до 8).

4.2 Динамическая аутентификация платежного приложения (DDA)

4.2.1 Формирование данных и установка подписи платежного приложения

Карта в соответствии со списком объекта DDOL формирует поля, определенные в таблице 1.

Таблица 1

Имя поля		Длина, байт		Описание
Signed Data Format (формат подписываемых данных)		1		Значение '0x15'
Public Key Algorithm Indicator (индикатор алгоритма подписи)		1		Идентифицирует алгоритм подписи; принимает значение '0x11', соответствующее алгоритму id-tc26-gost3410-2012-256
Public Key Parameters Indicator (индикатор набора параметров алгоритма подписи)		1		Идентифицирует набор параметров алгоритма подписи; принимает значение '0x01', соответствующее id-GostR3410-2001-CryptoPro-A-ParamSet
ICC Dynamic Data Length (длина динамических данных карты)		1		Длина динамических данных в байтах
ICC Dynamic Data (динамические данные карты)	IDN Length	L_{dd}	1	Динамические данные, сформированные картой или сохраненные на карте
	IDN		2—8	
Unpredictable Number		4		Случайное число, генерируемое терминалом

Данные таблицы 1 подписываются секретным ключом карты S_{icc} в соответствии с ГОСТ Р 34.10—2012 с длиной ключа порядка 256 бит. После чего формируется Signed Dynamic Application Data согласно таблице 2.

Таблица 2

Имя поля		Длина, байт		Описание
Data Header (заголовок)		1		Значение '0x6a'
Signed Data Format (формат данных)		1		Значение '0x15'
Public Key Algorithm Indicator (индикатор алгоритма подписи)		1		Идентифицирует алгоритм подписи; принимает значение '0x11', соответствующее алгоритму id-tc26-gost3410-2012-256
Public Key Parameters Indicator (индикатор набора параметров алгоритма подписи)		1		Идентифицирует набор параметров алгоритма подписи; принимает значение '0x01', соответствующее id-GostR3410-2001-CryptoPro-A-ParamSet
ICC Dynamic Data Length (длина динамических данных карты)		1		Длина динамических данных в байтах
ICC Dynamic Data (динамические данные карты)	IDN Length	L_{dd}	1	Динамические данные, сформированные картой или сохраненные на карте
	IDN		2—8	
Signature (подпись)		64		Подпись от данных, приведенных в таблице 1, в соответствии с ГОСТ Р 34.10—2012 256 бит
Data Trailer		1		'0xbc'

Полученный результат (Signed Dynamic Application Data) направляется терминалу в поле данных ответа на команду INTERNAL AUTHENTICATE.

4.2.2 Проверка подписи данных платежного приложения карты терминалом

Проверка терминалом полученного значения Signed Dynamic Application Data выполняется с помощью открытого ключа карты P_{icc}. Для этого:

- извлекается открытый ключ удостоверяющего центра платежной системы;
- верифицируется сертификат открытого ключа эмитента $C_{icc-iss}$ согласно Р 1323565.1.015—2018;
- извлекается открытый ключ эмитента $P_{icc-iss}$;
- верифицируется сертификат открытого ключа карты C_{icc} согласно Р 1323565.1.015—2018;
- извлекается открытый ключ карты P_{icc};
- формируются данные таблицы 1;
- выполняется проверка цифровой подписи (Signature), приведенной в таблице 2, в соответствии с ГОСТ Р 34.10—2012 с длиной ключа порядка 256 бит;
- производится проверка элемента «Формат данных» (Signed Data Format), который должен быть равен '0x15'.

Карта считается успешно аутентифицированной, когда все проверки завершились успешно. В этом случае терминал запоминает значение IDN, если оно присутствует в данных Signed Dynamic Application Data, для последующей пересылки эмитенту при верификации.

4.3 Комбинированная аутентификация платежного приложения (CDA)

4.3.1 Формирование данных и установка подписи платежного приложения

Карта формирует объект Transaction Data Hash Code, для чего используется алгоритм ГОСТ Р 34.11—2012 с длиной ключа порядка 256 бит, выполняемый над приведенными ниже данными, взятыми в следующем порядке:

- поля данных объектов, определенных в списке PDOL, взятые в том же порядке, в котором они приведены в PDOL;
- поля данных объектов, определенных в списке CDOL1, взятые в том же порядке, в котором они приведены в CDOL1;

- поля данных объектов, определенных в списке CDOL2, взятые в том же порядке, в котором они приведены в CDOL2;
- значения полей Tag, Length, Value объектов данных (за исключением объекта Signed Dynamic Application Data), возвращаемых картой в ответе на первую (вторую) команду GENERATE AC, взятые в том же порядке, в котором они возвращаются терминалу.

После формирования Transaction Data Hash Code карта создает Signed Dynamic Application Data, для чего формирует поля, определенные в таблице 3.

Таблица 3

Имя поля		Длина, байт	Описание
Signed Data Format (формат подписываемых данных)		1	Значение '0x15'
Public Key Algorithm Indicator (индикатор алгоритма подписи)		1	Идентифицирует алгоритм подписи; принимает значение '0x11', соответствующее алгоритму id-tc26-gost3410-2012-256
Public Key Parameters Indicator (индикатор набора параметров алгоритма подписи)		1	Идентифицирует набор параметров алгоритма подписи; принимает значение '0x01', соответствующее id-GostR3410-2001-CryptoPro-A-ParamSet
ICC Dynamic Data Length (длина динамических данных карты)		1	Длина динамических данных в байтах
ICC Dynamic Data (динамические данные карты)	IDN Length	1	Динамические данные, сформированные картой или сохраненные на карте
	IDN	2 — 8	
	CID	1	
	Криптограмма TC, AAC или ARQC	8	
	Transaction Data Hash Code	32	
Unpredictable Number		4	Случайное число, генерируемое терминалом

Затем данные, приведенные в таблице 3, подписываются секретным ключом карты S_{icc} в соответствии с ГОСТ Р 34.10—2012 с длиной ключа порядка 256 бит. После чего формируется Signed Dynamic Application Data согласно таблице 4.

Таблица 4

Имя поля	Длина, байт	Описание
Data Header (заголовок)	1	Значение '0x6A'
Signed Data Format (формат подписываемых данных)	1	Значение '0x15'
Hash Algorithm Indicator (идентификатор алгоритма хэширования)	1	Идентифицирует алгоритм хэширования; принимает значение '0x11', соответствующее алгоритму id-tc26-gost3411-2012-256
Public Key Algorithm Indicator (индикатор алгоритма подписи)	1	Идентифицирует алгоритм подписи; принимает значение '0x11', соответствующее алгоритму id-tc26-gost3410-2012-256
Public Key Parameters Indicator (индикатор набора параметров алгоритма подписи)	1	Идентифицирует набор параметров алгоритма подписи; принимает значение '0x01', соответствующее id-GostR3410-2001-CryptoPro-A-ParamSet

Окончание таблицы 4

Имя поля	Длина, байт	Описание
ICC Dynamic Data Length (длина динамических данных карты)	1	Длина динамических данных в байтах
ICC Dynamic Data (динамические данные карты)	L_{dd}	Динамические данные, сформированные картой или сохраненные на карте
Signature (подпись)	64	Подпись от данных, приведенных в таблице 3, в соответствии с ГОСТ Р 34.10—2012 с длиной ключа порядка 256 бит
Data Trailer	1	'0xBC'

Полученный результат (Signed Dynamic Application Data) направляется терминалу в поле данных ответа на команду GENERATE AC.

Структура поля данных ответа на команду GENERATE AC представлена в таблице 5.

Таблица 5

Имя поля	Тэг	Длина, байт	Описание
CID	'9F27'	1	Определяет тип криптограммы
ATC	'9F36'	2	Счетчик транзакций приложения
Signed Dynamic Application Data	'9F4B'	120	Подписанные критические данные приложения при использовании DDA или CDA
Issuer Application Data	'9F10'	32	Issuer Application Data дает эмитенту информацию о приложении в процессе онлайн-транзакции в авторизационном запросе и, после завершения транзакции, в записях по клирингу

4.3.2 Проверка подписи данных платежного приложения карты терминалом

Проверка терминалом полученного значения Signed Dynamic Application Data выполняется с помощью открытого ключа карты P_{icc}. Для этого:

- извлекается открытый ключ удостоверяющего центра платежной системы;
- верифицируется сертификат открытого ключа эмитента $C_{icc-iss}$ согласно Р 1323565.1.015—2018;
- извлекается открытый ключ эмитента $P_{icc-iss}$;
- верифицируется сертификат открытого ключа карты C_{icc} согласно Р 1323565.1.015—2018;
- извлекается открытый ключ карты P_{icc};
- формируются данные таблицы 3;
- выполняется проверка цифровой подписи (Signature), приведенная в таблице 4, в соответствии с ГОСТ Р 34.10—2012 с длиной ключа порядка 256 бит;
- выполняется проверка элемента «Формат данных» (Signed Data Format), который должен быть равен '0x15';
- производится проверка равенства значений CID, полученных из подписанных данных и из поля данных ответа на команду GENERATE AC;
- производится проверка равенства значений Transaction Data Hash Code, полученных из подписанных данных и вычисленных терминалом самостоятельно на основе имеющихся в его распоряжении значений данных, используемых для вычисления Transaction Data Hash Code.

Карта считается успешно аутентифицированной, когда все проверки завершились успешно. В этом случае терминал запоминает значение IDN для последующей пересылки эмитенту при верификации.

Приложение А
(справочное)

Контрольные примеры

Приводимое ниже значение счетчика АТС, а также значения ключей карты S_{icc}, P_{icc}, мастер-ключ MK_{IDN} рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящих рекомендациях.

Все числовые значения приведены в десятичной или шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления.

В данном приложении двоичные строки из V^*, длина которых кратна 4, записываются в шестнадцатеричном виде, а символ конкатенации («||») опускается. То есть строка $a \in V_{4r}$ будет представлена в виде $a_{r-1}a_{r-2}\dots a_0$, где $a_i \in \{0,1,\dots,9,a,b,c,d,e,f\}, i = 0,1,\dots,r-1$. Соответствие между двоичными строками длины 4 и шестнадцатеричными строками длины 1 задается естественным образом (таблица А.1).

Преобразование, ставящее в соответствие двоичной строке длины 4*r* шестнадцатеричную строку длины *r*, и соответствующее обратное преобразование для простоты записи опускаются.

Таблица А.1 — Соответствие между двоичными и шестнадцатеричными строками

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

А.1 Исходные данные

$$ATC = 0010_{16}$$

$$MK_{IDN} = 4ea368db926da5b101c32d34f0b24803\backslash\backslash 53db104e44dd57df907e00594b299dcd_{16}$$

Закрытый ключ карты:

$$S_{icc} = d92d431d20375cd2a537cd648e14b60b\backslash\backslash 4c21a15a579861b7be419b16ed861874_{16}$$

Открытый ключ карты:

$$P_{icc} = 030654acd14ad85d6b246ec4a195b334\backslash\backslash$$
$$ecfef93c1f22b67cf81ff7d35e8dd618\backslash\backslash$$
$$e538c3b327e93b136697ed5c86173b44\backslash\backslash$$
$$341c5f5b9792e95362170a993d84a472_{16}$$

Символ «\\» обозначает перенос числа на новую строку.

А.1.1 Формирование объекта ICC Dynamic Number (IDN)

С помощью исходных данных и мастер-ключа MK_{IDN}, получается следующее значение IDN:

$$\text{IDN} = f8262238_{16}$$

А.1.2 Динамическая аутентификация платежного приложения

Для динамической аутентификации формируются следующие данные:

$$Data = 1511010504f826223801020304_{16}$$

Для формирования подписи от данных *Data* вычисляется их хэш-код:

$$HashData = 4d2f6846422cea0e25d78af8b5d50546\backslash\backslash$$
$$68cc8d553d45e98f43dd20847003bfee_{16}$$

С помощью случайного числа *k*, равного

$$k = a1f3db706b09f11176c591c6078e19ba\backslash\backslash$$
$$3ab9185944f71661057679400f4886d8_{16}$$

и закрытого ключа карты S_{icc} получается следующее значение подписи от данных *Data*:

$$Sign = 83775ddc8833ac7a67f48daaa807572e\backslash\backslash$$
$$c84cd013bc45d15b8146834b440ac1cb\backslash\backslash$$
$$5b0356cccd0a07d93d7844d6d1a6ca13\backslash\backslash$$
$$c1d118ee5637dcc58789d61f9ba645bf_{16}$$

В итоге получается следующее значение объекта Signed Dynamic Application Data:

$$\text{Signed Dynamic Application Data} = 6a1511010504f8262238\backslash\backslash$$
$$83775ddc8833ac7a67f48daaa807572e\backslash\backslash$$
$$c84cd013bc45d15b8146834b440ac1cb\backslash\backslash$$
$$5b0356cccd0a07d93d7844d6d1a6ca13\backslash\backslash$$
$$c1d118ee5637dcc58789d61f9ba645bf\backslash\backslash$$
$$bc_{16}$$

А.1.3 Комбинированная аутентификация платежного приложения

Для комбинированной аутентификации формируются следующие данные:

$$Data = 1511012e04f8262238\backslash\backslash$$
$$0092122fbe92122fbe\backslash\backslash$$
$$c84cd013bc45d15b8146834b440ac1cb\backslash\backslash$$
$$5b0356cccd0a07d93d7844d6d1a6ca13\backslash\backslash$$
$$01020304_{16}$$

Для формирования подписи от данных *Data* вычисляется их хэш-код:

$$HashData = c1872c6de7596424d8c92ecce260f7f1\\ ff6636b01a88160872f635e0de4e6bd1_{16}$$

С помощью случайного числа *k*, равного

$$k = d5149e302f75abcccbb59525d8cc3348\\ bf3bd942a8b38428171b36f10182ca35_{16}$$

И закрытого ключа карты S_{icc} получается следующее значение подписи от данных *Data*:

$$Sign = f9a8b82ab6205562171c9d8ab82b0b4e\\ 66a28923f01c2399b9d5218956208bfb\\ 0bdc3cbc360fc252cf8a86bb105b7125\\ c0a2776e92bcf099f8a386b1c638b87c_{16}$$

В итоге получается следующее значение объекта Signed Dynamic Application Data:

$$\text{Signed Dynamic Application Data} = 6a1511012e04f8262238\\ 0092122fbe92122fbe\\ c84cd013bc45d15b8146834b440ac1cb\\ 5b0356cccd0a07d93d7844d6d1a6ca13\\ f9a8b82ab6205562171c9d8ab82b0b4e\\ 66a28923f01c2399b9d5218956208bfb\\ 0bdc3cbc360fc252cf8a86bb105b7125\\ c0a2776e92bcf099f8a386b1c638b87c\\ bc_{16}$$

А.2 Исходные данные

$$ATC = 0010_{16}$$

$$MK_{IDN} = 23df44a5dd9e2c755504dc4c736427b8\\ 6478841d8fea535fb09c34a1410f3097_{16}$$

Закрытый ключ карты:

$$S_{icc} = 05050505050505050505050505050505\\ 05050505050505050505050505050505_{16}$$

Открытый ключ карты:

$$P_{icc} = 2221df1866280f2cfd78d2d5f0f4719a\\ caa187bf4fab1d8198ab53c9c800fbf2\\ 4db2a57d9c26c61a886cfa10041566ad\\ 01080083ed2456e5355d7467cbec327d_{16}$$

А.2.1 Формирование объекта ICC Dynamic Number (IDN)

С помощью исходных данных и мастер-ключа MK_{IDN} получается следующее значение IDN:

$$\text{IDN} = 00663246509fd5_{16}$$

А.2.2 Динамическая аутентификация платежного приложения
Для динамической аутентификации формируются следующие данные:

$$Data = 151101080700663246509fd511211308_{16}$$

Для формирования подписи от данных *Data* вычисляется их хэш-код:

$$HashData = 7bff6d3d1e8d9b1916d289e50158f47e\backslash\backslash$$
$$b927e75cc1d1e4bc4dded448889544b4_{16}$$

С помощью случайного числа *k*, равного

$$k = 91ccaa44f9e692abcf7deb01cf8f92c5\backslash\backslash$$
$$b900768bdb7b753be6c1ae94d25a8e46_{16}$$

И закрытого ключа карты S_{icc} получается следующее значение подписи от данных *Data*:

$$Sign = ea90354fee62ab026461cd134791fd1a\backslash\backslash$$
$$d6aa2c6ad6b884f2923ebfece5247cda\backslash\backslash$$
$$cd9863cc78f57b101f6cb725c64d550e\backslash\backslash$$
$$d07f9b601cd1939b28721d249153c152_{16}$$

В итоге получается следующее значение объекта Signed Dynamic Application Data:

$$\text{Signed Dynamic Application Data} = 6a151101080700663246509fd5\backslash\backslash$$
$$ea90354fee62ab026461cd134791fd1a\backslash\backslash$$
$$d6aa2c6ad6b884f2923ebfece5247cda\backslash\backslash$$
$$cd9863cc78f57b101f6cb725c64d550e\backslash\backslash$$
$$d07f9b601cd1939b28721d249153c152\backslash\backslash$$
$$bc_{16}$$

А.2.3 Комбинированная аутентификация платежного приложения
Для комбинированной аутентификации формируются следующие данные:

$$Data = 151101310700663246509fd5\backslash\backslash$$
$$405c75b8ec5c75b8ec\backslash\backslash$$
$$d6aa2c6ad6b884f2923ebfece5247cda\backslash\backslash$$
$$cd9863cc78f57b101f6cb725c64d550e\backslash\backslash$$
$$11211308_{16}$$

Для формирования подписи от данных *Data* вычисляется их хэш-код:

$$HashData = 622dbab100c54abbddf831d14c471345\backslash\backslash$$
$$c9dd37f0e0333c03cb0c0e38843eae88_{16}$$

С помощью случайного числа *k*, равного

$$k = e303ff5cccbf166b14cb2ef8291844e7\backslash\backslash$$
$$3b9d05265586030519a88be1c3c8b4e3_{16}$$

и закрытого ключа карты S_{icc} получается следующее значение подписи от данных *Data*:

$$Sign = d8a0cda7911e3f0d8a3cfe248d0462c2\backslash\backslash$$
$$9c96d1c6501009f69e6c69329c646af7\backslash\backslash$$

$$d3106b5e447b54202b73284cc65d8274\backslash\backslash$$
$$a919bf42607e9ae46ee30a89446d3a73_{16}$$

В итоге получается следующее значение объекта Signed Dynamic Application Data:

$$\text{Signed Dynamic Application Data} = 6a151101310700663246509fd5\backslash\backslash$$
$$405c75b8ec5c75b8ec\backslash\backslash$$
$$d6aa2c6ad6b884f2923ebfece5247cda\backslash\backslash$$
$$cd9863cc78f57b101f6cb725c64d550e\backslash\backslash$$
$$d8a0cda7911e3f0d8a3cfe248d0462c2\backslash\backslash$$
$$9c96d1c6501009f69e6c69329c646af7\backslash\backslash$$
$$d3106b5e447b54202b73284cc65d8274\backslash\backslash$$
$$a919bf42607e9ae46ee30a89446d3a73\backslash\backslash$$
$$bc_{16}$$

A.3 Исходные данные

$$ATC = 0010_{16}$$
$$MK_{IDN} = 326236064be404964d716c47db6b8dab\backslash\backslash$$
$$75d9cb0cb599db240c782db8fa140ac7_{16}$$

Закрытый ключ карты:

$$S_{icc} = 246954f9881d2918f373c01b6d8c9cc0\backslash\backslash$$
$$01563d191078316e8a3ae11741829523_{16}$$

Открытый ключ карты:

$$P_{icc} = 4fc5f57ab09aa6f0f7433edefbb4bcbe\backslash\backslash$$
$$4368d64fcf5ec69452982cfaef61fdc6\backslash\backslash$$
$$ae37764bc9f910905995e92389537ff3\backslash\backslash$$
$$b632938a4a6b8e5d1bee20dee371e258_{16}$$

A.3.1 Формирование объекта ICC Dynamic Number (IDN)

С помощью исходных данных и мастер-ключа MK_{IDN} получается следующее значение IDN:

$$\text{IDN} = b074461b04c6479e_{16}$$

A.3.2 Динамическая аутентификация платежного приложения

Для динамической аутентификации формируются следующие данные:

$$Data = 151101090 8b074461b04c6479e12aa1698_{16}$$

Для формирования подписи от данных *Data* вычисляется их хэш-код:

$$HashData = 06eb19d75d4894d5257993fcd34996c2\backslash\backslash$$
$$b24fa403b07e81f66609da6b0f793d50_{16}$$

С помощью случайного числа *k*, равного

$$k = 15b318cfe252177f9bba5fbfbb418a45\backslash\backslash$$
$$7ca308f25e6a85987ff1e71b9c804933_{16}$$

И закрытого ключа карты S_{icc} получается следующее значение подписи от данных *Data*:

$$Sign = c232895a96827d6d9dab17019ff2e7b2\backslash\backslash$$
$$1995a29d7f956f3c8331f80f765cd941\backslash\backslash$$
$$3a0d0686964425395abcde18b78272cb\backslash\backslash$$
$$3f9bdec417124b514364cd99237ee985_{16}$$

В итоге получается следующее значение объекта Signed Dynamic Application Data:

$$\text{Signed Dynamic Application Data} = 6a1511010908b074461b04c6479e\backslash\backslash$$
$$c232895a96827d6d9dab17019ff2e7b2\backslash\backslash$$
$$1995a29d7f956f3c8331f80f765cd941\backslash\backslash$$
$$3a0d0686964425395abcde18b78272cb\backslash\backslash$$
$$3f9bdec417124b514364cd99237ee985\backslash\backslash$$
$$bc_{16}$$

А.3.3 Комбинированная аутентификация платежного приложения

Для комбинированной аутентификации формируются следующие данные:

$$Data = 1511013208b074461b04c6479e\backslash\backslash$$
$$405c75b8ec5c75b8ec\backslash\backslash$$
$$3a0d0686964425395abcde18b78272cb\backslash\backslash$$
$$c232895a96827d6d9dab17019ff2e7b2\backslash\backslash$$
$$12aa1698_{16}$$

Для формирования подписи от данных *Data* вычисляется их хэш-код:

$$HashData = 676a396f98f92398cc3436fbfc2cb571\backslash\backslash$$
$$7399fcc9b8bb601ff7544fe8b0421875_{16}$$

С помощью случайного числа *k*, равного

$$k = dc4038595ad9e94013ad898665e46617\backslash\backslash$$
$$1a5f4c7cc4cf688e494b67f250cc09ef_{16}$$

и закрытого ключа карты S_{icc} получается следующее значение подписи от данных *Data*:

$$Sign = f881574fdddd25b547e31f17d99bc4e0\backslash\backslash$$
$$e7dee679c9af018fd32d36bf27ab6fb3\backslash\backslash$$
$$0f6d07ff7b1f8c974cca1feb736e6fc4\backslash\backslash$$
$$1309eae6d24f09d90bd3ad1b5e465cb6_{16}$$

В итоге получается следующее значение объекта Signed Dynamic Application Data:

$$\text{Signed Dynamic Application Data} = 6a1511013208b074461b04c6479e\backslash\backslash$$
$$405c75b8ec5c75b8ec\backslash\backslash$$
$$3a0d0686964425395abcde18b78272cb\backslash\backslash$$
$$c232895a96827d6d9dab17019ff2e7b2\backslash\backslash$$

$$f881574fdddd25b547e31f17d99bc4e0\\
e7dee679c9af018fd32d36bf27ab6fb3\\
0f6d07ff7b1f8c974cca1feb736e6fc4\\
1309eae6d24f09d90bd3ad1b5e465cb6\\
bc_{16}$$

УДК 681.3.06:006.354 ОКС 35. 040

Ключевые слова: информационная технология, криптографическая защита информации, оффлайновая аутентификация, электронная подпись, платежная карта, платежное приложение

БЗ 3—2018/54

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

Сдано в набор 06.03.2018. Подписано в печать 21.03.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10. Тираж 20 экз. Зак. 459.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru