ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.007— 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения 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. № 2015-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 алгоритмов 2
4.1 Алгоритм формирования проверочного параметра карты [CVP (iCVP, CVP2)] 2
4.2 Алгоритм формирования проверочного значения PIN (PVV) 3
Приложение А (справочное) Контрольные примеры 4

Введение

В настоящих рекомендациях рассмотрены алгоритмы формирования значений CVP, который используется для проверки подлинности карты «МИР», и PVV, необходимого для проверки значения PIN при онлайновой аутентификации.

Разработка настоящих рекомендаций вызвана необходимостью внедрения процедур для формирования проверочных параметров карты в платежных приложениях.

Примечание — Настоящие рекомендации дополнены приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN

Information technology. Cryptographic data security.
Using block encryption algorithms in generation of a payment card verification parameter and PIN verification value

Дата введения — 2018—06—01

1 Область применения

Описанные в настоящих рекомендациях алгоритмы рекомендуется применять при формировании проверочного параметра платежной карты (CVP) и проверочного значения PIN (PVV) в платежной системе «МИР».

CVP формируется при эмиссии карты. Проверка CVP выполняется при проведении транзакций по магнитной полосе, проверке чиповых карт в моде магнитной полосы (iCVP) и/или в транзакциях электронной коммерции путем сравнения сформированного и переданного значения CVP (CVP2).

PVV формируется при эмиссии карты. При онлайновой проверки PIN, во время получения эмитентом операции, в которой присутствует криптограмма PIN, выполняется его проверка путем формирования и сравнения PVV на основании данных, считанных с карты «МИР» (*PAN, PVKI*), и ключа *PVK* на хосте эмитента.

2 Нормативные ссылки

В настоящих рекомендациях использована нормативная ссылка на следующий стандарт:

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

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 **эмитент:** Банк, выпустивший платежную карту.

3.1.2 **держатель карты:** Лицо, на имя которого выпущена платежная карта.

3.2 Обозначения

В настоящих рекомендациях используют 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 $A||B = (a_{n1-1}, a_{n1-2}, ..., a_0, b_{n2-1}, b_{n2-2}, ..., b_0) \in V_{n1+n2}$;

$\oplus$ — покоординатное сложение по модулю 2;

0 ... 0h — дополнение десятичными нулями последовательности до тех пор, пока ее длина не станет равной 16.

CVK — ключ карты для вычисления CVP при эмиссии карт и проверке транзакций по магнитной полосе и в электронной коммерции. Ключ генерируется в HSM с помощью ФДСЧ и хранится в зашифрованном виде в базе данных (БД) хоста эмитента. Длина значения равна 32 байтам;

CVP — проверочный параметр платежной карты (Card Verification Parameter). Длина значения равна трем десятичным цифрам;

CVP2 — проверочный параметр карты, который размещен на оборотной стороне карты и использован для выполнения платежных операций без предъявления карты (вычисляется аналогично вычислению CVP). Длина значения равна трем десятичным цифрам;

$E_K(M)$ — функция зашифрования;

iCVP — проверочный параметр карты, который размещен на чипе карты в составе track2 Equivalent Data и использован при проведении транзакций по чиповым картам в моде магнитной полосы (вычисляется аналогично вычислению CVP). Длина значения равна трем десятичным цифрам;

PAN — номер карты (Primary Account Number). Длина значения равна от 12 до 20 десятичных цифр;

PAN_11 — последние 11 десятичных цифр *PAN*, исключая проверочный символ;

PAN_16 — первые 16 десятичных цифр *PAN*. Если значение *PAN* менее 16, то дополняется нулями. Длина значения равна 16 десятичным цифрам;

PIN — персональный идентификационный номер (Personal identification number). Длина значения равна от 4 до 12 десятичных цифр;

PIN_4 — четыре первые десятичные цифры PIN;

PVK — ключ карты для вычисления PVV при эмиссии карт и проверке транзакций по магнитной полосе. Ключ генерируется в HSM с помощью ФДСЧ и хранится в зашифрованном виде в БД хоста эмитента. Длина значения равна 32 байтам;

PVKI — индекс ключа проверки PIN (PIN verification key index). Цифра в интервале 0 ... 6;

PVV — проверочное значение PIN (PIN Verification Value). Длина значения равна четырем десятичным цифрам;

SVC — сервисный код (Service code). Длина значения равна трем десятичным цифрам;

YYMM — срок действия карты. Длина значения равна четырем десятичным цифрам, причем первые две цифры соответствуют году, а две последние — месяцу.

4 Описание алгоритмов

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

4.1 Алгоритм формирования проверочного параметра карты [CVP (iCVP, CVP2)]

Для получения значения CVP (iCVP, CVP2) изначально вычисляют значение двух блоков:

- первый блок состоит из 16 шестнадцатеричных символов, который формируется по правилу *Block*1 = *PAN_16;*

- второй блок также состоит из 16 шестнадцатеричных символов и формируется по правилу:

Block2 = (*YYMM*||*SVC*||0 ... 0*h*), если длина *PAN* менее или равна 16.

Если длина более 16, то:

Block2 = (не вошедшие в первый блок цифры *PAN*||*YYMM*||*SVC*||0 ... 0*h*),

где *SVC* принимает значения 000 (для вычисления значения CVP2), 999 (для вычисления значения iCVP) или одно из значений, приведенных в таблице 1 (для вычисления значения CVP).

Таблица 1

Позиция	Значение	Описание
1	2	Карта с микропроцессором для трансграничных операций
2	0	Ограничений на способ авторизации транзакции нет, в частности операция может быть обслужена в офлайновом режиме
	2	Операция по карте обязательно авторизуется эмитентом в режиме реального времени
3	0	Любая услуга и обязательная верификация держателя карты по PIN (No restrictions and PIN Required)
	1	Любая услуга и любой метод верификации держателя карты (No restrictions)

Далее значение первого блока зашифровывается с помощью алгоритма шифрования по ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z с использованием ключа *CVK*:

$Block1 = E_{CVK}(Block1)$.

После чего покоординатно складывается по модулю 2 со значением второго блока:

$Block2 = Block1 \oplus Block2$.

Полученный результат снова зашифровывается с помощью алгоритма шифрования по ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z с использованием ключа *CVK*:

$E_{CVK}(Block2)$.

Полученная двоичная последовательность интерпретируется как натуральное число. Значение CVP (iCVP, CVP2) полагается равным остатку от деления данного числа на 1000. Соответствие между двоичной последовательностью и натуральным числом задается естественным образом.

4.2 Алгоритм формирования проверочного значения PIN (PVV)

Для вычисления PVV последовательность (*PAN*_11||*PVKI*||*PIN*_4), состоящая из шестнадцатеричных символов, зашифровывается с помощью алгоритма шифрования ГОСТ 28147—89 в режиме простой замены с узлом замены id-tc26-gost-28147-param-Z с использованием ключа *PVK*.

Полученная двоичная последовательность интерпретируется как натуральное число. Значение PVV полагается равным остатку от деления данного числа на 10 000. Соответствие между двоичной последовательностью и натуральным числом задается естественным образом.

Приложение А
(справочное)

Контрольные примеры

Приводимые ниже значения параметров PIN, *PAN*, *PVKI*, срока действия карты, а также значения ключей *CVK*, *PVK* 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. Представление числа из десятичной системы счисления в шестнадцатеричный вид происходит по следующему правилу: каждая цифра десятичного числа переводится в одну цифру шестнадцатеричного числа. Например, целое число 1213456789_{10} представляется в шестнадцатеричном виде, как число 1213456789_{16}. Соответствие между десятичными и шестнадцатеричными цифрами задается естественным образом (таблица А.1).

В данном приложении двоичные строки из V^*, длина которых кратна 4, записаны в шестнадцатеричном виде, а символ конкатенации («||») опускают. 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 опускают.

Таблица А.1 — Соответствие между числами в двоичной, шестнадцатеричной и десятичной системе счисления

Число в двоичной системе счисления	Число в шестнадцатеричной системе счисления	Число в десятичной системе счисления
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	a	10
1011	b	11
1100	c	12
1101	d	13
1110	e	14
1111	f	15

А.1 Исходные данные

Для вычисления проверочного значения карты (CVP) и проверочного значения PIN (PVV) используют следующие данные:

PIN = 1234567_{10}
PAN = $1234567890123456 71_{10}$
Срок действия карты: *YYMM* = 1704_{10}

Сервисный код: $SVC = 999_{10}$
$PVKI = 5_{10}$
Ключ карты для вычисления значения CVP:
$CVK = 0102030405060708111213141516171 8\backslash\backslash$
$212223242526272831323334353637 38_{16}$
Ключ карты для вычисления значения PVV:
$PVK = 0102030405060708111213141516171 8\backslash\backslash$
$212223242526272831323334353637 38_{16}$
Символ «\\» обозначает перенос числа на новую строку.

А.1.1 Вычисление значения CVP

$Block1 = 1234567890123456_{10} = 1234567890123456_{16}$
$Block2 = 7117049990000000_{10} = 7117049990000000_{16}$

В результате работы алгоритма вычисления проверочного значения карты (CVP) получится следующее значение шифрограммы $06128a1bd2a9f966_{16}$, что соответствует натуральному числу 437563965911464294.
Тогда значение CVP будет равно:
$CVP = 294_{10}$

А.1.2 Вычисление значения PVV

$(PAN_11||PVKI||PIN_4) = 7890123456751234_{10} = 7890123456751234_{16}$

В результате работы алгоритма вычисления проверочного значения PIN (PVV) получится следующее значение шифрограммы: $deedf3b7ba3e5caf_{16}$, что соответствует натуральному числу 16063763416329641135.
Тогда значение PVV будет равно:
$PVV = 1135_{10}$

А.2 Исходные данные

Для вычисления проверочного значения карты (CVP) и проверочного значения PIN (PVV) используют следующие данные:
$PIN = 1234_{10}$
$PAN = 6789012345673_{10}$
Срок действия карты: $YYMM = 1912_{10}$
Сервисный код: $SVC = 201_{10}$
$PVKI = 1_{10}$
Ключ карты для вычисления значения CVP:
$CVK = 000102030405060708090a0b0c0d0e0f\backslash\backslash$
$101112131415161718191a1b1c1d1e21_{16}$
Ключ карты для вычисления значения PVV:
$PVK = 3b8fd0a39151b2fba7ad72ca7fbda0ad\backslash\backslash$
$62ce02d74ae00e3aff24b2221b5f83ca_{16}$

А.2.1 Вычисление значения CVP

$Block1 = 6789012345673000_{10} = 6789012345673000_{16}$
$Block2 = 1912201000000000_{10} = 1912201000000000_{16}$

В результате работы алгоритма вычисления проверочного значения карты (CVP) получится следующее значение шифрограммы: $4c9020058f537db7_{16}$, что соответствует натуральному числу 5516944751780396471.
Тогда значение CVP будет равно:
$CVP = 471_{10}$

А.2.2 Вычисление значения PVV

$(PAN_11||PVKI||PIN_4) = 7890123456711234_{10} = 7890123456711234_{16}$

В результате работы алгоритма вычисления проверочного значения PIN (PVV) получится следующее значение шифрограммы: $37c81b3e0eba2c56_{16}$, что соответствует натуральному числу 4019492620777172054.
Тогда значение PVV будет равно:
$PVV = 2054_{10}$

А.3 Исходные данные

Для вычисления проверочного значения карты (CVP) и проверочного значения PIN (PVV) используют следующие данные:
$PIN = 010203040506_{10}$
$PAN = 98765432112341_{10}$
Срок действия карты: $YYMM = 2001_{10}$

Сервисный код: $SVC = 000_{10}$

$PVKI = 0_{10}$

Ключ карты для вычисления значения CVP:

$CVK = 000102030405060708090a0b0c0d0e0f\backslash\backslash$
$101112131415161718191a1b1c1d1e33_{16}$

Ключ карты для вычисления значения PVV:

$PVK = 000102030405060708090a0b0c0d0e0f\backslash\backslash$
$101112131415161718191a1b1c1d1e24_{16}$

А.3.1 Вычисление значения CVP

$Block1 = 9876543211234100_{10} = 9876543211234100_{16}$

$Block2 = 2001000000000000_{10} = 2001000000000000_{16}$

В результате работы алгоритма вычисления проверочного значения карты (CVP) получится следующее значение шифрограммы: $1843ed76f2da2f95_{16}$, что соответствует натуральному числу 1748502175486193557.

Тогда значение CVP будет равно:

$CVP = 557_{10}$

А.3.2 Вычисление значения PVV

$(PAN_11||PVKI||PIN_4) = 7654321123410102_{10} = 7654321123410102_{16}$

В результате работы алгоритма вычисления проверочного значения PIN (PVV) получится следующее значение шифрограммы: $7bf5bc5c796ce20c_{16}$, что соответствует натуральному числу 8932252541319438860.

Тогда значение PVV будет равно:

$PVV = 8860_{10}$

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификация, ключ, платежная карта, платежное приложение, проверочное значение PIN, проверочный параметр платежной карты

БЗ 1—2018/91

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
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. 99.

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