КАЗАХСТАНСКИЙ ЦЕНТР МЕЖБАНКОВСКИХ РАСЧЕТОВ НБ РК

Процедуры работы с криптографическими ключами межбанковской системы платежных карточек

Нормативный документ

КЦМР _____

2016 г.

КАЗАХСТАНСКИЙ ЦЕНТР МЕЖБАНКОВСКИХ РАСЧЕТОВ НБ РК

Утверждены приказом
РГП КЦМР НБ РК
от «21» января 2016 года
№82-Д

Процедуры работы с криптографическими ключами межбанковской системы платежных карточек

Нормативный документ
КЦМР _____

Согласовано
Заместитель генерального
директора
_____Инкаров Б.Б.
«____»_____2016 г.

Заместитель генерального
директора
_____Орынбеков К.З.
«____»_____2016 г.

2016 г.

СОДЕРЖАНИЕ

1. Общие положения

1. Процедуры работы с криптографическими ключами межбанковской системы платежных карточек (далее – Процедуры) определяют порядок и принципы взаимодействия участника межбанковской системы платежных карточек с Операционным центром в процессе обмена криптографическими ключами.

2. Основной задачей данных Процедур является определение порядка безопасного распределения криптографических ключей, применяемого при обработке и передаче информации между участниками. Действие Процедур не распространяется на процедуры обращения с криптографическими ключами системы ФАСТИ, определенными нормативными документами удостоверяющего центра Операционного центра.

2. Термины и определения

3. В настоящих Процедурах используются следующие термины и определения:

1) ключ (криптографический ключ, ключ шифрования) – секретная информация, используемая криптографическим алгоритмом при шифровании или расшифровке данных, вычислении кодов аутентичности (MAC – Message Authentication Code);

2) средство криптографической защиты информации (СКЗИ) – программно–аппаратный комплекс, осуществляющий безопасное хранение и обработку криптографических ключей, а также реализующий криптографические алгоритмы с их использованием;

3) Hardware Security Module (HSM) – отдельное высокопроизводительное аппаратное СКЗИ, ориентированное на управление криптографическими ключами, обеспечение строгой аутентификации и прочие криптографические задачи авторизационного центра;

4) Personal Identification Number (PIN) – то же, что и Персональный Идентификационный Номер (ПИН);

5) Zone Master Key (ZMK) – зональный мастер ключ, используемый для обмена различными по назначению ключами между сторонними организациями;

6) Zone Control Master Key (ZCMK) – то же, что и ZMK в терминологии платежной системы VISA;

7) Acquirer Working Key (AWK) – рабочий ключ эквайера, используемый для передачи ПИН-блока от участника Операционному центру;

8) Issuer Working Key (IWK) – рабочий ключ эмитента, используемый для передачи ПИН-блока от Операционного центра участнику;

9) Zone PIN Key (ZPK) – зональный рабочий ключ, используемый для передачи ПИН-блока между участниками.

10) Zone Authentication Key (ZAK) - рабочий ключ, используемый для формирования кода аутентичности транзакции (MAC).

3. Основные положения

4. Процедура обмена криптографическими ключами между Операционным центром и участником состоит из двух основных этапов:

1) генерация Операционным центром ключа ZMK и передача его участнику;

2) обмен рабочими ключами AWK, IWK или ZPK и прочими криптографическими ключами.

5. Участник обязан:

1) применять безопасные методы работы с криптографическими ключами, исключающими любую возможность появления ключей в открытом незашифрованном виде;

2) обеспечить сохранность криптографических ключей организационными и техническими мерами;

3) использовать уникальные криптографические ключи в каждой области применения этих ключей;

4) в случае компрометации криптографического ключа следовать Главе 6 данных Процедур.

6. Участнику запрещено разглашать криптографические ключи, используемые для взаимодействия с Операционным центром, или передавать их третьим лицам.

4. Генерация и передача зонального ключа ZMK

7. Участник обязан в письменной форме уведомить Операционный центр о трех назначенных ответственных за хранение открытых компонент ключа ZMK, одновременно являющимися их получателями, с указанием следующих реквизитов для каждого ответственного:

1) полные Фамилия Имя Отчество;

2) занимаемая должность;

3) полный почтовый адрес получателя;

4) контактные телефоны и e-mail.

8. Ответственным за компоненты ключа участника запрещается:

1) быть одновременно получателем двух и более компонент одного ключа ZMK;

2) находиться в непосредственном служебном подчинении или находиться в подчинении у одного и того же руководителя структурного подразделения;

3) находиться в прямом родстве.

9. Генерацию ключа ZMK осуществляет непосредственно Операционный центр с помощью собственных СКЗИ. Для передачи ключа ZMK ответственным за хранение компонент ключа участника, формируются три компоненты ключа и упаковываются в три различных конверта, которые до передачи участнику, хранятся у трех ответственных за хранение открытых компонент ключа Операционного центра.

10. Передача компонент ключа ZMK участнику возможна следующими способами:

1) ответственные за хранение открытых компонент ключа участника самостоятельно получают компоненты ключа непосредственно на территории Операционного центра;

2) компоненты ключа пересылаются ответственным участника с помощью специальной почтовой связи и/или курьерской службы.

В последнем случае конверты с компонентами ключа ZMK отправляются участнику с сообщением ему даты отправки и реквизитов осуществляющих пересылку организаций. В один день запрещается отправлять более одной компоненты одной и той же курьерской службой.

11. Ответственные за хранение открытых компонент ключа ZMK участника при получении компонент ключа ZMK обязаны убедиться в целостности полученных конвертов и отсутствии следов внешнего воздействия на них, и только после этого могут приступить к формированию и загрузке ключа ZMK в СКЗИ участника. Загрузка ключа ZMK считается успешной, если контрольная сумма загруженного ключа совпадает с контрольной суммой, переданной от Операционного центра. По окончании процедуры загрузки ключа ZMK конверты с компонентами ключа необходимо уничтожить методом, исключающим их восстановление. Должен быть составлен акт загрузки ключа ZMK произвольной формы с обязательным указанием контрольной суммы собранного ключа и подписями ответственных за хранение открытых компонент ключа ZMK, копия которого направляется в Операционный центр.

12. Ключ ZMK может заменяться в любое время по взаимному согласованию сторон.

5. Обмен рабочими криптографическими ключами

13. Инициировать процесс обмена рабочими криптографическими ключами может как Операционный центр, так и непосредственно участник. Рабочий ключ шифруется с помощью ключа ZMK, который Операционный центр ранее передал участнику, и передаётся другой стороне с помощью любых открытых или закрытых каналов связи, например: электронная почта, факс, телефонная связь и т.п.

14. Для загрузки рабочих ключей используются СКЗИ на территории стороны – получателя. Проверку целостности полученного рабочего ключа стороны обмена проводят при помощи сверки контрольной суммы ключа. После загрузки ключа, сторона – получатель сообщает другой стороне по электронной почте контрольную сумму загруженного ключа.

15. Для шифрования ПИН–блока стороны могут использовать как пару ключей AWK и IWK, так и один ключ ZPK, для вычисления кодов аутентичности используется ключ ZAK.

16. Рабочие ключи могут заменяться в любое время по взаимному согласованию сторон.

6. Компрометация криптографических ключей

17. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

1) утрата (хищение) СКЗИ или носителей ключевой информации, в том числе, с последующим их обнаружением;

2) передача криптографических ключей по линии связи в открытом виде или непреднамеренное их раскрытие;

3) нарушение правил хранения криптографических ключей;

4) вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

5) несанкционированное или безучётное копирование ключевой информации;

6) все случаи, когда нельзя достоверно установить, что произошло с СКЗИ или носителем ключевой информации (в том числе случаи, когда ключевой носитель вышел из строя, и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

События 1) – 4) должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

18. При наступлении любого из перечисленных выше событий участник должен немедленно прекратить связь с процессинговой системой Операционного центра и сообщить о факте компрометации (или предполагаемом факте компрометации) Операционному центру по телефону, с дублированием по электронной почте, или другим доступным способом. В любом случае участник обязан убедиться, что сообщение о компрометации получено и/или прочтено адресатом.

19. При подтверждении факта компрометации действующих ключей участник обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и инициировать процесс обмена новыми ключами.

Лист регистрации изменений

№п/п	№ раздела, подраздела, пункта	Дата внесения изменений	Основание для внесения изменений (№, дата приказа)	№, дата утверждения и ввода в действие изменений	Подпись лица, внесшего изменения

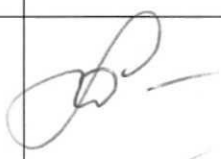
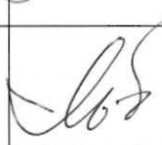
Лист согласования

КЦМР НД _____

Составил

Наименование подразделения КЦМР	**Должность исполнителя**	**Имя и фамилия исполнителя**	**Подпись**	**Дата**
ОПК	Начальник отдела	С. Абилхасимов		14.11.16

Согласовано

Наименование подразделения КЦМР	**Должность**	**Имя и фамилия исполнителя**	**Подпись**	**Дата**
Управление разработки и развития	Начальник управления	Анефиев Р.А.		
Управление безопасности	Начальник управления	Коршунов И.В.		
Управление операционно-технического обеспечения	Начальник управления	Дупленко Г.А.		14.11.16г.
Отдел бухгалтерского учета	Начальник отдела	Газюра В.А.		
Финансовый отдел	Начальник отдела	Олейник И.В.		
Общий отдел	Начальник отдела	Жарылгасов Ж.Б.