ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

**Р 1323565.
1.011—
2017**

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN

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 19 декабря 2017 г. № 2019-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 2
4.1 Процедура зашифрования PIN (терминал) 2
4.2 Процедура расшифрования и верификации PIN (карта) 3
Приложение А (справочное) Контрольные примеры 4

Введение

В настоящих рекомендациях рассмотрен порядок использования алгоритма согласования ключей для аутентификации PIN в офлайновом режиме. Данная процедура выполняется в рамках верификации держателя карты.

Верификация держателя карты производится в целях идентификации лица, получившего карту от ее эмитента (клиента банка), с лицом, совершающим по карте операцию. Данная процедура обработки транзакции выполняется после динамической/комбинированной аутентификации карты терминалом, в процессе которой терминал проверяет сначала сертификат карты, считанный с нее, а затем генерирует случайное число, отправляет его карте для заверения, после чего проверяет полученную в ответ подпись этого случайного числа и служебную информацию. Передача карте в режиме офлайн зашифрованного PIN для верификации выполняется в том случае, если картой и терминалом согласован метод верификации держателя карты "Enciphered PIN verification performed by ICC".

Разработка настоящих рекомендаций вызвана необходимостью внедрения процедур для аутентификации PIN в платежных приложениях.

Примечание — Настоящие рекомендации дополнены приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN

Information technology. Cryptographic data security.
Using key matching and block encryption algorithms in offline PIN verification

Дата введения — 2018—06—01

1 Область применения

Описанные в настоящих рекомендациях алгоритмы рекомендуется применять при проверке PIN 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 34.13—2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

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

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 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 использованы следующие обозначения:

V_n — конечномерное векторное пространство размерности n;

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

$C_{ICC\text{-}PIN}$ — сертификат открытого ключа карты для проверки PIN;

$C_{ICC\text{-}ISS}$ — сертификат эмитента карты;

$D_K(M)$ — функция расшифрования;

$E_K(M)$ — функция зашифрования;

H_{256} — функция хэширования в соответствии с ГОСТ Р 34.11—2015. Длина значения равна 32 байтам;

IUN — случайное число карты (ICC Unpredictable Number), генерируемое картой в ответ на команду GET CHALLENGE в том случае, когда терминал выбирает метод верификации держателя карты Enciphered PIN Offline. Длина значения равна 8 байтам;

KEK_{VKO} — ключ шифрования, формируемый в соответствии с алгоритмом VKO_GOSTR3410_2012_256, описанным в Р 50.1.113—2016. Длина значения равна 32 байтам;

kP — точка эллиптической кривой кратности *k*;

m, *q* — параметры эллиптической кривой id-GostR3410-2001-CryptoPro-A-ParamSet;

PIN — персональный идентификационный номер (Personal identification number) (4—12 десятичных цифр);

PIN-block — данные для вычисления шифрограммы. Длина значения равна 8 байтам.

UKM — фиксированный параметр, значение которого равно UKM = (0x00||0x00||0x00||0x00||0x00||0x00||0x00||0x01). Длина значения равна 8 байтам;

*VKO_GOSTR*3410_2012_256 — алгоритм согласования ключей, определенный в Р 50.1.113—2016;

x — закрытый ключ терминала. Длина значения равна 32 байтам;

xP — открытый ключ терминала. Длина значения равна 64 байтам;

y — закрытый ключ карты. Длина значения равна 32 байтам;

yP — открытый ключ карты. Длина значения равна 64 байтам.

4 Описание алгоритмов

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

4.1 Процедура зашифрования PIN (терминал)

Для зашифрования PIN на стороне терминала необходимо сформировать шифрограмму на основе ключа шифрования KEK_{VKO} и значения*PIN-block.*

Формирование ключа шифрования KEK_{VKO} происходит в соответствии с алгоритмом согласования ключей VKO_GOSTR3410_2012_256, описанным в Р 50.1.113—2016.

Для этого сертификат открытого ключа карты $C_{ICC\text{-}PIN}$ проверяется с использованием раннее считанного с карты сертификата эмитента карты $C_{ICC\text{-}ISS}$. После чего формируется эфемерная ключевая пара терминала: *x* — закрытый ключ терминала и *xP* — открытый ключ терминала в соответствии с ГОСТ Р 34.10—2012.

На основе полученных параметров вычисляется ключ шифрования:

$K(x, y, UKM) = (m/q \cdot UKM \cdot x \bmod q)(yP)$,

$KEK_{VKO}(x, y, UKM) = H_{256}(K(x, y, UKM))$

PIN-block формируется в виде:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

Значение в каждом столбце имеет длину 4 бита.

Значение знаков *PIN-block* определены в таблице 1.

Таблица 1

Знак в *PIN-block*	Имя	Значение
C	Контрольное поле	'2' ('0010'b)
N	Длина PIN	4-битный двоичный номер с допустимыми значениями в двоичном представлении от '0100'b до '1100'b (от 4 до 12 в десятичном представлении)
P	Цифра PIN	4-битное представление цифры PIN с допустимыми значениями в двоичном представлении от '0000'b до '1001'b (от 0 до 9 в десятичном представлении)
P/F	Цифра PIN/заполнитель	Определяется длиной PIN
F	Заполнитель	4-битное двоичное число '1111'b

Для вычисления шифрограммы применяется алгоритм зашифрования согласно ГОСТ 28147—89 в режиме CBC по ГОСТ Р 34.13—2015 с вектором инициализации $IV = 0$ (то же, что и двукратное применение алгоритма шифрования в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z):

$E_{KEK_{VKO}}$ (*IUN*||*PIN-block*)

Полученная шифрограмма и открытый ключ терминала отправляются на карту.

4.2 Процедура расшифрования и верификации PIN (карта)

Перед началом процедуры расшифрования и верификации PIN проверяются значения всех необходимых счетчиков, если хоть одно из них достигло своего предельного значения, то обработка прекращается.

Формирование ключа шифрования KEK_{VKO} происходит в соответствии с алгоритмом согласования ключей VKO_GOSTR3410_2012_256, описанным в Р 50.1.113—2016:

$K(x, y, UKM) = (m/q \cdot \text{UKM} \cdot y \bmod q)(xP)$,

$KEK_{VKO}(x, y, UKM) = H_{256}(K(x, y, UKM))$

С помощью полученного ключа KEK_{VKO} расшифровывается шифрограмма по алгоритму расшифрования согласно ГОСТ 28147—89 в режиме CBC по ГОСТ Р 34.13—2015 с вектором инициализации $IV = 0$ (то же, что и двукратное применение алгоритма расшифрования в соответствии с ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z):

$D_{KEK_{VKO}}$ (*IUN*||*PIN-block*)

После расшифрования и проверки формата *PIN-block* из него извлекается значение PIN, которое сравнивается со значением, хранимым на карте. Если проверка значения *IUN*, формата *PIN-block* или значения PIN выдала неверный результат, то обработка прекращается и происходит возврат ошибки терминалу.

Приложение А
(справочное)

Контрольные примеры

Приводимые ниже значения параметров PIN, *IUN*, а также значения ключей терминала *x*, *xP* и значения ключей карты *y*, *yP* 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 $a_{r-1}\, a_{r-2} \ldots a_0$, где $a_i \in \{0, 1, \ldots, 9, a, b, c, d, e, f\}$, $i = 0, 1, \ldots, r-1$. Соответствие между двоичными строками длины 4 и шестнадцатеричными строками длины 1 задается естественным образом (таблица А.1).

Преобразование, ставящее в соответствие двоичной строке длины $4r$ 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

Для вычисления секретного ключа и последующего шифрования *PIN-block* используются следующие данные:

PIN = 1234567_{10}
IUN = $1d80603c8544c727_{16}$

Закрытый ключ терминала:
x = *d*92*d*431*d*20375*cd*2*a*537*cd*648*e*14*b*60*b*\\
4*c*21*a*15*a*579861*b*7*be*419*b*16*ed*861874$_{16}$
Открытый ключ терминала:
xP = 030654*acd*14*ad*85*d*6*b*246*ec*4*a*195*b*334\\
*ecfef*93*c*1*f*22*b*67*cf*81*ff*7*d*35*e*8*dd*618\\
*e*538*c*3*b*327*e*93*b*136697*ed*5*c*86173*b*44\\
341*c*5*f*5*b*9792*e*95362170*a*993*d*84*a*472$_{16}$

Закрытый ключ карты:
y = 246954*f*9881*d*2918*f*373*c*01*b*6*d*8*c*9*cc*0\\
01563*d*191078316*e*8*a*3*ae*11741829523$_{16}$
Открытый ключ карты:
yP = 4*fc*5*f*57*ab*09*aa*6*f*0*f*7433*edefbb*4*bcbe*\\
4368*d*64*fcf*5*ec*69452982*cfaef*61*fdc*6\\
*ae*37764*bc*9*f*910905995*e*92389537*ff*3\\
*b*632938*a*4*a*6*b*8*e*5*d*1*bee*20*dee*371*e*258$_{16}$

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

А.1.1 Ключ шифрования

Используя исходные данные, формируется ключ шифрования KEK_{VKO}:
KEK_{VKO} = *ae*9*fcf*1983*ffa*8160*ab*8*bff*66*c*78*c*890\\
385496*c*69*db*2*c*035*fd*321*cfec*3*bcf*36*d*$_{16}$

А.1.2 Зашифрование PIN

PIN-block = 271234567*ffffffff*$_{16}$

В результате применения алгоритма зашифрования PIN получится следующее значение шифрограммы:
$E_{KEK_{VKO}}$ (*IUN*||*PIN-block*) = 5*e*227*e*64*f*83*e*8*a*5470*e*03*b*97086*c*4*f*$_{16}$

А.1.3 Расшифрование PIN

С использованием приведенных значений KEK_{VKO} и значения шифрограммы с помощью операции расшифрования воспроизводится исходное значение PIN.

А.2 Исходные данные

Для вычисления секретного ключа и последующего шифрования *PIN-block* используются следующие данные:

PIN = 1234487$_{10}$
IUN = 2*d*82603*c*8544*c*727$_{16}$

Закрытый ключ терминала:
x = 0505050505050505050505050505050505\\
0505050505050505050505050505050505$_{16}$
Открытый ключ терминала:
xP = 2221*df*1866280*f*2*cfd*78*d*2*d*5*f*0*f*4719*a*\\
*caa*187*bf*4*fab*1*d*8198*ab*53*c*9*c*800*fbf*2\\
4*db*2*a*57*d*9*c*26*c*61*a*886*cfa*10041566*ad*\\
01080083*ed*2456*e*5355*d*7467*cbec*327*d*$_{16}$

Закрытый ключ карты:
y = *d*92*d*431*d*20375*cd*2*a*537*cd*648*e*14*b*60*b*\\
4*c*21*a*15*a*579861*b*7*be*419*b*16*ed*861874$_{16}$
Открытый ключ карты:
yP = 030654*acd*14*ad*85*d*6*b*246*ec*4*a*195*b*334\\
*ecfef*93*c*1*f*22*b*67*cf*81*ff*7*d*35*e*8*dd*618\\
*e*538*c*3*b*327*e*93*b*136697*ed*5*c*86173*b*44\\
341*c*5*f*5*b*9792*e*95362170*a*993*d*84*a*472$_{16}$

А.2.1 Ключ шифрования

Используя исходные данные, формируется ключ шифрования KEK_{VKO}:
KEK_{VKO} = 165*e*107572*d*0*cb*10*cd*2*c*43558713*e*181\\
87*a*75*b*3812*b*020*f*00*b*3*d*05166*a*201*e*1*e*$_{16}$

А.2.2 Зашифрование PIN

PIN-block = 271234487*ffffffff*$_{16}$

В результате применения алгоритма зашифрования PIN получится следующее значение шифрограммы:
$E_{KEK_{VKO}}$ (*IUN*||*PIN-block*) = *ee*8*f*229*bc*105*f*29039*b*7*af*06*e*0058*d*59$_{16}$

А.2.3 Расшифрование PIN

С использованием приведенных значений KEK_{VKO} и значения шифрограммы с помощью операции расшифрования воспроизводится исходное значение PIN.

А.3 Исходные данные

Для вычисления секретного ключа и последующего шифрования *PIN-block* используются следующие данные:

PIN = 1234347$_{10}$
IUN = 3*d*82603*c*8544*c*727$_{16}$

Закрытый ключ терминала:
x = 246954f9881d2918f373c01b6d8c9cc0\\
01563d191078316e8a3ae11741829523$_{16}$
Открытый ключ терминала:
xP = 4fc5f57ab09aa6f0f7433$e$de$fbb4$bcbe$\\
4368d64fcf5ec69452982$cfaef$61fdc6\\
ae37764bc9f910905995e92389537ff3\\
b632938a4a6b8e5d1bee20dee371e258$_{16}$
Закрытый ключ карты:
y = 0505050505050505050505050505050505\\
0505050505050505050505050505050505$_{16}$
Открытый ключ карты:
yP = 2221df1866280f2cfd78d2d5f0f4719a\\
caa187bf4fab1d8198ab53c9c800fbf2\\
4db2a57d9c26c61a886cfa10041566ad\\
01080083ed2456e5355d7467$cbec$327d_{16}

А.3.1 Ключ шифрования

Используя исходные данные, формируется ключ шифрования KEK_{VKO}:
KEK_{VKO} = b6da0eeb6cbc0ca99b20$c$becadcb6e75\\
b77ee8e318e1eba28ada53c8d7086363$_{16}$

А.3.2 Зашифрование PIN

PIN-$b$lock = 271234567$fffffff_{16}$

В результате применения алгоритма зашифрования PIN получится следующее значение шифрограммы:
$E_{KEK_{VKO}}$ (IUN||PIN-block) = 5c8e839b19e2031c01352611c2d2a379$_{16}$

А.3.3 Расшифрование PIN

С использованием приведенных значений KEK_{VKO} и значения шифрограммы с помощью операции расшифрования воспроизводится исходное значение PIN.

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификация, ключ, функция хэширования, шифрование PIN, верификация PIN, платежное приложение, платежная карта

БЗ 1—2018/95

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 20.12.2017. Подписано в печать 13.02.2018. Формат 60 × 84$^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 19 экз. Зак. 103.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru
Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001, Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru