Регистрационный № Н-1020
от 3 декабря 2008 года
Департамент инжиниринга бизнес процессов

«У Т В Е Р Ж Д Е Н»
Правлением АО «Казкоммерцбанк»
Протокол № 275
от «01» декабря 2008 г.

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «Казкоммерцбанк»

Алматы 2015

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящий Регламент Удостоверяющего центра АО «Казкоммерцбанк» (далее – «Регламент») разработан в соответствии с требованиями законодательства Республики Казахстан и регламентирует порядок деятельности Удостоверяющего центра АО «Казкоммерцбанк» (далее по тексту Регламента – «Удостоверяющий центр» или «УЦ»).

Деятельность УЦ, связанная с реализацией (использованием и хранением) средств криптографической защиты, осуществляется на основании лицензии, выданной КНБ РК (Комитетом Национальной Безопасности РК), номер ЦА №222 от 30.10.2005г. (ЦА - Центр авторизации от center of authority).

Удостоверяющий Центр АО Казкоммерцбанк использует для изготовления Регистрационного свидетельства Удостоверяющего Центра и формирования Электронной цифровой подписи программное средство криптографической защиты информации "Тумар CSP" v3.4, соответствующее 4 уровню безопасности, установленному СТ РК 1073 – 2002. Использование комплекса "Тумар CSP" разрешено лицензией, выданной в соответствии с условиями договора №ГТ-41/2006 от 12.12.2006г. ТОО Научно-исследовательской лабораторией "Гамма Технологии".

Для Пользователей выпускаются ключи и Регистрационные свидетельства стандарта "RSA" с использованием программного обеспечения "RSA Certificate Manager 6.7" (фирмы "RSA Security Inc."), сертифицированного по международному стандарту "Common Criteria" по уровню "EAL4+" (наивысший достижимый уровень соответствия для продуктов типа "Инфраструктура открытых ключей" на дату утверждения документа).

1 Публикация Регламента

В целях обеспечения возможности ознакомления клиентов и иных заинтересованных лиц с Регламентом, электронная версия Регламента размещается на Интернет-сайте Банка www.qazkom.kz . Кроме того, текст Регламента размещается в помещениях подразделений Банка и его филиалов, осуществляющих выдачу Регистрационных свидетельств, консультирование Клиентов по вопросам их применения, таким образом, чтобы он был доступен для ознакомления последними с его содержанием.

2 Область применения Регламента

Регламент определяет порядок, общие особенности и условия предоставления Удостоверяющим центром услуг по выдаче Регистрационных свидетельств (в том числе Сертификатов), удостоверению соответствия Открытого ключа Электронной цифровой подписи Закрытому ключу Электронной цифровой подписи, по подтверждению достоверности Регистрационного свидетельства, а также общие вопросы применения Регистрационных свидетельств (Сертификатов), Электронных цифровых подписей.

Конкретные порядок, условия, особенности отношений Банка и клиентов (Заявителей) по вопросам, регламентируемых настоящим документом, юридические требования, ответственность Участников Системы электронного документооборота Банка при использовании Регистрационных свидетельств, определяются в договорах (соглашениях), заключаемых с Банком, внутренними нормативными документами Банка, устанавливающими особенности предоставления услуг Банка на основании Электронных документов.

3 Термины и сокращения

В Регламенте используются следующие термины и сокращения:

Аутентификация – процедура подтверждения неотрекаемости и правильности составления Электронного документа, осуществляемая путем использования процедур

безопасности, определенных Банком с учетом особенностей Систем электронного документооборота согласного настоящему Регламенту, иным внутренним документам Банка.

Владелец Регистрационного свидетельства - физическое лицо, на имя которого выдано Регистрационное свидетельство, правомерно владеющее Закрытым ключом Электронной цифровой подписи, соответствующим Открытому ключу Электронной цифровой подписи, указанному в Регистрационном свидетельстве.

Закрытый ключ Электронной цифровой подписи - последовательность электронных цифровых символов, известная Владельцу Регистрационного свидетельства и предназначенная для создания Электронной цифровой подписи с использованием Средств Электронной цифровой подписи.

Заявитель - физическое, являющееся клиентом Банка и желающее стать Владельцем Регистрационного свидетельства или юридическое лицо, желающие зарегистрировать Регистрационные свидетельства своих уполномоченных лиц (полученных последними в качестве физических лиц) для обеспечения создания Электронных документов, которые были бы равнозначны документам на бумажном носителе.

Заявление – оформленное в Банке:

- физическим лицом заявление на изготовление ключей и Регистрационного свидетельства, регистрацию Регистрационного свидетельства.
- юридическим лицом заявление на регистрацию Регистрационного свидетельства уполномоченных лиц Заявителя в качестве используемого для подтверждения Электронных документов юридического лица.

Заявление оформляется по форме, определенной законодательством Республики Казахстан и внутренними документами Банка, подписывается Заявителем (его уполномоченными представителями – для юридических лиц) в момент личного присутствия в Банке (за исключением случаев, установленных Регламентом). Заявление юридического лица дополнительно скрепляется печатью юридического лица

Карт-ридер – электронно-механическое устройство, обеспечивающее взаимодействие используемого Пользователем оборудования с чипом в Носителе ключей в целях создания Электронных документов с использованием его Электронной цифровой подписи на применяемом им оборудовании.

Компрометация ключа - утрата доверия к тому, что используемый ключ (пара ключей) обеспечивает безопасность Электронного документа. К событиям, связанным с компрометацией ключа (пары ключей), относятся, в том числе, следующие события:

- утрата, по любому основанию, Носителя ключевой информации (в том числе с его последующим обнаружением);
- увольнение по любому основанию уполномоченного лица юридического лица, Регистрационное свидетельство которого использовалось для подтверждения Электронных документов юридического лица. В таком случае замена ключей производится только при условии наличия заявления юридического лица (в отсутствие такого заявления соответствующие ключи могут далее использоваться физическим лицом для подтверждения собственных документов);
- случаи, когда нельзя достоверно установить, что произошло с Закрытым ключом Электронной цифровой подписи (в том числе случаи, когда Закрытый ключ Электронной цифровой подписи вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Неотрекаемость – невозможность отказа отправителя (автора) Электронного документа от факта отправки (подписи) соответствующего документа или сообщения. Неотрекаемость предполагает, что Электронный документ является достоверным, он направлен и подтвержден Владельцем Регистрационного свидетельства (установлено авторство), содержание Электронного документа не имеет несанкционированных изменений после его подтверждения

отправителем, автор Электронного документа, подтвердивший Электронный документ согласен с содержанием подтвержденного им Электронного документа.

Носитель ключевой информации (смарт-карта или токен) - защищенное хранилище, содержащее файлы Сертификата, включающего Открытый ключ Электронной цифровой подписи (публичный) и Электронную цифровую подпись Банка, а также служебные файлы, используемые для целей создания, визуализации и использования ЭЦП. Внешний вид Носителя ключевой информации: смарт-карты см. на рис. 10, токен – на рис 11.

Объектный идентификатор - цифровой код, присваиваемый в соответствии с рекомендациями ITU-T серии X.660|ISO/IEC 9834.

Отзыв (аннулирование) Регистрационного свидетельства - процедура признания Регистрационного свидетельства недействительным (аннулированным).

Открытый ключ Электронной цифровой подписи – последовательность электронных данных, доступная любому лицу и предназначенная для подтверждения подлинности Электронной цифровой подписи в Электронном документе, для идентификации Сертификата, которым подтвержден Электронный документ.

Пользователь – Владелец Регистрационного свидетельства, использующий Регистрационное свидетельство (Сертификат) для создания Электронной цифровой подписи и подтверждения Электронных документов.

Регистрационное свидетельство - документ на бумажном носителе и электронный документ (Сертификат), выдаваемый Удостоверяющим центром для подтверждения соответствия Электронной цифровой подписи требованиям, установленным законодательством Республики Казахстан. Сертификат с учетом особенностей используемой системы передачи данных может также использоваться для шифрования Электронного документа.

Регистрация Регистрационного свидетельства - внесение Регистрационного свидетельства в Регистр Регистрационных свидетельств Удостоверяющего центра, в котором ведется учет действующих и отозванных (аннулированных), приостановленных Регистрационных свидетельств.

Регистр – документ, в котором Удостоверяющим центром ведется учет действующих и отозванных (аннулированных) Регистрационных свидетельств.

Система электронного документооборота (далее – СЭД) – система обмена Электронными документами между Банком и иными Участниками системы электронного документооборота. Отношения между Банком и иными Участниками системы электронного документооборота регулируются законодательством Республики Казахстан, настоящим Регламентом, иными внутренними нормативными документами Банка.

Сертификат – наименование, применяемое в международной практике к электронному экземпляру Регистрационного свидетельства.

Список отозванных Регистрационных свидетельств (далее – СОРС, англ. Certificate Revocation List, сокр. CRL) – Электронный документ, созданный и подписанный Удостоверяющим центром и содержащий информацию о Регистрационных свидетельствах, выпущенных Удостоверяющим центром, действие которых прекращено или приостановлено.

Средства Электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности Электронной цифровой подписи.

Удостоверяющий центр (далее - УЦ) **-** подразделение Банка, удостоверяющее соответствие Открытого ключа Электронной цифровой подписи Закрытому ключу Электронной цифровой подписи, подтверждающее достоверность Регистрационного свидетельства.

Уполномоченный орган - государственный орган, осуществляющий реализацию государственной политики и государственное регулирование деятельности в сфере информатизации.

Участник Системы электронного документооборота - физическое или юридическое лицо, государственный орган или должностное лицо, участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения Электронных документов.

Электронная цифровая подпись (далее - ЭЦП) **-** уникальный набор электронных символов, созданный посредством Сертификата и Закрытого ключа Электронной цифровой подписи Владельца Регистрационного свидетельства, обеспечивающий неотрекаемость документа.

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством Электронной цифровой подписи.

Pin-код – секретный код, известный только Пользователю, на имя которого выдано Регистрационное свидетельство (Сертификат). Pin-код обеспечивает возможность использования Носителя ключевой информации только лицом, знающим Pin-код.

4 Область использования Регистрационного свидетельства

Сертификаты, выданные Банком в соответствии с настоящим Регламентом, используются для формирования ЭЦП в Электронных документах, направляемых по Системам электронного документооборота, поддержки неотрекаемости таких документов. Таким образом, использование Сертификата в Электронных документах позволяет обеспечить подтверждение целостности, подлинности таких документов, идентифицировать лицо, отправившее документ, согласие такого лица с документом, то есть подтвердить аутентичность документа.

Соответственно:

- Пользователь, используя действительный Сертификат, может сформировать ЭЦП и подтвердить ею Электронный документ. Участники Системы электронного документооборота (в том числе Банк), получив такой Электронный документ, будут идентифицировать его как оригинальный документ Пользователя. Формы Электронных документов, особенности и условия их направления Пользователем, определяются требованиями и возможностями соответствующей используемой Системы электронного документооборота;
- Банк, используя свой Сертификат, подтверждает своей ЭЦП Электронные документы, направляемые другим Участникам Системы электронного документооборота, в том числе заверяет выдаваемые Пользователям Сертификаты, Списки отозванных Регистрационных свидетельств;
- работники Банка, используя свой Сертификат, подтверждают своей ЭЦП Электронные документы, направляемые другим Участникам Системы электронного документооборота используемой в служебных целях (в корпоративной Системе электронного документооборота).

Сертификаты могут использоваться для подтверждения Электронных документов, направляемых Банку через Системы электронного документооборота, как при нахождении Пользователя в Республике Казахстан, так и в момент его нахождения за рубежом (при условии, что соответствующие Системы электронного документооборота доступны за рубежом).

Политика применения Сертификатов предполагает их использование для создания ЭЦП. Общие принципы процесса приема от Пользователя Электронных документов, заверенных ЭЦП, зависят от учетной политики Банка, требований внутренних нормативных документов, регламентирующих применение ЭЦП и процессов инициации и подтверждения подписи уполномоченных лиц.

Такие Электронные документы, в зависимости от возможностей и требований информационных систем Банка (Систем электронного документооборота), могут быть оформлены в виде:

- XML-документов;
- PDF-документов;
- Электронных документов локального формата (Onlinebank, БТА-онлайн и др.).
- Электронных документов систем внутреннего документооборота (WorkFlow и др.)
- сообщений Электронной почты.

Принципы работы с Электронными документами, систем Банка, требующих использования ЭЦП, их меры защиты и каналы связи описаны в соответствующих внутренних нормативных документах Банка, регламентирующих работу этих систем и/или предоставление соответствующих услуг Банка на основании Электронных документов.

4.1 Политики применения Регистрационных свидетельств (Сертификатов)

Формализованное представление использования Регистрационных свидетельств описывается следующей Политикой применения сертификатов (**ППС**):

Политика	Группа пользователей	Улучшенный ключ	Использование ключа	Алгоритм	Назначение
Политика I	Работники Банка	Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2) Конечная система IP-безопасности (1.3.6.1.5.5.7.3.5) Пользователь IP-безопасности (1.3.6.1.5.5.7.3.7) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)	ЭЦП, Обеспечение неотрекаемости, Шифрование ключей, Шифрование данных, Согласование ключей (f8)	1.2.840.113549.1.1.1 RSA	Формирование и проверка ЭЦП, подтверждение целостности и авторства информации, вход в корпоративную сеть Банка
Политика II	Клиенты Банка	Конечная система IP-безопасности (1.3.6.1.5.5.7.3.5) Пользователь IP-безопасности (1.3.6.1.5.5.7.3.7) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)	ЭЦП, Обеспечение неотрекаемости, Шифрование ключей, Шифрование данных, Согласование ключей (f8)		Формирование и проверка ЭЦП, подтверждение целостности и авторства информации
Политика III	Портальные системы Банка	Конечная система IP-безопасности (1.3.6.1.5.5.7.3.5) Пользователь IP-безопасности (1.3.6.1.5.5.7.3.7) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)	ЭЦП, Обеспечение неотрекаемости, Шифрование ключей, Шифрование данных, Согласование ключей (f8)		Формирование и проверка ЭЦП, подтверждение целостности и авторства информации, аутентификация систем, подписание документов портальной системы
Политика IV	УЦ		ЭЦП, подписание Сертификатов, Автономное подписание СОРС, Подписание СОРС (86)		Подписание Сертификатов сертификатов, подписание СОРС (CRL)

4.2 Требования к формированию и проверке ЭЦП клиента

4.2.1. Требования к формированию ЭЦП клиента

по смарт-карте:

1) Формирование ЭЦП осуществляется внутри Носителя ключевой информации с использованием ее встроенного RSA-сопроцессора. Алгоритм подписи – RSA.
2) Система команд Носителя ключевой информации стандартизована ISO 7816.
3) Для работы с Носителем ключевой информации требуется Карт-ридер.
4) Для работы с Карт-ридером используется поставляемый с ним драйвер.
5) Драйвер должен обеспечивать возможность работы с Носителем ключевой информации по протоколу PCSC.
6) Передача данных в чип Носителя ключевой информации (во встроенный RSA-сопроцессор) и генерация ЭЦП производится по протоколу PCSC командами стандарта ISO 7816.
7) Возможна работа с Носителем ключевой информации через Microsoft Crypto API. Для этого необходима установка программного обеспечения Axalto Cryptoprovider на компьютер Пользователя и импорт Сертификата из карты в хранилище Windows (Закрытый ключ Электронной цифровой подписи остается в памяти Носителя ключевой информации).

по токен:

1) Формирование ЭЦП осуществляется внутри Носителя ключевой информации с использованием встроенного защищенного микроконтроллера с энергонезависимой памятью. Алгоритм подписи – RSA.
2) Для работы с Носителем ключевой информации требуются полнофункциоинальные драйвера.
3) Полнофункциональные драйвера доступны на http://kaztoken.kz/index.php/ru/zagruzki/
4) Передача данных в Носитель ключевой информации и генерация ЭЦП производится по протоколу PCSC командами стандарта ISO 7816.

4.2.2. Требования к проверке ЭЦП клиента

1) ЭЦП, сформированная в порядке, определенном в п. 4.2.1. настоящего Регламента, проверяется Открытым ключом Электронной цифровой подписи Пользователя.
2) Открытый ключ Электронной цифровой подписи Пользователя является частью Сертификата Пользователя.
3) Сертификат Пользователя может присылаться вместе с Электронным документом, подписанным ЭЦП.
4) Сертификат Пользователя может копироваться из Регистра по регистрационному номеру Сертификата, присланному с подписанным ЭЦП Электронным документом.
5) Сертификат Пользователя может копироваться из данных проверяющей системы, куда он записывается при регистрации Пользователя в проверяющей системе.
6) Перед проверкой ЭЦП необходимо проверить действительность Сертификата Пользователя.
7) ЭЦП проверяется по стандартному алгоритму RSA.
8) Рекомендуемые библиотеки:
   - Microsoft CryptoAPI

- Sun Java Cryptoprovider
- Bouncingcastle Java-библиотека
- OpenSSL

4.2.3. Требования к проверке Сертификата Пользователя

1) Сертификат Пользователя содержит ЭЦП Удостоверяющего центра.
2) Сертификат Пользователя проверяется Выпускающим Сертификатом Удостоверяющего центра.
3) ЭЦП Выпускающего Сертификата Удостоверяющего центра проверяется Корневым Сертификатом Удостоверяющего центра.
4) Корневой Сертификат и Выпускающий Сертификат должны храниться в проверяющей системе.
5) Должна быть предусмотрена защита от подмены корневых Сертификатов в проверяющей системе.
6) Сертификат пользователя должен быть проверен по СОРС (CRL), генерируемому ежесуточно, и deltaCRL, генерируемому каждые 15 минут.
7) Выпускающий Сертификат Удостоверяющего центра также должен быть проверен по CRL.
8) СОРС должен своевременно обновляться с адреса, указанного в Сертификатах как пункт распространения CRL (CRL distribution point).
9) Подпись CRL должна быть проверена при получении нового СОРС с сайта.

ОБЩИЕ ПОЛОЖЕНИЯ

5 Услуги, предоставляемые Удостоверяющим Центром

В процессе своей деятельности Удостоверяющий Центр предоставляет Пользователям УЦ следующие виды услуг:

физическим лицам:

- выпускает Регистрационное свидетельство и выдает его на руки Владельцу Регистрационного свидетельства на бумажном носителе (по запросу владельца) и/или в электронном виде;
- создает Средствами Электронной цифровой подписи на имя физического лица Закрытый и Открытый ключи ЭЦП, Сертификат, соответствующий Открытому ключу, и вместе с иными необходимыми данными записывает их на Носитель ключевой информации. Носитель ключевой информации также выдается на руки Владельцу Регистрационного свидетельства;
- регистрирует и хранит созданный Сертификат в Регистре;
- подтверждает принадлежность, подлинность и действительность каждого Регистрационного свидетельства (или Сертификата), а также соответствие Закрытого ключа ЭЦП Открытому ключу ЭЦП;
- информирует Пользователей путем размещения на официальном сайте Банка и/или адресными рассылками на их электронные адреса о событиях, которые могут повлиять на использование Регистрационных свидетельств (Сертификатов).

6 Функционирование Удостоверяющего Центра

Удостоверяющий центр состоит из сектора администрирования и сектора сертификации, которые обеспечивают выполнение функций администрирования, регистрации и технической эксплуатации программно-аппаратных средств, используемых для выполнения услуг, предоставляемых Удостоверяющим центром.

Сектор администрирования осуществляет мероприятия по эксплуатации программных и технических средств обеспечения деятельности УЦ, техническое обеспечение процедуры подтверждения Электронной цифровой подписи, предоставляет пользователям УЦ сведения об аннулированных и приостановленных Регистрационных свидетельствах (Сертификатах), взаимодействует с Пользователями в части разрешения вопросов, связанных с применением Средств ЭЦП, ключей и Регистрационных свидетельств (Сертификатов), изготовляемых Удостоверяющим центром.

Сектор сертификации регистрирует Регистрационные свидетельства (Сертификаты), изготавливает и отзывает Регистрационные свидетельства (Сертификаты), приостанавливает и возобновляет их действие, взаимодействует с подразделениями Банка, ответственными за выдачу изготовленных Регистрационных свидетельств (Сертификатов) и Карт-ридеров Заявителям.

7 Прекращение деятельности Удостоверяющего центра

Деятельность Удостоверяющего Центра может быть прекращена в порядке, установленном законодательством Республики Казахстан, в том числе в случае соответствующего распоряжения Председателя Правления Банка.

В случае прекращения деятельности УЦ за тридцать дней до прекращения своей деятельности информирует об этом всех участников обслуживаемых им Систем электронного документооборота и Уполномоченный орган.

При прекращении деятельности УЦ выданные им Регистрационные свидетельства и соответствующие ключи Электронной цифровой подписи, сведения о Владельцах Регистрационных свидетельств передаются в другие удостоверяющие центры по согласованию с Владельцами Регистрационных свидетельств, при наличии соответствующих соглашений между удостоверяющими центрами.

По истечении срока 30 дней Регистрационные свидетельства и соответствующие ключи Электронной цифровой подписи, не переданные в другие удостоверяющие центры, прекращают свое действие и подлежат хранению в соответствии с законодательством Республики Казахстан.

ПРАВА

8 Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

1) отказать в предоставлении услуг Удостоверяющего центра в случае не предоставления Заявителем и (или) предоставления не в полном объеме документов, необходимых для выпуска Регистрационного свидетельства / регистрации существующего Регистрационного свидетельства. Перечень таких документов определяется в разделе 15 настоящего Регламента;
2) отказать в предоставлении услуг Заявителю, не являющемуся клиентом Банка;
3) отказать в приеме Заявления, если Банком ранее уже принято Заявление того же Заявителя и оно находится на стадии рассмотрения или Банком начат процесс изготовления Регистрационного свидетельства на имя данного Заявителя.
4) отказать в приеме Заявления, если у Заявителя уже есть не отозванное (не аннулированное) Регистрационное свидетельство, до завершения действия которого больше 1 месяца.
5) отказать в предоставлении услуг, если в Заявлении отражена недостоверная информация;
6) отозвать (аннулировать) Регистрационное свидетельство (Сертификат) в случаях, определенных в разделе 18 настоящего Регламента. В таком случае об отзыве (аннулировании) Регистрационного свидетельства (Сертификата) Банк направляет соответствующее уведомление его Владельцу с указанием причин, по которым выполнен отзыв (аннулирование);
7) приостановить действие Регистрационного свидетельства (Сертификата) с уведомлением Владельца Регистрационного свидетельства с обязательным указанием причин.

9 Права клиентов Банка

Клиенты Банка имеют следующие права:

1) Заявители могут обратиться в Удостоверяющий центр с Заявлением для изготовления Регистрационного свидетельства или для регистрации существующих Регистрационных свидетельств (Сертификатов) в качестве используемых для подтверждения Электронных документов Заявителей юридических лиц;
2) получить Регистрационное свидетельство Удостоверяющего центра в бумажном и электронном виде (Сертификат);
3) применять Регистрационное свидетельство, выданное/зарегистрированное Удостоверяющим центром и его копию в электронной форме – Сертификат, для проверки ЭЦП Удостоверяющего центра в Регистрационных свидетельствах, изготовленных Удостоверяющим Центром;
4) использовать список аннулированных (отозванных) и приостановленных Регистрационных свидетельств, формируемый Удостоверяющим центром, для проверки статуса своего Регистрационного свидетельства;
5) обратиться в УЦ за подтверждением подлинности Электронных цифровых подписей в Электронных документах;
6) обратиться в УЦ за подтверждением подлинности ЭЦП Удостоверяющего центра в изготовленных им Регистрационных свидетельствах;
7) обратиться в УЦ для аннулирования (отзыва) или приостановления/ возобновления действия Регистрационного свидетельства (в течение срока его действия);
8) воспользоваться действующей ЭЦП для подписания предоставляемых в электронной форме Заявлениях (для повторного выпуска Регистрационного свидетельства), а также для подписания заявлений на отзыв (аннулирование) действия Регистрационного свидетельства.

ОБЯЗАННОСТИ

10 Обязанности Удостоверяющего центра

10.1 Не позднее 10 рабочих дней с даты принятия к исполнению электронной заявки **физического лица** на выпуск ЭЦП (при условии предоставления в Банк Заявления на ЭЦП, приложения к нему всех необходимых документов согласно разделу 15 Регламента и оплаты Услуг) Удостоверяющий центр:

1) создает (генерирует) на имя Заявителя в форме электронного файла Сертификат, Закрытый ключ Электронной цифровой подписи и Открытый ключ Электронной цифровой подписи, записывает их на Носитель ключевой информации;
2) регистрирует изготовленный Сертификат путем внесения каждого Регистрационного свидетельства в Регистр УЦ;
3) выдает Владельцу Регистрационного свидетельства, Носитель ключевой информации и Pin-код к нему, позволяющие использовать ЭЦП для подписания Электронных документов, передаваемых от имени Клиента (и/или юридических лиц, уполномоченным лицом которых является Владелец Регистрационного свидетельства) в Банк и (или) третьим лицам;
4) предоставляет Заявителю доступ на сайт Банка для копирования необходимых сервисных программ;
5) выдает Карт-ридер (если в Заявлении клиентом было указано на необходимость его предоставления).

10.2 Удостоверяющий центр обеспечивает регистрацию Регистрационных свидетельств в соответствии с порядком регистрации, определенным настоящим Регламентом.

10.3 Удостоверяющий центр обязан не разглашать (публиковать) регистрационную информацию Пользователей, за исключением информации, используемой для идентификации Владельцев Регистрационных свидетельств и заносимой в изготавливаемые Регистрационные свидетельства.

10.4 Удостоверяющий центр обеспечивает изготовление Регистрационных свидетельств в соответствии с форматом и порядком идентификации, определенным в настоящем Регламенте. УЦ обязан обеспечить уникальность регистрационных (серийных) номеров изготавливаемых Регистрационных свидетельств.

10.5 Удостоверяющий Центр обязан отозвать (аннулировать) Регистрационное свидетельство по заявлению его владельца незамедлительно, но не позднее 1-го рабочего дня с момента получения заявления об отзыве. При этом Удостоверяющий центр заносит сведения об отозванном Регистрационном свидетельстве в Список отозванных Регистрационных свидетельств (СОРС) с указанием даты и времени отзыва.

СОРС Удостоверяющего Центра предоставляется в электронной форме в формате, определенном RFC 3280 (Certificate and Certificate Revocation List (CRL) Profile) и настоящим Регламентом.

10.6 УЦ обязан официально уведомить Владельца Регистрационного свидетельства:

1) о факте отзыва (аннулирования) или приостановления/ возобновления Регистрационного свидетельства. Срок уведомления – не более 1-го рабочего дня с момента занесения сведений об отозванном (аннулированном) свидетельстве в СОРС. Опубликование СОРС, содержащим сведения об отозванном (аннулированном) свидетельстве будут считаться официальным уведомлением;
2) о приостановлении Регистрационного свидетельства путем занесения соответствующих сведений в СОРС;
3) уведомление о предстоящем завершении срока действия Регистрационного свидетельства (Сертификата) - высылается заранее, за 45 календарных дней до завершения срока действия Регистрационного свидетельства (Сертификата);

4) о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования Регистрационного свидетельства.

Уведомления Пользователям направляются на их электронный адрес (email), если он был указан в заявлении на изготовление регистрационного свидетельства или в "Личный кабинет" клиента в финансовом портале Банка Homebank, или если это указано выше – путем занесения соответствующих сведений в СОРС.

10.7 УЦ обязан публиковать Список отозванных Регистрационных свидетельств (СОРС).
В каждом изготовленном Удостоверяющим центром Регистрационном свидетельстве в бумажном и электронном виде (в Сертификате) указаны электронные адреса, по которым через Интернет-браузер можно скачать последнюю версию Списка отозванных Регистрационных свидетельств, чтобы проверить статус Сертификата (приложение №4, поле "Точки распространения списков отзыва (CRL)").

Полный СОРС формируется ежесуточно и публикуется по адресу:
http://cert1.kkb.kz/Kazkommertsbank%20Issuing%20CA.crl

Дельта СОРС или новейший СОРС (приложение №4, поле "Новейший CRL") генерируется сервером УЦ каждые 15 минут. Он имеет меньший объем в байтах и показывает все серийные номера регистрационных свидетельств, отозванных и приостановленных только за последние 15 минут. Публикуется по следующему адресу:
http://cert1.kkb.kz/Kazkommertsbank%20Issuing%20CA_delta.crl

10.8 Регистр

УЦ ведет в электронном виде Регистр всех изготовленных Регистрационных свидетельств, - в течение срока деятельности УЦ. При этом об отозванных, аннулированных и приостановленных Регистрационных свидетельствах, которые были отражены в Регистре, УЦ публикует сведения в виде СОРС в порядке, отраженном в п. 10.8 Регламента.

11 Обязательства Пользователей

Пользователь обязан:

11.1 использовать Регистрационное свидетельство в строгом соответствии с Регламентом, заключенными с Банком договорами и соглашениями, действующим законодательством Республики Казахстан, а также исполнять иные обязанности, установленные законодательством Республики Казахстан;

11.2 не допускать неправомерного распространения информации о каждом/любом Закрытом ключе ЭЦП, защищать Pin-кодом каждый Носитель ключевой информации и хранить их в надежном месте, исключающем доступ к ним неуполномоченных лиц;

11.3 принимать меры для защиты Закрытых ключей ЭЦП, Носителей ключевой информации, Pin-кодов от неправомерного доступа и использования, а также хранить Открытые ключи ЭЦП в порядке, установленном законодательством;

11.4 немедленно, любыми доступными способами, информировать Банк о возникновении угрозы несанкционированного доступа к выданным ключам в следующих случаях:
- разглашение Pin-кода(-ов) или подозрение в его (их) разглашении;
- утеря каждого/любого Носителя ключевой информации или подозрение в его копировании третьими лицами;
- иных необходимых, по мнению Пользователя, случаях;

11.5 обеспечить выполнение технических требований, установленных заключенными с Банком договорами (соглашениями) о порядке использования ЭЦП, и использовать Систему электронного документооборота только на технически исправном оборудовании.

11.6 проверять действительность своего Сертификата по Списку отозванных Регистрационных свидетельств (СОРС) перед каждым использованием Сертификата;

11.7 указывать в Заявлении только достоверную информацию (в том числе при повторном выпуске Регистрационного свидетельства);

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

12 Типы конфиденциальной информации

Закрытый ключ Электронной цифровой подписи является конфиденциальной информацией Владельца Регистрационного свидетельства. Удостоверяющий центр не депонирует и не архивирует Закрытые ключи Электронной цифровой подписи.

Услуги Удостоверяющего центра предоставляются только тем клиентам Банка, которые предоставят свое письменное согласие на раскрытие сведений о них в Регистре и в СОРС.

Информация о Пользователях (помимо отражаемой в Регистре и в СОРС), имеющаяся у Удостоверяющего центра, считается конфиденциальной и не подлежит распространению.

Информация, хранящаяся в журналах аудита Удостоверяющего центра, считается конфиденциальной и не подлежит разглашению.

13 Информация, не являющаяся конфиденциальной

Информация, включаемая в Регистрационное свидетельство и СОРС, издаваемое Удостоверяющим Центром, не считается конфиденциальной.

14 Предоставление конфиденциальной информации

Удостоверяющий Центр не раскрывает информацию, являющуюся конфиденциальной, каким бы то ни было третьим лицам за исключением случаев, предусмотренных действующим законодательством Республики Казахстан или при вступлении в законную силу решения суда.

ПРОЦЕДУРЫ И МЕХАНИЗМЫ

Детальное описание взаимодействия подразделений Банка закреплено в технологической карте "Порядок выпуска и выдачи регистрационных свидетельств".

15 Процедура подачи Заявлений (в том числе при повторном выпуске)

Выдача Регистрационных свидетельств физическим лицам, а также регистрация Регистрационных свидетельств физических лиц в качестве используемых для подтверждения Электронных документов юридических лиц, производится на основании Заявления и заключенного с Банком договора (соглашения) в соответствии с действующим законодательством Республики Казахстан настоящим Регламентом и иными внутренними нормативными документами Банка.

Заявитель должен пройти процесс регистрации, состоящий из:

- для политик I и II - подачи Заявления установленного образца;
- для политики III — подачи служебной записки от заинтересованного Департамента в адрес Удостоверяющего центра с приложением Заявления, заполненного работником Банка по форме приложения;
- для политики IV — не требуется, инициируется Удостоверяющим центром.

1. Подача Заявления

Заявление предоставляется в Удостоверяющий центр по формам установленным:

– Приложением №1 к Регламенту, - для Заявителей физических лиц;
– Приложением №2 к Регламенту, - для Заявителей юридических лиц.

Заявление может быть предоставлено Заявителем в Банк через операционное подразделение филиала (для физических лиц) либо через ответственного работника филиала (для юридических лиц).

Физические лица для инициации вопроса рассмотрения Удостоверяющим центром возможности выпуска Регистрационного свидетельства до представления в Банк Заявления представляют Интернет-заявку через web-портал "www.homebank.kz". В таком случае предоставление необходимых документов, а также подписание Заявления осуществляются в операционном подразделении филиала Банка непосредственно при получении Регистрационного свидетельства. Списание средств со счета Заявителя производится по правилам оплаты Интернет- услуг.

Для получения/регистрации Регистрационного свидетельства (Сертификата) в Удостоверяющий центр вместе с Заявлением предоставляются следующие документы:

физическими лицами:

1) оригинал и копия (1 экземпляр) документа, удостоверяющего личность;

Операционный работник филиала Банка сверяет оригиналы вышеуказанного документа Заявителя с копией и проставляет соответствующую отметку «копия верна». После чего оригинал документа возвращаются Заявителю, копия размещается в досье Заявителя.

юридическими лицами:

1) документы, подтверждающие полномочия лиц, указанных в Заявлении:
   – решение участника (-ов)/акционеров о назначении лица руководителем (если в Заявлении указан руководитель); либо
   – если в документе с образцом подписей указан не руководитель, - доверенность, за подписью руководителя юридического лица или иных уполномоченных лиц, в которой четко указано, что предоставляется право первой подписи; или копия (заверенная печатью клиента) приказа о назначении с предоставлением права первой подписи (если такой порядок назначения и право действовать без доверенности установлены учредительными документами клиента);

2) копии документов, которые в соответствии с настоящим разделом Регламента предоставляются для выдачи Регистрационных свидетельств физическими лицами (на каждое лицо, указанное в Заявлении);
3) копии Регистрационных свидетельств, выданных лицам, указанным в Заявлении в качестве физических лиц;

Заявитель юридическое лицо до предоставления копий вышеуказанных документов физических лиц в Удостоверяющий центр самостоятельно сверяет их с оригиналами и проставляет на копиях документов соответствующую отметку «копия верна», а также заверяет копии подписью уполномоченного лица и печатью Заявителя. Копии документов передаются в Удостоверяющий центр и помещаются в досье Заявителя.

В случае изменения информации, указанной в предоставленных Заявителем документах, Заявитель обязан представить документы, подтверждающие такие изменения, в максимально короткие сроки, но не позднее 5 рабочих дней с даты соответствующих изменений.

2. Повторный выпуск Регистрационного свидетельства.

Повторный выпуск Регистрационного свидетельства возможен в случаях:

1. истечения срока действия Регистрационного свидетельства (до окончания которого остается не более 1 календарного месяца). За 30 дней до окончания срока действия имеющегося (действительного) Регистрационного свидетельства Пользователь может подать Заявление на выпуск нового Регистрационного свидетельства (взамен Регистрационного свидетельства, срок которого заканчивается, - повторный выпуск). При этом, если Заявитель имеет действующую ЭЦП Заявление (на повторный выпуск) может быть представлено в УЦ в виде Электронного документа. При этом сведения, содержащиеся в Заявлении, подтверждаются действующей Электронной цифровой подписью Заявителя, сформированной с использованием действующего Регистрационного свидетельства (которое не было отозвано/ аннулировано).
2. порчи Носителя ключевой информации;
3. утраты Носителя ключевой информации;
4. Компрометации ключа.

В случае повторного выпуска Регистрационных свидетельств Заявители представляют в Банк Заявления (с отметками о повторном выпуске), а также те документы, которые изменились после предоставления в Банк согласно настоящему Регламенту.

16 Структура Регистрационных свидетельств

1. Сертификаты Удостоверяющего центра АО "Казкоммерцбанк" генерируются с помощью лицензионного программного обеспечения RSA Certificate Manager (SN №428001999) и подразделяются на:

- Сертификат корневого центра сертификации "Kazkommertsbank Root CA" (срок действия 11 лет, размер открытого ключа - 4096 бит).
- Сертификат выпускающего центра сертификации "Kazkommertsbank Issuing CA" (срок действия 5 лет, размер открытого ключа - 4096 бит).
- Сертификат Владельца Регистрационного свидетельства на смарт карте/на токен (срок действия – 3 года или не более срока, оставшегося до окончания срока действия сертификата выпускающего центра сертификации, размер открытого ключа - 1024 бит).

2. Цепочка подписания Сертификатов:

- Сертификат Владельца Регистрационного свидетельства (например, "Pertov Petr") подписывается выпускающим центром сертификации УЦ,

- Сертификат выпускающего центра сертификации УЦ ("Kazkommertsbank Issuing CA") подписывается Сертификатом корневого центра сертификации УЦ,
- Сертификат корневого центра сертификации ("Kazkommertsbank Root CA") самоподписан (см. на рисунках 3, 6, 9 вкладку "Путь сертификации").

В соответствие с требованиями законодательства РК корневой сертификат Удостоверяющего центра переподписан с применением программного средства криптографической защиты информации "Тумар CSP" v3.4 (соответствующего 4 уровню безопасности, установленному СТ РК 1073 – 2002) и сохраняется бессрочно для подтверждения достоверности.

3. Регистрационные свидетельства выдаются Заявителям в форме Электронного документа - Сертификата и его копии на бумажном носителе. Форма Сертификатов определена в рисунках №1-9, Формы Регистрационных свидетельств определена в Приложениях №4-7 к настоящему Регламенту.

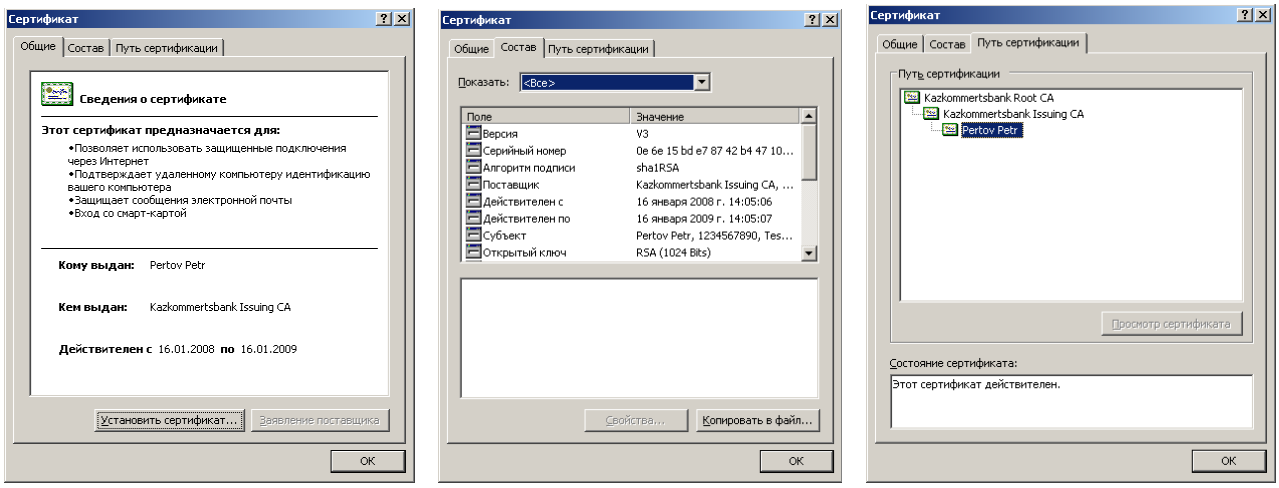

Рис.1-3. Сертификат Владельца регистрационного свидетельства.

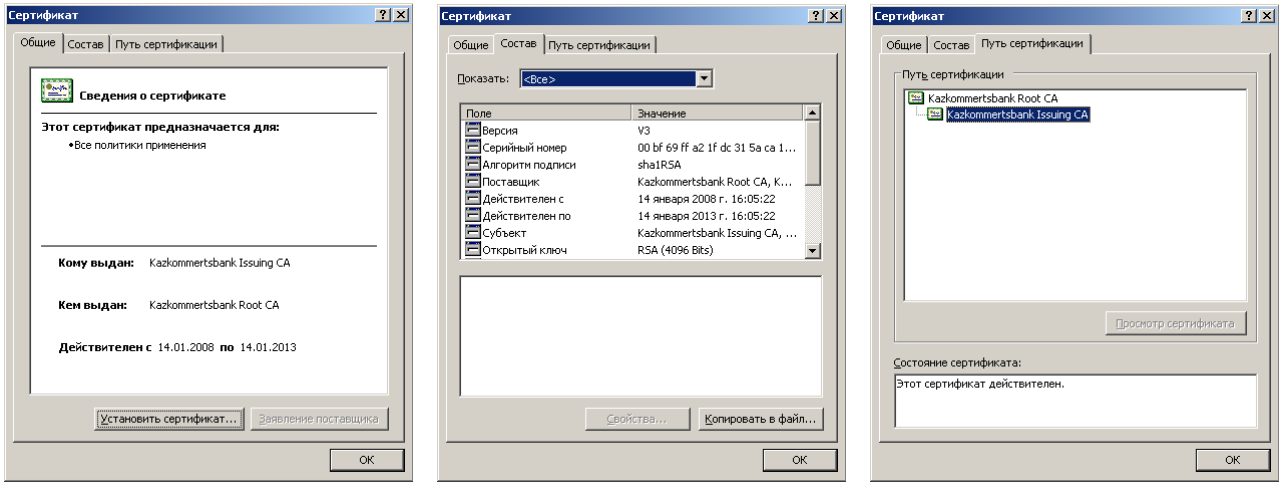

Рис.4-6. Сертификат выпускающего центра сертификации УЦ.

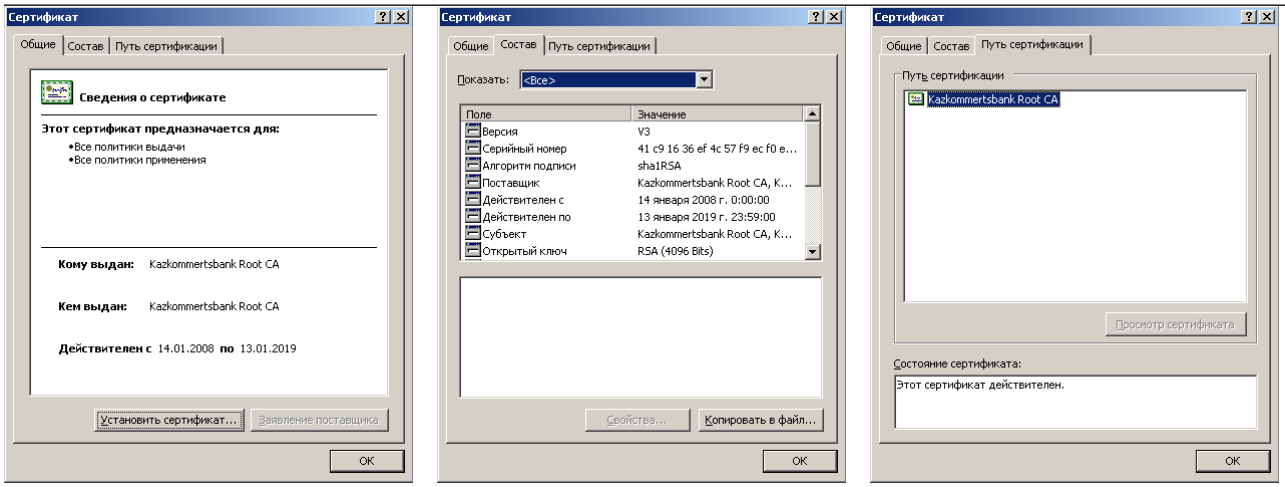

Рис.7-9. Сертификат корневого центра сертификации УЦ.

4. Структура Регистрационных свидетельств (Сертификатов), выпущенных Удостоверяющим центром в соответствии с международным стандартом X.509v.3, представлена в Приложениях №№4-8 к Регламенту. Сведения, которые содержатся в Регистрационном свидетельстве (Сертификате) в виде расширений по стандарту X.509v.3:
   - Открытый ключ Электронной цифровой подписи Владельца включен в расширение "Идентификатор ключа субъекта" (2.5.29.14).
   - Электронная цифровая подпись Удостоверяющего центра включена в расширение "Идентификатор ключа центра сертификатов" (2.5.29.35).
   - Область применения Сертификатов описана в расширении "Использование ключа" (2.5.29.15) и имеет значения:
     ✓ Для владельцев: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8).
     ✓ Для корневого и выпускающего: Цифровая подпись, Подписание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) (86).
   - Сведения о ресурсе, на котором размещается список отозванных Регистрационных свидетельств (COPC) включены в расширение "Точки распространения списков отзыва (CRL)" (2.5.29.31).
5. В качестве Носителей ключевой информации используется смарт-карта "Gemalto Palmera protect v.5"/токен Kaztoken, На выпущенном Носителе ключевой информации записываются файлы Сертификата, включающего Открытый ключ Электронной цифровой подписи (публичный) и Электронную цифровую подпись Банка. По умолчанию ПИН-код для всех выпускаемых смарт-карт устанавливается "1234". При первом использовании смарт-карты Пользователь обязан изменить ПИН-код. ПИН-код для ключей на токен генерируется в системе и выдается Пользователю на бумажном носителе в запечатанном виде по акту приема-передачи вместе с токен.
6. Номер Регистрационного свидетельства на бумажном носителе присваивается согласно Регистру сотрудником УЦ. Серийный номер Сертификата является уникальным.
7. Сертификаты корневого и выпускающего центров УЦ публикуются на официальном сайте Банка. Их закрытый ключ хранится в аппаратно-программном криптографическом модуле (HSM nCipher nShield 500 F3) .
8. На смарт-карту эмбоссируется следующая информация:

1. фамилия имя (буквы прописные, шрифт латинский) Владельца Регистрационного свидетельства (например, GOLOVKO OLEG);
2. месяц и год истечения срока действия (ММ/ГГГГ) /например, 12/2012/;
3. ИИН - 582411881414;

Рис. 10. Носитель ключевой информации (смарт-карта).

Рис. 11. Носитель ключевой информации (токен).

17 Выдача изготовленного Регистрационного свидетельства

По окончании процедуры изготовления ключей и Регистрационного свидетельства Заявителю выдаются:

1) Регистрационное свидетельство в виде электронного документа, заверенное ЭЦП УЦ, по форме Приложения №4. Дополнительно по просьбе Клиента может выдаваться регистрационное свидетельство на бумажном носителе с логотипом и печатью Банка по форме Приложения №5;
2) Сертификат, включающий Открытый ключ Электронной цифровой подписи (публичный) и Электронную цифровую подпись Банка, Закрытый ключ Электронной цифровой подписи, записанные на Носитель ключевой информации;
3) Инструкция пользования ЭЦП;
4) Карт-ридер (если указано в Заявлении).

Экземпляр открытого ключа Электронной цифровой подписи Удостоверяющего центра в форме Электронного документа публикуется на официальном сайте Банка.

Передача Регистрационного свидетельства, Носителя ключевой информации и Карт-ридера Заявителю осуществляется с составлением акта приема-передачи. Со стороны Банка Акт подписывается уполномоченным лицом и скрепляется печатью Банка.

18 Отзыв (аннулирование) Регистрационного свидетельства

1. Основания для отзыва (аннулирования) Регистрационного свидетельства

Отзыв (аннулирование) Регистрационного свидетельства производится Удостоверяющим центром:

по требованию Владельца Регистрационного свидетельства, либо его представителя, действующего на основании соответствующей доверенности;
по истечении срока действия Регистрационного свидетельства;
в случае смерти Владельца Регистрационного свидетельства;
на основании вступившего в законную силу решения суда;
порчи Носителя ключевой информации;

утраты Носителя ключевой информации;
Компрометации ключа;
в иных случаях, установленных законодательством Республики Казахстан и настоящим Регламентом.

Отзыв (аннулирование) Регистрационного свидетельства по требованию Владельца Регистрационного свидетельства осуществляется при получении Удостоверяющим центром заявления, оформленного по форме Приложения №3 к настоящему Регламенту. Заявление на отзыв (аннулирование) Регистрационного свидетельства подается заявителем:

- в электронной форме круглосуточно, 7 дней в неделю, через соответствующую услугу портала www.Homebank.kz. Если электронное заявление на отзыв подтверждается действующей, не аннулированной ЭЦП отзыв осуществляется УЦ незамедлительно, но не более 1-го рабочего дня, после получения заявления на отзыв (аннулирование). В случае возникновения подозрений на угрозу несанкционированного доступа к Носителю ключевой информации или его утере и порче, компрометации ключа заявление на отзыв (аннулирование) не подтверждается ЭЦП. В этом случае действие Сертификата после получения Интернет-заявления приостанавливается по умолчанию на 3 рабочих дня и автоматически возобновляется, если в течение этих 3 дней от Заявителя не поступает заявление письменной форме;
- в рабочее время в отделениях филиалов Банка в письменном виде. Заявление исполняется не позднее дня следующего за днем его поступления в Банк.

В случае отзыва (аннулирования) Регистрационного свидетельства Удостоверяющий центр оповещает об этом участников Системы электронного документооборота путем незамедлительного внесения данных о таком Регистрационном свидетельстве в СОРС с указанием даты и времени отзыва (аннулирования) Регистрационного свидетельства.

19 Срок хранения Регистрационного свидетельства

Изготовленные Регистрационные свидетельства, направленные из УЦ в РКО и не полученные заявителем ожидают выдачи в течение 2 месяцев, затем снова возвращаются в УЦ. Хранение Регистрационных свидетельств Удостоверяющим Центром осуществляется до окончания срока их действия.

Срок архивного (после окончания срока действия) хранения открытого (публичного) ключа Электронной цифровой подписи устанавливается равным не менее 5 лет.

20 Порядок проведения экспертизы при возникновении конфликтных ситуаций (разногласий)

1. При осуществлении обмена Электронными документами с помощью Системы электронного документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения Электронных документов, а также использованием в данных документах ЭЦП. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

1.1. неподтверждение подлинности Электронных документов средствами ЭЦП;
1.2. искажение Электронного документа;
1.3. оспаривание факта отправления и/или доставки Электронного документа;
1.4. оспаривание времени отправления и/или доставки Электронного документа;
1.5. оспаривание аутентичности экземпляров Электронного документа и/или подлинника и копии Электронного документа на бумажном носителе.

2. В случаях разногласий Удостоверяющий центр предоставляет Участникам Электронного документооборота всю имеющуюся информацию: подтверждает (не-) достоверность Регистрационного свидетельства, удостоверяет соответствие Открытого ключа Электронной цифровой подписи закрытому ключу Электронной цифровой подписи.

Экспертиза легитимности ЭЦП в Электронном документе проводится с применением лицензионного программного обеспечения "АРМ разбора конфликтных ситуаций".

3. В случае возникновения конфликтной ситуации Сторона, предполагающая возникновение конфликтной ситуации, должна незамедлительно, но не позднее, чем в течение 3 рабочих дней после возникновения конфликтной ситуации, направить уведомление о возникновении конфликтной ситуации другой Стороне.

4. Уведомление (направленное на электронный адрес) о предполагаемом наличии конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации, а также требования к другой Стороне. В уведомлении должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации. Уведомление о наличии конфликтной ситуации оформляется и отправляется в виде Электронного документа, а в случае, если это невозможно, то составляется на бумажном носителе и направляется с нарочным, либо иным способом, обеспечивающим подтверждение вручения уведомления адресату.

5. Сторона, которой направлено уведомление, обязана незамедлительно, однако не позднее чем в течение следующего рабочего дня, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

6. После получения информации уведомителем:

6.1. конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Стороны, которой было направлено уведомление, и отзывает свои требования, указанные в уведомлении;

6.2. в случае если уведомитель не удовлетворен информацией, полученной от Стороны, которой направлялось уведомление, для рассмотрения конфликтной ситуации формируется экспертная комиссия (далее – Комиссия).

7. В состав Комиссии входят сотрудники ДИТЗ Банка (с привлечением сотрудника УЦ) и представители Клиента.

8. По инициативе любой из сторон к работе Комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, обладающие необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

9. Сформированная Комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени отправки Электронного документа, его подлинности, а также о подписании Электронного документа конкретной ЭЦП, аутентичности отправленного документа полученному.

10. Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению Комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.

11. Все действия, предпринимаемые Комиссией для выяснения фактических обстоятельств, а также выводы, сделанные Комиссией, заносятся в Протокол работы экспертной комиссии. Данный протокол является основным документом работы Комиссии и должен быть подписан всеми ее членами.

12. При необходимости проведение проверки наличия или отсутствия фактических обстоятельств, свидетельствующих о факте и времени отправки Электронного документа проводится при участии компаний, обеспечивающих функционирование линий связи между Клиентом и Банком.

13. При проверке ЭЦП в Электронном документе открытые ключи ЭЦП, использованные для проверки, и факт подтверждения или не подтверждения подписи фиксируются в Протоколе работы Комиссии.

14. В случае подтверждения ЭЦП, значения Открытых ключей ЭЦП в составе Сертификатов, указанных в протоколе проверки, необходимо сравнить со значениями открытых ключей ЭЦП соответствующих бумажных копий, подписанных Банком. При совпадении их значений, авторство подписи под документом Стороны, направившей Электронный документ, считается установленным. Если при этом Сторона, направившая Электронный документ, настаивает на том, что данный Электронный документ она не отправляла, Комиссия может вынести решение о компрометации Закрытого ключа ЭЦП Стороны, направившей Электронный документ, что не является признанием оспариваемого Электронного документа не подлинным.

15. Если проверка ЭЦП Стороны, направившей Электронный документ, под оспариваемым Электронным документом дает отрицательный результат, то Комиссией принимается решение о том, что данная Сторона не направляла Электронный документ другой Стороне. Оспариваемый документ признается не подлинным.

16. По итогам работы Комиссии составляется Акт в необходимом количестве экземпляров (по числу членов комиссии), который подписывается всеми членами Комиссии и направляется каждой из Сторон по одному экземпляру. Акт содержит следующую информацию:

16.1. фактические обстоятельства, послужившие основанием возникновения разногласий;

16.2. протокол работы Комиссии;

16.3. выводы Комиссии.

17. Если на предложение Банка о создании Комиссии ответ Клиента не был получен или получен отказ от содействия в работе Комиссии или если Клиентом чинились препятствия работе Комиссии, Банк вправе составить акт в одностороннем порядке с указанием причины его составления. В акте приводится обоснование выводов о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого Электронного документа. Указанный акт составляется в двух экземплярах, подписывается Банком, и один экземпляр направляется Клиенту по почте.

18. Акт Комиссии является основанием для вынесения окончательного решения по конфликтной ситуации.

19. Стороны признают, что Акт, составленный Комиссией, является обязательным для Сторон и может служить доказательством при дальнейшем разбирательстве спора в суде в случае отсутствия согласия по спорным вопросам.

ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

21 Сроки действия ключей Удостоверяющего Центра

Срок действия Сертификата корневого центра сертификации "Kazkommertsbank Root CA" - 11 лет (размер открытого ключа - 4096 бит).

Срок действия Сертификата выпускающего центра сертификации "Kazkommertsbank Issuing CA" - 5 лет (размер открытого ключа - 4096 бит).

22 Сроки действия Регистрационных свидетельств Владельцев Регистрационных свидетельств

Срок действия Регистрационного свидетельства, выдаваемого УЦ клиентам, составляет 3 года.

23 Изменение информации, хранящейся на Носителе ключевой информации

Изменение информации, хранящейся на каждом/любом Носителе ключевой информации, недопустимо. Исключение составляет изменение владельцем Pin-кода.

24 Архивное хранение документированной информации

Архивированию подлежит следующая документированная информация:

досье Заявителя, в состав которого входят копии документов, предоставленных Заявителем при подаче заявления, Заявления и Заявления на отзыв (аннулирование);

Акты приема-передачи Регистрационных свидетельств.

Архивное хранение документированной информации УЦ осуществляется в соответствии с внутренним нормативным документам Банка, предусматривающим процедуру хранения и уничтожения документов в АО «Казкоммерцбанк».

25 Смена ключей Удостоверяющего центра

1. Плановая смена ключей Удостоверяющего центра

Процедура плановой смены ключей Удостоверяющего Центра осуществляется в следующем порядке:

- центр сертификации Удостоверяющего центра формирует новый закрытый и соответствующий ему открытый ключ Электронной цифровой подписи УЦ;
- центр сертификации Удостоверяющего центра изготавливает Регистрационное свидетельство и подписывает его Электронной цифровой подписью с использованием нового Закрытого ключа ЭЦП.

2. Внеплановая смена ключей Удостоверяющего центра

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации Закрытого ключа Электронной цифровой подписи Удостоверяющего центра.

Процедура внеплановой смены ключей Удостоверяющего центра выполняется в порядке, определенной процедурой плановой смены ключей Удостоверяющего центра.

После выполнения процедуры внеплановой смены ключей Удостоверяющего центра, предыдущее Регистрационного свидетельство Удостоверяющего центра аннулируется (отзывается) путем занесения в CORC.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

26 Аудит безопасности

С целью проверки деятельности УЦ, в том числе по выдаче Регистрационных свидетельств (Сертификатов), удостоверению соответствия Открытого ключа Электронной цифровой подписи Закрытому ключу Электронной цифровой подписи, по подтверждению достоверности Регистрационного свидетельства требованиям настоящего Регламента действующим нормативным правовым актам Республики Казахстан в области использования и эксплуатации средств криптографической защиты информации организуется постоянный внутренний аудит Департаментом Служба Внутреннего аудита в рамках утвержденного плана.

27 Инженерно-технические меры защиты информации

1. Обеспечение надежности и устойчивости функционирования Удостоверяющего центра.

Аппаратно-программные средства УЦ контролируют корректность работы критических функций и целостность всех компонент УЦ.

2. Размещение технических средств Удостоверяющего Центра

Серверы Удостоверяющего Центра, СКЗИ "ТУМАР – CSP", "П-Card" и телекоммуникационное оборудование размещены в выделенном помещении (далее по тексту – серверное помещение).

3. Физический доступ в серверные помещения

Серверное помещение оборудовано системой контроля доступа, включая систему видеонаблюдения на базе контроллеров "ПИКАР".

Идентификационные средства доступа в серверное помещение выдаются сотрудникам УЦ по служебной записке руководителя Удостоверяющего Центра.

4. Электроснабжение и кондиционирование воздуха

Технические средства ПК Удостоверяющего Центра подключены к гарантированной сети электроснабжения Банка. Электрические сети и электрооборудование, используемые в серверном помещении отвечают требованиям действующих "Правил устройства электроустановок", "Правил технической эксплуатации электроустановок потребителей", "Правил техники безопасности при эксплуатации электроустановок потребителей".

Серверы и телекоммуникационное оборудование УЦ подключены к источникам бесперебойного питания. Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

5. Предупреждение и защита от возгорания

Серверное помещение оборудовано установкой газового пожаротушения. Стойки с аппаратурой помещены в пожарозащищенные сейфы. Пожарная безопасность серверного помещения обеспечивается в соответствии с нормами и требованиями, устанавливаемыми законодательством Республики Казахстан.

28 Аппаратно-программные меры защиты информации

1. Организация доступа к техническим средствам Удостоверяющего центра

Доступ к техническим средствам Удостоверяющего центра, размещенным в серверном помещении, осуществляется с использованием системы контроля доступа.

2. Организация доступа к программным средствам Удостоверяющего центра

Серверы и рабочие места сотрудников УЦ оснащены аппаратно-программными комплексами защиты от несанкционированного доступа. Доступ системных администраторов общесистемного программного обеспечения серверов осуществляется в присутствии

сотрудников УЦ, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения.

3. Резервное копирование

Программно-аппаратные средства Удостоверяющего центра обеспечивают ежесуточное полное резервное копирование информации УЦ.

4. Контроль целостности технических средств

Контроль целостности технических средств Удостоверяющего центра обеспечивается опечатыванием корпусов устройств и шкафов-стоек, препятствующих их неконтролируемому вскрытию. Опечатывание выполняется перед вводом технических средств в эксплуатацию, и после выполнения регламентных работ.

Ответственность за выполнение мероприятий по контролю возложена на системного администратора УЦ.

5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности УЦ и программными средствами, предоставляемыми пользователям, в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Республики Казахстан.

Защита программно-технических средств обеспечения деятельности Удостоверяющего центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана не ниже 4-го класса защиты.

29 Организационные меры защиты информации

1. Предъявляемые требования к персоналу Удостоверяющего центра

Инженерно-технический персонал УЦ отвечает квалификационным требованиям, имеет опыт работы с операционными системами, средствами криптографической защиты информации, а также техническими средствами защиты информации.

2. Организация доступа персонала к документам и документации

Доступ сотрудников Удостоверяющего центра к документам и документации, составляющей документальный фонд УЦ, организован в соответствии с функциональными обязанностями и действующим порядком работы со служебной информацией.

3. Охрана здания и помещений

Удостоверяющий центр охраняется службой охраны здания и помещений Банка.

Программные и технические средства обеспечения деятельности Удостоверяющего центра

Для реализации своих услуг и обеспечения жизнедеятельности Удостоверяющий центр использует следующие программные и технические средства:

1. Программный комплекс обеспечения реализации целевых функций Удостоверяющего центра;
2. Технические средства обеспечения работы УЦ;
3. Аппаратно-программные средства защиты информации.

30 Программный комплекс обеспечения реализации целевых функций Удостоверяющего центра

Целевые функции УЦ реализованы с помощью программного обеспечения "RSA Certificate Manager 6.7" фирмы "RSA Security Inc.", которое предназначено для обеспечения следующих целевых функций Удостоверяющего центра:

1. регистрация Пользователей;
2. создание Закрытых ключей Электронных цифровых подписей Пользователей по их заявлениям;
3. изготовление Регистрационных свидетельств Пользователей в электронной и бумажной форме;
4. отзыв действия Регистрационных свидетельств Пользователя;
5. смена ключей Пользователей;
6. ведение Регистра, поддержание его актуальности;
7. генерация Списка отозванных Регистрационных свидетельств, поддержание их актуальности (CORC);
8. проверка уникальности Открытых ключей Электронной цифровой подписи в издаваемых УЦ Регистрационных свидетельствах;
9. проверка легитимности Регистрационного свидетельства по публикациям CORC;
10. напоминание о завершении срока действия Регистрационного свидетельства;
11. хранение Регистрационного свидетельств и CORC, публикуемых УЦ;
12. проверка ЭЦП (в формате PKCS#7) файла бинарных данных с использованием необходимых Регистрационных свидетельств;
13. выдача результатов проверки ЭЦП и Регистрационного свидетельства в виде протокола в форме электронного журнала с возможностью вывода бумажной копии.

31 Технические средства обеспечения работы УЦ

Технические средства обеспечения работы УЦ включают в себя:

1. Основной и Резервный Сервера УЦ;
2. Аппаратно-программное СКЗИ «ТУМАР – CSP» версии 3.4, «П-Card»;
3. Сервер Сетевого справочника;
4. Телекоммуникационное оборудование;
5. Компьютеры рабочих мест сотрудников Удостоверяющего центра;
6. Устройства печати на бумажных носителях (принтеры).

32 Программные и аппаратно-программные средства защиты информации

1. Аппаратно-программная защита базы данных и сервера Удостоверяющего центра обеспечивается аппаратным модулем защиты (Hardware Security Module – HSM) "nCipher nShield 500 F3" (производство Великобритания), соответствующим международному уровню защиты FIPS 140-2.

2. Межсетевой экран для обеспечения защиты информации при сетевом взаимодействии с отделом регистрации УЦ и Сетевым справочником;
3. Устройства обеспечения бесперебойного питания оборудования УЦ;
4. Штатные средства защиты информации от повреждения данных;
5. Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений Удостоверяющего центра;
6. Устройства обеспечения противопожарной безопасности помещений Удостоверяющего центра.

Исп. Давлидова Ш.А.
Ведущий специалист
Департамент развития Онлайнбанк
тел. 56839

Приложение № 1

Процесс № _____

ЗАЯВЛЕНИЕ НА ИЗГОТОВЛЕНИЕ КЛЮЧЕЙ И РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА И/ИЛИ РЕГИСТРАЦИЮ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА
(от физического лица)

Настоящим я

Фамилия	
Имя	
Фамилия (латиница)	
Имя (латиница)	
Отчество	
Адрес места проживания	
Наим. Области, района	
Наим. Населенного пункта	
Серия, номер паспорта/ удостоверения личности	
Кем и когда выдан	
ИИН	
РНН	
Наименование места работы	
Наименование должности	
Адрес электронной почты	
Контактный телефон	

Прошу (необходимо выбрать соответствующие пункты):

1. изготовить на мое имя ключи электронной цифровой подписи и регистрационное свидетельство открытого ключа электронной цифровой подписи,

2. зарегистрировать следующий открытый ключ электронной цифровой подписи с регистрационным свидетельством и открытым ключом: _____(значение открытого ключа) мое регистрационное свидетельство, созданное Удостоверяющим Центром "АО Казкоммерцбанк" с идентификационным номером:_____в регистре регистрационных свидетельств удостоверяющего центра в соответствии с указанными в настоящем заявлении сведениями.

Область использования регистрационного свидетельства: **Цифровая подпись, Неотрекаемость, Шифрование данных, Согласование ключей** (ключ может быть использован для целей обеспечения целостности и авторства информации, формирования и проверки электронной цифровой подписи электронных документов и информации, установление идентичности в процессе аутентификации и т.д.).

Срок действия регистрационного свидетельства: **3 года**.

Данные о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи и обозначение стандарта алгоритма электронной цифровой подписи: **RSA**, идентификатор алгоритма: **1.2.840.113549.1.1.1 RSA**.

Настоящим Заявитель подтверждает свое согласие на раскрытие сведений о нем в Регистре Регистрационных свидетельств, Списке отозванных Регистрационных свидетельств.

Вниманию Клиента! Нижеследующие поля используются в случае соответствующей необходимости:

- ✓ Выдать Карт-ридер - Да/нет (ненужное вычеркнуть)
- ✓ На основании данного Заявления производится повторный выпуск регистрационного свидетельства - Да/нет (ненужное вычеркнуть)

Подпись_____
Ф.И.О. _____
Дата: г.

Заявление принял(а): _____Сотрудник Банка МП

Приложение № 2

Процесс № _____

ЗАЯВЛЕНИЕ НА ИЗГОТОВЛЕНИЕ КЛЮЧЕЙ И РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА И/ИЛИ РЕГИСТРАЦИЮ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА
(от юридического лица)

Настоящим

Наименование юридического лица	
Юридический адрес	
Свидетельство о регистрации №	
Кем и когда выдано свидетельство	

просит на имя уполномоченного лица:

Фамилия	
Имя	
Отчество	
Адрес	
Наим. области, района	
Наим. населенного пункта	
Серия, номер паспорта/ удостоверения личности	
РНН	
ИИН	
Действующий на основании Доверенности №	
Адрес электронной почты	
Наименование должности	
Контактный телефон	

(необходимо выбрать соответствующие пункты):

☐ изготовить на мое имя ключи электронной цифровой подписи и регистрационное свидетельство открытого ключа электронной цифровой подписи

☐ зарегистрировать следующий открытый ключ электронной цифровой подписи с регистрационным свидетельством и открытым ключом: _____(значение открытого ключа) мое регистрационное свидетельство, созданное Удостоверяющим Центром "АО Казкоммерцбанк" с идентификационным номером:_____в регистре регистрационных свидетельств удостоверяющего центра в соответствии с указанными в настоящем заявлении сведениями.

Область использования регистрационного свидетельства: **Цифровая подпись, Неотрекаемость, Шифрование данных, Согласование ключей** (ключ может быть использован для целей обеспечения целостности и авторства информации, формирования и проверки электронной цифровой подписи электронных документов и информации, установление идентичности в процессе аутентификации и т.д.).

Срок действия регистрационного свидетельства: **3 года**.

Данные о средствах электронной цифровой подписи, используемых для создания соответствующего закрытого ключа электронной цифровой подписи и обозначение стандарта алгоритма электронной цифровой подписи: **RSA**, идентификатор алгоритма: **1.2.840.113549.1.1.1 RSA**.

Вниманию Клиента! Нижеследующие поля используются в случае соответствующей необходимости:

- ✓ Выдать Карт-ридер - Да/нет (ненужное вычеркнуть)

Должность _____
Подпись_____
Ф.И.О. _____

Дата: г.

Заявление принял(а): _____Сотрудник Банка МП

Приложение № 3

ЗАЯВЛЕНИЕ НА ОТЗЫВ (АННУЛИРОВАНИЕ) РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА (от физического лица)

Настоящим я,

_____,

(Фамилия, имя, отчество)

проживающий (-ая) по адресу:

_____

_____,

серия и номер паспорта/удостоверения, кем и когда выдан, место жительства, ИИН в связи с

_____,

(причина отзыва (аннулирования)

_____

регистрационного свидетельства: компрометация закрытого ключа,

_____

прекращение работы и т.д.)

прошу отозвать (аннулирования) регистрационное свидетельство с серийным номером _____

_____

(серийный номер и дата выдачи

_____

регистрационного свидетельства)

Подпись_____ Ф.И.О _____

Дата "___"_____ 200__г.

МП

Приложение №4

Регистрационное свидетельство на бумажном носителе и (или)
в форме электронного документа
№ _____

Версия: _____
Серийный номер регистрационного свидетельства:
_____
Идентификатор алгоритма ЭЦП: _____
Имя издателя регистрационного свидетельства: _____
Алгоритм криптографического преобразования издателя регистрационного свидетельства:_____
Срок действия регистрационного свидетельства:
Действительно с _____ по _____
Имя Владельца регистрационного свидетельства: _____
Закрытый ключ владельца регистрационного свидетельства:
длина ключа: _____ бит
Открытый ключ владельца регистрационного свидетельства:
длина ключа: _____ бит
значение:_____
_____
Назначение ключа: _____
Область применения ключа:

Флаг	Применение ключа

Средство ЭЦП: _____
Регистрационное свидетельство в формате _____: см. приложение
ЭЦП издателя под настоящим регистрационным свидетельством: _____
_____
«___» _____ 20__ г.

Приложение № 5

Регистрационное свидетельство №_____

Версия: X.509 V.3
Серийный номер: 0E6E15BDE78742B4471060F106C558EF

Издатель:
Kazkommertsbank Issuing CA
Полное имя:
CN=Kazkommertsbank Issuing CA, O=Kazkommertsbank, C=KZ

Владелец:
Pertov Petr
Полное имя:
CN=Pertov Petr, OU=1234567890, O=Test, E=petr@test.kz, C=KZ

Алгоритм подписи: sha1RSA

Срок действия: с 16 января 2008 г. 14:05:06 по 16 января 2009 г. 14:05:07
Алгоритм открытого ключа:
Идентификатор алгоритма: 1.2.840.113549.1.1.1 RSA
Длина: 1024
Параметры: 05 00
Значение:

```
30 81 89 02 81 81 00 c5 3e 47 92 69 1d e8 29 24 b6 2d df 25 d3 22 4c 8b 0f 7b f9
1a 46 d2 7b bf 16 2e 56 5d ea 60 d1 d0 f2 5f 14 e4 ca b5 9f 97 0d 1e cc 6f 04 03
0b 47 98 5a 02 53 fa ed 17 fb 24 61 50 30 08 30 02 7b 0c 47 4f 3c a7 b3 ef 09 03
a2 7b 61 c7 d5 09 47 a7 33 d8 d2 be 53 ca 77 ad 75 85 1f 91 94 9a 99 86 96 28 8c
51 fc 3f 28 9d b3 71 2a ad 8c ee c2 67 86 e4 4b 55 68 3e 2c d5 5b 92 79 d4 e9 c3
02 03 01 00 01
```

Расширения сертификата X.509:
Расширение: 2.5.29.14
Название: Идентификатор ключа субъекта
Значения:

```
53 ed 32 29 7d 04 7e 2c 62 bc c0 90 84 48 a4 a9 4a 9d a1 3e
```

Расширение: 2.5.29.15 (критическое)
Название: Использование ключа
Значения:

Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)

Расширение: 2.5.29.17
Название: Дополнительное имя субъекта
Значения:
Внешний адрес эл. почты: petr@test.kz

Расширение: 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значения:
[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:
URL=http://www.qazkom.kz /certroot/Kazkommertsbank%20Issuing%20CA.crl
[2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:
URL=http://cert1.kkb.kz/Kazkommertsbank%20Issuing%20CA.crl

Расширение: 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значения:
Идентификатор ключа=1c 88 a4 f6 e5 ba be 15 3b cb e7 e6 36 6f 48 31 01 c8 5f ae

Расширение: 2.5.29.37
Название: Улучшенный ключ
Значения:
Вход со смарт-картой (1.3.6.1.4.1.311.20.2.2) Конечная система IP-безопасности (1.3.6.1.5.5.7.3.5) Пользователь IP-безопасности (1.3.6.1.5.5.7.3.7) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Расширение: 2.5.29.46
Название: Новейший CRL
Значения:
[1]Новейший CRL Имя точки распространения: Полное имя: URL=http://www.qazkom.kz /certroot/Kazkommertsbank%20Issuing%20CA_delta.crl
[2]Новейший CRL Имя точки распространения: Полное имя: URL=http://cert1.kkb.kz/Kazkommertsbank %20Issuing%20CA_delta.crl

Отпечаток (sha1):
`8c 03 4e e1 62 05 e5 55 c5 03 76 65 1b 68 dc 0a b4 69 30 f2`

Регистрационное свидетельство в формате X.509 PEM:

```
MIIDkDCCAnigAwIBAgIFAMGDrLcwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCS1oxDDAKBgNVBAoTA0
tLQjELMAkGA1UECxMCQ0ExDzANBgNVBAMTBktLQiBDQTEYMBYGCSqGSIb3DQEJARYJY2FAa2tiLmt6MB4X
DTA3MTEwODA5MTgxM1oXDTEyMTEwNjA5MTgxM1owgYkxCzAJBgNVBAYTAktaMQ8wDQYDVQQHEwZBbG1hdH
kxDzANBgNVBAoTBktBWktPTTEVMBMGA1UECxMMNjAwNDEwMTgzODI5MRwwGgYDVQQDExNOQVpJUkEgTklM
RElLRVNIRVZBMSMwIQYJKoZIhvcNAQkBFhRubmlsZGlrZXNoZXZhQGtrYi5rejCBnzANBgkqhkiG9w0BAQ
EFAAOBjQAwgYkCgYEAhuJ2pR93Hy66+dYKuoH0XQ0Cvx//BYHCcfWRLRljORdnAVXBektMR9ngJtlzF7pU
tZsode2SeN1IXkhqBiXexEozjLQjJ93cHQ8ROuLrz5WsmsDVHMh6RUTUky76wdFKfAehaCaTxlN+RDuioL
fki2nwKF1+BDumg0ONd59SnksCAwEAAaOBtzCBtDAdBgNVHQ4EFgQUfBjqIdVuAKCyA6hml0IyY4TsLbIw
HwYDVR0jBBgwFoAU712nYyivxvN+d0LbneCElQZ9clMwDAYDVR0TBAUwAwEBADAOBgNVHQ8BAf8EBAMCBP
AwNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL3d3dy5ra2Iua3ovY2VydHJvb3Qva2tiY2EuY3JsMB0GA1Ud
JQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQQFAAOCAQEAA5MaSruBr01LDDKjYiCh7b
5aVpkIpxBI47BcngnvSbncFlPXD2NjCNgyZG1s9Nkj2cxWEbCZVisvFC+1qVy3PBVP4IH6nOEbZDcvasQI
N1ELfm0IsJKGw1mBeLBdnGeDybhnXcXEAluKknxJbc1FBpYN0kTrz1zdXIGRFhcjwJq6EIYiWgvvGFphJ5
bCcoJHFkVCXV1X1K8W5ykfDK0r65jo6XqR0J/jR6IzDI12pPTe+76FeGH5xcRMa1TjKxlHwwy1YzwzJCt/
nFNVNyVz3gN2MxUzyKGMDRPr1i8yUpXY2diHAEGdHgYIZUNVkeBMlPvpZbTYwNQD1+xp0gFqkw==
```


Директор Департамента Развития Онлайнбанк _____ Серазитдинов Р. М.

Дата "_____" _____20____г.

М.П.

Приложение № 6

Регистрационное свидетельство выпускающего центра сертификации УЦ

Версия: X.509 V.3
Серийный номер: 00BF69FFA21FDC315ACA1A44EE75FA02A9

Издатель:
Kazkommertsbank Root CA
Полное имя:
CN=Kazkommertsbank Root CA, O=Kazkommertsbank, C=KZ

Владелец:
Kazkommertsbank Issuing CA
Полное имя:
CN=Kazkommertsbank Issuing CA, O=Kazkommertsbank, C=KZ

Алгоритм подписи: sha1RSA

Срок действия: с 14 января 2008 г. 16:05:22 по 14 января 2013 г. 16:05:22

Алгоритм открытого ключа:
Идентификатор алгоритма: 1.2.840.113549.1.1.1 RSA
Длина: 4096
Параметры: 05 00
Значение:

```
30 82 02 0a 02 82 02 01 00 a6 e4 16 de f1 a7 89 38 fd 10 f0 06 65 d7 22 0e e1 14 7c e3 51 bc f4
9c cc 3f 44 e5 74 3c e6 b4 c8 23 52 23 4f b7 11 71 57 e8 71 14 a3 39 3a 02 05 36 9c d3 b1 05 10
b2 25 83 cd fd 9a 85 d5 67 38 cd 5c fe 70 2d 2c c6 2c 9d ce 49 e3 13 7f ee 9f 1c 3c 24 f3 e2 f0
0f fe 7a 5e e4 ea 76 8a e8 a9 77 50 fa c2 55 2d d8 c5 30 47 23 7c 18 36 25 b2 7f 42 34 e0 51 9c
8b dc fd 96 b4 6b d6 0a da 79 5d 19 f0 a1 bc c7 79 14 b1 00 cd eb 9b 53 36 79 d2 3a f2 e0 fd a8
c3 67 77 c0 b0 f1 8b 50 4b 02 4c 93 2e 65 0a 4a 41 e3 c1 44 7b ca 7a 8a c0 f7 d9 53 e3 28 d8 e6
bd d7 81 75 0c 34 35 4e 67 e7 93 47 04 aa a0 a8 54 b3 a6 6b f7 a4 ad e1 ab eb 23 38 68 c7 87 0d
94 9d 1c 27 34 03 e6 ce 94 ec 5b 3b a1 9e 03 8c b6 92 b6 5f 87 31 71 62 eb 79 f3 81 7b 65 95 7c
78 27 2c 55 66 95 51 19 3f ea 43 54 44 fe 86 e0 de 34 aa 09 f5 d6 1e 54 f2 15 7a 11 a6 ee f1 95
b1 23 b1 ab c4 e9 ff bd 67 27 5a 07 52 64 65 b1 58 64 92 49 81 7c 6b 3b 6a ec 2b e0 10 ff d2 9f
74 a9 d3 5c aa a6 5f bb 08 f1 a7 c3 de a9 25 44 d7 40 8e 8b b7 36 77 20 15 44 3d 44 c8 95 3a 38
2a c7 8e 59 7e ed 99 c1 40 81 b4 e5 30 f8 f2 9d c0 75 6e a3 61 ba 9a 73 f5 63 0c f6 7f 6e 44 29
bb db 71 39 58 c9 61 34 60 d7 b5 83 ca 47 df 2d de 21 08 60 7e 6d 43 df b3 38 8b 04 81 24 28 a8
84 09 93 b4 7d 7b 6b bf 8d 9c cd f5 00 d9 de c6 98 44 16 b3 b2 98 7e 84 6b be 41 f7 81 aa 69 f9
e8 70 ab e1 a2 8a 1b 64 dd ad 4b 38 cb f6 98 5d a2 04 7e a6 65 e9 0d 2f e6 20 7d d8 0a 76 b5 f5
eb 36 b3 3f c1 d3 96 80 6a 5e 51 50 48 9d 1a f3 46 d0 e1 6c 37 c3 e4 f2 6f 6c 08 4e b9 a0 ae 59
ec b8 97 18 f7 32 f9 67 35 02 03 01 00 01
```

Расширения сертификата X.509:
Расширение: 2.5.29.14
Название: Идентификатор ключа субъекта
Значения:

```
1c 88 a4 f6 e5 ba be 15 3b cb e7 e6 36 6f 48 31 01 c8 5f ae
```

Расширение: 2.5.29.15 (критическое)
Название: Использование ключа
Значения:

Цифровая подпись, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (86)

Расширение: 2.5.29.19
Название: Основные ограничения
Значения:
Тип субъекта=ЦС Ограничение на длину пути=Отсутствует

Расширение: 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значения:

[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://www.qazkom.kz /certroot/Kazkommertsbank%20Root%20CA.crl

[2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cert1.kkb.kz/Kazkommertsbank%20Root%20CA.crl

Расширение: 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значения:
Идентификатор ключа=1b 28 32 e7 12 70 7a 33 7c 91 73 64 88 b3 30 78 b5 d2 7b 78

Отпечаток (sha1):

```
c3 47 b2 ea c2 7c 6c 89 d9 c2 91 48 1f 7a a3 0d 92 74 26 e1
```

Регистрационное свидетельство в формате X.509 PEM:

```
MIIDkDCCAnigAwIBAgIFAMGDrLcwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCS1oxDDAKBgNVBAoTA0
tLQjELMAkGA1UECxMCQ0ExDzANBgNVBAMTBktLQiBDQTEYMBYGCSqGSIb3DQEJARYJY2FAa2tiLmt6MB4X
DTA3MTEwODA5MTgxM1oXDTEyMTEwNjA5MTgxM1owgYkxCzAJBgNVBAYTAktaMQ8wDQYDVQQHEwZBbG1hdH
kxDzANBgNVBAoTBktBWktPTTEVMBMGA1UECxMMNjAwNDEwMTgzODI5MRwwGgYDVQQDExNOQVpJUkEgTklM
RElLRVNIRVZBMSMwIQYJKoZIhvcNAQkBFhRubmlsZGlrZXNoZXZhQGtrYi5rejCBnzANBgkqhkiG9w0BAQ
EFAAOBjQAwgYkCgYEAhuJ2pR93Hy66+dYKuoH0XQ0Cvx//BYHCcfWRLRljORdnAVXBektMR9ngJtlzF7pU
tZsode2SeN1IXkhqBiXexEozjLQjJ93cHQ8ROuLrz5WsmsDVHMh6RUTUky76wdFKfAehaCaTxlN+RDuioL
fki2nwKF1+BDumg0ONd59SnksCAwEAAaOBtzCBtDAdBgNVHQ4EFgQUfBjqIdVuAKCyA6hml0IyY4TsLbIw
HwYDVR0jBBgwFoAU712nYyivxvN+d0LbneCElQZ9clMwDAYDVR0TBAUwAwEBADAOBgNVHQ8BAf8EBAMCBP
AwNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL3d3dy5ra2Iua3ovY2VydHJvb3Qva2tiY2EuY3JsMB0GA1Ud
JQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQQFAAOCAQEAA5MaSruBr01LDDKjYiCh7b
5aVpkIpxBI47BcngnvSbncFlPXD2NjCNgyZG1s9Nkj2cxWEbCZVisvFC+1qVy3PBVP4IH6nOEbZDcvasQI
N1ELfm0IsJKGw1mBeLBdnGeDybhnXcXEAluKknxJbc1FBpYN0kTrz1zdXIGRFhcjwJq6EIYiWgvvGFphJ5
bCcoJHFkVCXV1X1K8W5ykfDK0r65jo6XqR0J/jR6IzDI12pPTe+76FeGH5xcRMa1TjKxlHwwy1YzwzJCt/
nFNVNyVz3gN2MxUzyKGMDRPr1i8yUpXY2diHAEGdHgYIZUNVkeBMlPvpZbTYwNQD1+xp0gFqkw==
```

Директор Департамента Развития Онлайнбанк _____ Серазитдинов Р. М

Дата "_____" _____20____г.

М.П.

Приложение № 7

Регистрационное свидетельство корневого центра сертификации УЦ

Версия: X.509 V.3
Серийный номер: 41C91636EF4C57F9ECF0EC155E5C42F4
Издатель:
Kazkommertsbank Root CA
Полное имя:
CN=Kazkommertsbank Root CA, O=Kazkommertsbank, C=KZ

Владелец:
Kazkommertsbank Root CA
Полное имя:
CN=Kazkommertsbank Root CA, O=Kazkommertsbank, C=KZ

Алгоритм подписи: sha1RSA

Срок действия: 14 января 2008 г. 0:00:00 по 13 января 2019 г. 23:59:00

Алгоритм открытого ключа:
Идентификатор алгоритма: 1.2.840.113549.1.1.1 RSA
Длина: 4096
Параметры: 05 00
Значение:

```
30 82 02 0a 02 82 02 01 00 88 40 f1 34 7c 67 3f 71 ee e0 4e cc 29 54 ba 79 e7 00 a0 fb 64 ea 1f
d2 bf a8 5d 64 05 1a 07 5c 7a 7e 5a 40 49 b7 09 28 09 a7 9a 68 65 29 81 14 77 6e bc 55 43 0b c4
18 e5 b8 4c f8 7b 50 b1 aa 28 ad 02 b2 b2 22 b5 0f 20 0e 26 73 19 03 1d d5 38 5d 24 7b 55 bf c3
40 76 3f 72 a6 5d 28 a0 0f 28 f4 34 ff d1 be 64 43 31 8a 9a 75 90 60 5a 8e 7e f6 a3 9a 66 e2 1f
79 ac e7 e1 99 94 fb 72 f0 c3 ed 4e 98 ab 01 91 64 bf 5c 00 4b ac 6c 48 9b da 83 1c 9e f6 7a b6
1b 21 11 ba c7 a4 4a c8 99 e5 33 e1 ca d3 30 eb c0 5e 45 3b b7 0a b9 37 c5 90 e9 62 47 ff 8d f1
50 a8 7d 63 60 03 89 9f 65 c9 74 6d 1d 7e 1a 30 57 4b 16 e3 ea 88 77 0d 7f 65 88 19 30 22 36 49
08 68 2e 19 cd 21 70 9f 77 3b 18 04 6b c5 0e c2 11 bb 58 f1 22 96 c8 e8 02 93 20 e2 ac 61 29 a0
09 a1 75 0f ad 33 d0 30 7d b4 01 4d 64 3e 1c 39 21 ec c2 fd de eb e3 64 01 52 d0 2e 1e ea a8 01
4a 57 18 0b fb 55 80 7e c1 a2 4e 3d 37 0c 53 55 db e3 31 69 df c9 ff 46 2f 9f 40 c2 99 e7 b4 a0
51 9e bb b9 4c 5a 8f 66 c4 cd 1b 44 19 3f f2 80 57 6b 0f 7e 93 c5 00 cd 45 4d a7 0e c8 8e 4b 56
e2 8e 69 d5 af 05 28 e7 df aa 45 3d 15 d8 c2 75 9a 0a e5 16 10 e2 37 a6 ce 23 b6 59 50 bb 3a d9
13 99 37 aa 81 49 cc bf 98 e3 28 15 b2 6d ab 29 37 5d 22 24 e0 3e 90 a3 8b 42 b4 f2 51 16 10 a6
17 29 7c f2 8d 7e fd c0 69 56 6c 36 52 e0 bb a0 f5 69 62 61 64 99 78 bf 0d 14 eb 51 ce 5b 1b c6
80 db 01 c2 10 de 38 37 37 69 bb cd 46 50 5f e8 31 a1 34 e1 f4 d0 26 25 15 be 29 77 2d ec 3b 86
c1 07 d8 e5 db aa e6 0c b0 09 d8 7d 4e 33 d3 2d 70 5a 65 d2 ee 89 ca c8 30 b9 68 3a 1f b0 4c c7
85 77 04 6b 9d f6 7a 54 5b 02 03 01 00 01
```

Расширения сертификата X.509:
Расширение: 2.5.29.14
Название: Идентификатор ключа субъекта
Значения:

```
1b 28 32 e7 12 70 7a 33 7c 91 73 64 88 b3 30 78 b5 d2 7b 78
```

Расширение: 2.5.29.15 (критическое)
Название: Использование ключа
Значения:

Цифровая подпись, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (86)

Расширение: 2.5.29.19
Название: Основные ограничения
Значения:

Тип субъекта=ЦС Ограничение на длину пути=Отсутствует

Расширение: 2.5.29.31
Название: Точки распространения списков отзыва (CRL)

Значения:
[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://www.qazkom.kz /certroot/Kazkommertsbank%20Root%20CA.crl
[2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cert1.kkb.kz/Kazkommertsbank%20Root%20CA.crl

Расширение: 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значения:
Идентификатор ключа=1b 28 32 e7 12 70 7a 33 7c 91 73 64 88 b3 30 78 b5 d2 7b 78

Отпечаток (sha1):
72 bb b4 8b 21 2b 41 06 64 32 ae f8 25 33 82 c8 f9 a7 d0 51

Регистрационное свидетельство в формате X.509 PEM:
MIIDkDCCAnigAwIBAgIFAMGDrLcwDQYJKoZIhvcNAQEEBQAwUzELMAkGA1UEBhMCS1oxDDAKBgNVBAoTA0
tLQjELMAkGA1UECxMCQ0ExDzANBgNVBAMTBktLQiBDQTEYMBYGCSqGSIb3DQEJARYJY2FAa2tiLmt6MB4X
DTA3MTEwODA5MTgxM1oXDTEyMTEwNjA5MTgxM1owgYkxCzAJBgNVBAYTAktaMQ8wDQYDVQQHEwZBbG1hdH
kxDzANBgNVBAoTBktBWktPTTEVMBMGA1UECxMMNjAwNDEwMTgzODI5MRwwGgYDVQQDExNOQVpJUkEgTklM
RElLRVNIRVZBMSMwIQYJKoZIhvcNAQkBFhRubmlsZGlrZXNoZXZhQGtrYi5rejCBnzANBgkqhkiG9w0BAQ
EFAAOBjQAwgYkCgYEAhuJ2pR93Hy66+dYKuoH0XQ0Cvx//BYHCcfWRLRljORdnAVXBektMR9ngJtlzF7pU
tZsode2SeN1IXkhqBiXexEozjLQjJ93cHQ8ROuLrz5WsmsDVHMh6RUTUky76wdFKfAehaCaTxlN+RDuioL
fki2nwKF1+BDumg0ONd59SnksCAwEAAaOBtzCBtDAdBgNVHQ4EFgQUfBjqIdVuAKCyA6hml0IyY4TsLbIw
HwYDVR0jBBgwFoAU712nYyivxvN+d0LbneCElQZ9clMwDAYDVR0TBAUwAwEBADAOBgNVHQ8BAf8EBAMCBP
AwNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL3d3dy5ra2Iua3ovY2VydHJvb3Qva2tiY2EuY3JsMB0GA1Ud
JQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDBDANBgkqhkiG9w0BAQQFAAOCAQEAA5MaSruBr01LDDKjYiCh7b
5aVpkIpxBI47BcngnvSbncFlPXD2NjCNgyZG1s9Nkj2cxWEbCZVisvFC+1qVy3PBVP4IH6nOEbZDcvasQI
N1ELfm0IsJKGw1mBeLBdnGeDybhnXcXEAluKknxJbc1FBpYN0kTrz1zdXIGRFhcjwJq6EIYiWgvvGFphJ5
bCcoJHFkVCXV1X1K8W5ykfDK0r65jo6XqR0J/jR6IzDI12pPTe+76FeGH5xcRMa1TjKxlHwwy1YzwzJCt/
nFNVNyVz3gN2MxUzyKGMDRPr1i8yUpXY2diHAEGdHgYIZUNVkeBMlPvpZbTYwNQD1+xp0gFqkw==

Директор Департамента Развития Онлайнбанк _____ Серазитдинов Р. М

Дата "_____" _____20____г.

М.П.

Приложение № 8

Инструкция для Call Centre KAZKOM

1. Телефоны Удостоверяющего центра (УЦ): **55647, 55869** (в рабочие часы).
2. Синонимы: смарт-карта с ключом Электронной цифровой подписи, Носитель ключей, Носитель ключевой информации, Ключ ЭЦП, сертификат на смарт-карте, электронный сертификат.
3. Первичный пароль к смарт-карте "1234", его нужно сменить при первом же использовании.
4. Если пароль 3 раза введен неверно, смарт-карта блокируется и не подлежит разблокировке.
5. Если смарт-карта заблокирована, то клиент должен уведомить об этом УЦ для отзыва (аннулирования) сертификата, а затем, если требуется, подать заявку на повторный выпуск.
6. Если смарт-карта/токен ЭЦП утеряна, то клиент может:
   - в рабочие часы обратиться непосредственно в УЦ для аннулирования Сертификата,
   - либо, на странице сайта **Homebank>Настройки>Безопасность>Работа с сертификатами** самостоятельно удалить Сертификат, и позже, в рабочие часы, обратиться в УЦ для аннулирования Сертификата,
   - либо, если Интернет недоступен, попросить оператора Call Centre удалить Сертификат из Homebank (называя ключевое слово) и позже, в рабочие часы, обратиться в УЦ для аннулирования Сертификата.
7. Если истекает срок действия Регистрацилнного свидетельства и Носителя ключевой информации или требуется его повторный выпуск по другой причине, клиент может на странице сайта **Homebank>Финансы>Операции>Ключ ЭЦП (электронно-цифровая подпись)** подать заявку на выпуск нового Сертификата (повторный выпуск).
8. Неисправные Карт-ридеры подлежат замене только в течение 30 дней с момента выдачи в том же ЦБС, в котором были выданы (если неисправность не возникла в связи с механическими повреждениями иным физическим воздействием на Карт-ридер, неправильным его использованием Пользователем).