Регламент работы с криптографическими ключами Hardware Security Module (HSM)

Москва 2015

1. Общие положения

1.1. Определения и обозначения

Компрометация ключа: Утрата доверия к тому, что используемый криптографический ключ обеспечивает безопасность информации; констатация владельцем криптографического ключа обстоятельств, при которых возможно несанкционированное использование, либо подозрение на несанкционированное использование его криптографического ключа неуполномоченными лицами. К событиям, связанным с компрометацией криптографических ключей, в том числе, относятся:

- утрата носителей криптографического ключа;
- увольнение сотрудников, имевших доступ к криптографическому ключу;
- временный доступ посторонних лиц к криптографическому ключу;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к криптографическому ключу третьих или неуполномоченных лиц.

Криптограмма: Зашифрованные с помощью криптографического преобразования данные.

Криптографический ключ: Уникальная последовательность символов, предназначенная для преобразования данных при помощи криптографического алгоритма.

Криптографическое преобразование: Преобразование данных при помощи криптографического алгоритма.

Офицер безопасности АО «НСПК»: Физическое лицо, являющееся работником АО «НСПК», назначаемое приказом и уполномоченное производить следующие действия:

- внедрение и сопровождение системы генерации криптографических ключей для HSM АО «НСПК» (далее по тексту «Система HSM АО «НСПК»);
- контроль и обнаружение различных угроз, которым подвергается Система HSM АО «НСПК» и ее информационные ресурсы, а также реагирование на эти угрозы в реальном масштабе времени;
- выполнять административные мероприятия по установке, настройке и поддержке в работоспособном состоянии средств криптографической защиты информации, эксплуатируемых в Системе HSM АО «НСПК», включая работу с криптографическими ключами.

Офицер безопасности Участника: Физическое лицо, являющееся работником Кредитной организаций-участник, назначаемое приказом, либо иное уполномоченное ею лицо и уполномоченное производить следующие действия:

- внедрение и сопровождение системы генерации криптографических ключей для HSM Участника (далее по тексту «Система»);
- контроль и обнаружение различных угроз, которым подвергается Система и ее информационные ресурсы, а также реагирование на эти угрозы в реальном масштабе времени;
- выполнять административные мероприятия по установке, настройке и поддержке в работоспособном состоянии средств криптографической защиты информации, эксплуатируемых в Системе, включая работу с криптографическими ключами.

ОПКЦ НСПК: Операционный центр и платежный клиринговый центр национальной системы платежных карт.

Транспортный ключ (ZMK – Zone Master Key): Криптографический ключ, предназначенный для безопасной передачи ключей шифрования ПИН-блоков в рамках процедуры обмена ими между операционными центрами Участников и ОПКЦ НСПК. Генерируется и передается АО «НСПК» уполномоченным представителям операционных центров Участников.

Ключ шифрования ПИН-блоков (ZPK – Zone PIN Key): Криптографический ключ, предназначенный для безопасной передачи ПИН-блоков между операционными центрами Участников и ОПКЦ НСПК. Генерируется и передается АО «НСПК» уполномоченным представителям операционных центров Участников.

HSM: Аппаратный криптографический модуль (Hardware Security Module), криптографическое средство шифрования информации и управления ключами.

1.2. Область применения

Регламент работы с криптографическими ключами Hardware Security Module (HSM) (далее по тексту «Регламент») определяет взаимодействие между АО «НСПК» и Кредитной организаций-участником (далее по тексту «Участник»), присоединившейся к Правилам оказания операционных услуг и услуг платежного клиринга АО «НСПК» (далее по тексту «Правила ОПКЦ НСПК»), в части работы с транспортными ключами (т.н. ZMK –Zone Master Key) и ключами шифрования ПИН-блоков (т.н. ZPK – Zone PIN Key).

1.3. Назначение документа

Настоящий Регламент определяет порядок работы с транспортными ключами и ключами шифрования ПИН-блоков после присоединения Участника к Правилам ОПКЦ НСПК, а также

особенности применяемых ОПКЦ НСПК процедур, реализация которых потребует проведения Участниками организационных и технических мероприятий.

1.4. Внесение изменений в Регламент

Внесение изменений (дополнений) в настоящий Регламент, включая приложения к нему, производится АО «НСПК» в одностороннем порядке.

Новая версия настоящего Регламента с уведомлением о внесении изменений (дополнений) рассылается офицерам безопасности Участников.

Все изменения (дополнения), вносимые в настоящий Регламент, вступают в силу и становятся обязательными с даты уведомленияУчастников.

Любые изменения (дополнения), вносимые в настоящий Регламент, распространяются на всех Участников, присоединившихся к Правилам ОПКЦ НСПК, в том числе, ранее даты вступления изменений (дополнений) в силу.

2. Порядок управления криптографическими ключами HSM, выданными Участнику

2.1. Порядок назначение офицеров безопасности Участника

Участник либо уполномоченное им лицо назначает офицеров безопасности из числа своих сотрудников (не менее трех человек), которым предоставляется право получения чистой компоненты транспортного ключа и криптограмм ключей шифрования ПИН-блоков.

Участник либо уполномоченное им лицо в рамках процедуры подачи документов для присоединения к Правилам ОПКЦ НСПК направляет письмо со сведениями о лицах, которым предоставлено право работать с электронными документами, информация в которых защищена с использованием средств криптографической защиты информации, с полномочиями получения чистой компоненты транспортного ключа и (или) получения криптограмм ключей шифрования ПИН-блоков.

2.2. Процедура генерации и получения криптографических ключей для HSM

1. В случае положительного результата рассмотрения комплекта документов, представленных Участником в АО «НСПК» в соответствии с Правилами ОПКЦ НСПК, АО «НСПК» в соответствии с внутренним порядком осуществляет генерацию транспортного ключа и криптограмм ключей шифрования ПИН-блоков (рабочих ключей) для Участника.

2. В результате генерации транспортного ключа для Участника формируются три ПИН-конверта с его компонентами. В АО «НСПК» остается криптограмма данного ключа.

3. Каждый сформированный ПИН-конверт с двумя экземплярами Акта приема-передачи ПИН-конверта, оформленного в соответствии с Приложением 1 к настоящему Регламенту, упаковывается в отдельный сейф-пакет (конверт с контролем вскрытия).

4. АО «НСПК» генерирует криптограммы 3-х рабочих ключей (две для платежной системы Visa и одну для платежной системы MasterCard) для Участника, полученные на транспортном ключе, выдаваемого Участнику.

5. Зашифрованные рабочие ключи (криптограммы ключей шифрования ПИН-блоков) направляются АО «НСПК» на электронный адрес офицеров безопасности Участника, которым предоставлено право получения этих криптограмм.

6. АО «НСПК» направляет письмо с сейф-пакетом заказным почтовым отправлением с уведомлением о вручении, либо курьерской службой с пометкой «лично» каждому из трех офицеров безопасности Участника, либо передает офицеру безопасности Участника лично. Каждое такое письмо отправляется разными почтовыми (курьерскими) службами или, как минимум, разными рейсами одной почтовой службы.

7. В этом же письме в адрес офицеров безопасности Участника, которым предоставлено право получения криптограмм рабочих ключей, направляются два экземпляра Акта приема-передачи этих криптограмм, сборки транспортного кдюча и установки рабочих ключей, оформленного в соответствии с Приложением 2 к настоящему Регламенту, либо экземпляры актов передаются им лично.

8. Факт получения сейф-пакета с вложенным ПИН-конвертом, содержащим компоненту транспортного ключа, целостность сэйф-пакета и ПИН-конверта подтверждается собственноручной подписью офицера безопасности Участника в Акте приема-передачи ПИН-конверта, который он обязан направить в АО «НСПК» заказным почтовым отправлением с уведомлением о вручении, либо курьерской службой, либо передать АО «НСПК» лично.

9. Факт получения зашифрованных рабочих ключей, корректной сборки транспортного ключа, установки рабочих ключей в Систему подтверждается подписанием офицерами безопасности Участника Акта приема-передачи криптограмм рабочих ключей, сборки транспортного ключа и установки рабочих ключей. Участник обязан оформить и направить один экземпляр акта в АО «НСПК» заказным почтовым отправлением с уведомлением о вручении, либо курьерской службой, либо передать АО «НСПК» одним из офицеров безопасности Участника лично.

10. В случае непредставления офицерами безопасности Участника в АО «НСПК» оформленных в установленном порядке актов или, по крайней мере, их скан-копий на электронный адрес «officer@nspk.ru» в течение 10 рабочих дней с момента получения офицерами безопасности Участника всех трех компонент транспортного ключа, криптографические ключи, выданные Участнику и по которым не были получены соответствующие акты, будут считаться скомпрометированными.

2.3. Аннулирование действия криптографических ключей HSM

Аннулирование действия криптографических ключей HSM означает прекращение использование транспортного ключа и ключей шифрования ПИН-блоков, выданных Участнику, при взаимодействии операционного центра Участника с ОПКЦ НСПК.

Аннулирование действия криптографических ключей HSM осуществляется в следующих случаях:

- по письму Участника в АО «НСПК» с «Заявлением на аннулирование действия криптографических ключей HSM» (далее «Заявление») с указанием причины аннулирования, оформленному в соответствии с Приложением 3 к настоящему Регламенту;
- по истечению срока действия криптографического ключа HSM;
- по предоставлению в АО «НСПК» неопровержимых доказательств нарушения Правил ОПКЦ НСПК;
- при компрометации криптографических ключей Системы HSM АО «НСПК»;
- приостановление оказания Участнику операционных услуг и (или) услуг платежного клиринга ОПКЦ НСПК в соответствии с Правилами ОПКЦ НСПК.

В случае принятия решения по Заявлению АО «НСПК» информирует об этом офицеров безопасности Участника по контактному телефону или электронной почте не позднее 1 (одного) рабочего дня, следующего за рабочим днем, в течение которого было зарегистрировано Заявление.

В случае аннулирования по истечении срока действия криптографического ключа офицер безопасности Участника по контактному телефону или электронной почте информирует об офицеров безопасности АО «НСПК».

В случае приостановления оказания Участнику операционных услуг и (или) услуг платежного клиринга ОПКЦ НСПК, АО «НСПК» аннулирует действие всех криптографических ключей HSM для Участника.

В иных случаях АО «НСПК» направляет Участнику официальное письмо об аннулировании действия криптографических ключей HSM с указанием причины аннулирования выданных ему криптографических ключей.

2.4. Плановая смена криптографических ключей HSM

Процедура плановой смены криптографического ключа HSM осуществляется АО «НСПК». Процедура должна быть инициирована Участником за 1 месяц до истечения срока действия

криптографического ключа HSM и выполняется в два этапа – генерация новых криптографических ключей и аннулирование старых криптографических ключей в соответствии с подразделами 2.2 и 2.3 настоящего Регламента соответственно.

2.5. Внеплановая смена криптографических ключей HSM

Внеплановая смена криптографических ключей HSM осуществляется в следующих случаях:

- при компрометации криптографического ключа HSM;
- при компрометации криптографических ключей Системы HSM АО «НСПК»;
- в случае если Участник по каким-либо причинам не смог осуществить плановую смену криптографического ключа HSM в установленные для этой процедуры сроки;
- в иных случаях, вызванных форс-мажорными обстоятельствами.

Участник направляет в АО «НСПК» письмо с «Заявлением на внеплановую смену криптографических ключей HSM» с указанием причин внеплановой смены, оформленное в соответствии с Приложением 4 к настоящему Регламенту.

Внеплановая смена криптографических ключей HSM выполняется в два этапа – генерация новых криптографических ключей и аннулирование старых криптографических ключей в соответствии с подразделами 2.2 и 2.3 настоящего Регламента соответственно.

2.6. Компрометация криптографических ключей HSM

В случае компрометации ключей HSM офицеры безопасности Участник любым доступным способом уведомляет офицеров безопасности АО «НСПК» о факте компрометации криптографических ключей и направляет в АО «НСПК» письмо с «Заявлением на внеплановую смену криптографических ключей HSM» с указанием причин внеплановой смены – компрометация.

При компрометации транспортного ключа также считается скомпрометированными рабочие ключи, выданные Участнику.

При компрометации криптографических ключей HSM проводится процедура внеплановой смены криптографических ключей HSM в соответствии с подразделом 2.5 настоящего Регламента.

2.7. Сроки действия криптографических ключей HSM

Срок действия транспортного ключа и ключа шифрования ПИН-блоков, выданных Участнику, одинаковый и составляет 2 (два) года.

Период действия криптографических ключей HSM начинается с даты и времени их генерации.

Приложение 1

Шаблон Акта приема-передачи ПИН-конверта

00.00.0000

(дата)

АКТ[1]

приема-передачи ПИН-конверта с компонентой

транспортного ключа для Hardware Security Module (HSM)

Настоящий Акт приема-передачи составлен в том, что офицером безопасности Акционерного общества «Национальная система платежных карт» (далее АО «НСПК»):

Главный специалист Управления Безопасности И.И. Иванов (пример)

(должность, И.О. Фамилия)

в целях исполнения Правил оказания операционных услуг и услуг платежного клиринга АО «НСПК» направил сейф-пакет (конверт с контролем вскрытия), содержащий ПИН-конверт с частью транспортного ключа для HSM, офицеру безопасности:

Открытого акционерного общества «Банк» (далее ОАО «Банк»),

(название организации (краткое наименование), ИНН)

ИНН 1234567890 (пример)

Информация по транспортному ключу (далее ZMK):

Срок действия ZMK	00.00.0000	Номер части ZMK (компонента)	1 из 3
Идентификационный номер ZMK	0000		

Офицер безопасности

ОАО «Банк»

(краткое наименование организации)

Специалист Безопасности П.П. Петров

(должность, И.О. Фамилия)

- получил сейф-пакет, содержащий ПИН-конверт с компонентой ZMK;
- удостоверился в том, что целостность сейф-пакета и ПИН-конверта не нарушена.

[1] Один экземпляр Акта приема-передачи, подписанный офицером безопасности, должен быть предоставлен в АО «НСПК» в течение 10 рабочих дней.

Настоящий Акт приема-передачи составлен в 2-х экземплярах, один из которых хранится в АО «НСПК, а второй - в *ОАО «Банк»*

(краткое наименование организации)

От АО «НСПК»

От ОАО «Банк»

(краткое наименование организации)

_____ И.И. Иванов

_____ П.П. Петров

Приложение 2

Шаблон Акта приема-передачи криптограмм рабочих ключей, сборки транспортного ключа и установки рабочих ключей

00.00.0000

(дата)

АКТ[2]

приема-передачи криптограмм рабочих ключей, сборки транспортного ключа и установки рабочих ключей для Hardware Security Module (HSM)

Настоящий Акт составлен в том, что офицером безопасности Акционерного общества «Национальная система платежных карт» (далее АО «НСПК»):

Главный специалист Операционного департамента И.И. Иванов (пример)

(должность, И.О. Фамилия)

в целях исполнения Правил оказания операционных услуг и услуг платежного клиринга АО «НСПК» направлены криптограммы рабочих ключей для HSM офицерам безопасности:

Открытого акционерного общества «Банк» (далее ОАО «Банк»),

(название организации (краткое наименование), ИНН)

ИНН 234567890 (пример)

Информация по рабочим ключам (далее РК):

1. Visa AWK (Acquire Working Key)

Срок действия РК Visa AWK	00.00.0000
Идентификационный номер РК Visa AWK	0000

2. Visa IWK (Issuer Working Key)

Срок действия РК Visa IWK	00.00.0000
Идентификационный номер РК Visa IWK	0000

3. MasterCard CIS

Срок действия РК MasterCard CIS	00.00.0000
Идентификационный номер РК MasterCard CIS	0000

Офицеры безопасности *ОАО «Банк»*

(краткое наименование организации)

[2] Один экземпляр Акта приема-передачи, подписанный офицерами безопасности, должен быть предоставлен в АО «НСПК» в течение 10 рабочих дней.

Специалист ИТ-службы П.П. Петров

(должность, И.О. Фамилия)

Специалист Безопасности А.А. Сидоров

(должность, И.О. Фамилия)

получили криптограммы указанных рабочих ключей.

В целях исполнения Правил оказания операционных услуг и услуг платежного клиринга АО «НСПК» офицеры безопасности:

ОАО «Банк»

(краткое наименование организации)

Специалист ИТ-службы П.П. Петров

(должность, И.О. Фамилия)

Специалист Безопасности А.А. Сидоров

(должность, И.О. Фамилия)

Специалист Департамента платежных карт В.В. Васичкин

(должность, И.О. Фамилия)

собрали транспортный ключ и установили рабочие ключи в Систему, криптограммы которых были переданы офицером безопасности АО «НСПК».

Настоящий Акт составлен в 2-х экземплярах, один из которых хранится в АО «НСПК, а второй - в _____ .

От АО «НСПК»

_____ И.И. Иванов

От ОАО «Банк»

_____

(краткое наименование организации)

_____ П.П. Петров

_____А.А. Сидоров

_____В.В. Васичкин

Приложение 3

Форма Заявления на аннулирование действия криптографических ключей Hardware Security Module (HSM)

_____
(полное наименование организации, включая организационно-правовую форму)

В связи с _____
(причина аннулирования ключей)

просим аннулировать транспортный ключ (ZMK) HSM:

Идентификационный номер ZMK	0000

и (или) аннулировать ключи шифрования ПИН-блоков (рабочие ключи HSM - РК):

Идентификационный номер РК Visa AWK	0000
Идентификационный номер РК Visa IWK	0000
Идентификационный номер РК MasterCard CIS	0000

Руководитель организации _____ _____
(подпись) (фамилия, имя, отчество)

« » _____ 20 ___ г.

М.П.

(заполняется офицерами безопасности АО «НСПК»)

Настоящим подтверждается, что офицеры безопасности АО «НСПК» приняли Заявление на аннулирование действия криптографических ключей HSM с указанным(и) идентификационным(и) номером(ами). Аннулирование действия указанных ключей HSM произведено.

Офицер безопасности АО «НСПК» _____ _____
(Подпись) (И.О. Фамилия)

Офицер безопасности АО «НСПК» _____ _____
(Подпись) (И.О. Фамилия)

Офицер безопасности АО «НСПК» _____ _____
(Подпись) (И.О. Фамилия)

_____
(Дата)

Приложение 4

Форма Заявления на внеплановую смену криптографических ключей Hardware Security Module (HSM)

_____
(полное наименование организации, включая организационно-правовую форму)

В связи с _____
(причина внеплановой смены криптографических ключей)

Просим организовать внеплановую смену транспортного ключа (ZMK) HSM:

Идентификационный номер ZMK	0000

и (или) внеплановую смену ключей шифрования ПИН-блоков (рабочих ключей HSM - РК):

Идентификационный номер РК Visa AWK	0000
Идентификационный номер РК Visa IWK	0000
Идентификационный номер РК MasterCard CIS	0000

Руководитель организации _____ _____
(подпись) (фамилия, имя, отчество)

« » _____ 20 __ г.

М.П.

(заполняется офицерами безопасности АО «НСПК»)

Настоящим подтверждается, что офицеры безопасности АО «НСПК» приняли Заявление на внеплановую смену криптографических ключей HSM с указанным(и) идентификационным(и) номером(ами). Внепланова смена указанных ключей HSM произведена.

Офицер безопасности АО «НСПК» _____ _____
(Подпись) (И.О. Фамилия)

Офицер безопасности АО «НСПК» _____ _____
(Подпись) (И.О. Фамилия)

Офицер безопасности АО «НСПК» _____ _____
(Подпись) (И.О. Фамилия)

_____
(Дата)