Одобрено
Протоколом Правления
№ 0513/2 от 13.05.2024 г.

Утверждено
Постановлением Совета директоров
№ 0523/3 от 23.05.2024 г.

ПОЛИТИКА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «БАНК ЦЕНТРКРЕДИТ»

Версия 2.1

Алматы 2024

Оглавление

1 ВВЕДЕНИЕ

Настоящий документ содержит Политику применения регистрационных свидетельств Удостоверяющего центра АО «Банк ЦентрКредит» (далее – Политика).
Удостоверяющий центр АО «Банк ЦентрКредит» создан для оказания услуг по выдаче регистрационных свидетельств физическим лицам клиентам Банка на основании действующего законодательства Республики Казахстан:
- Закон Республики Казахстан «Об информатизации»;
- Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи»;
- Закон Республики Казахстан «О персональных данных и их защите»;
- Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре» от 27 октября 2020 года № 405/НҚ;
- Приказ Министра по инвестициям и развитию Республики Казахстан «Об утверждении Правил проверки подлинности электронной цифровой подписи» от 9 декабря 2015 года № 1187;
- Приказ Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 № 1231 «Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан»;
- СТ РК 1073–2007. Средства криптографической защиты информации. Общие требования.

1.1 Термины и определения

Термины «Электронная цифровая подпись» (ЭЦП), «Открытый ключ электронной цифровой подписи», «Закрытый ключ электронной цифровой подписи», «Регистрационное свидетельство», «Владелец регистрационного свидетельства», применяются в настоящем Документе в соответствии с Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи».
Другие специальные термины, применяемые в данном Документе, используются в следующем значении:

Термин	Определение
Аппаратный криптографический модуль (Hardware Security Module)	Аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами ЭЦП.
Аутентификация	Процесс или сервис безопасности, реализующий этот процесс, который предназначен для проверки того, что лицо (предмет) является тем, кем себя именует (чем он поименован)
Биометрическая аутентификация	Комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков
Банк	АО «Банк ЦентрКредит»
Закрытый ключ электронной цифровой подписи	Последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи
Идентификация	В контексте Политики, процесс (или результат процесса), который устанавливает идентичность физического лица (показывающий, что данное лицо является однозначно определенным реально существующим лицом), и состоит из двух этапов: • установление соответствия, предъявленного лицом имени реально существующей идентичности лица и • установление того, что лицо, обращающееся за доступом к чему-либо от определенного имени, на самом деле является тем лицом, которым себя именует (аутентификация)
Инфраструктура открытых ключей	Набор сил и средств (технических, материальных, людских и пр.), распределённых служб и компонентов, в совокупности используемых для решения криптографических задач (аутентификации, шифрования, контроля целостности и доказательности) на основе криптосистем с открытым ключом, способный самостоятельно обеспечить управление открытыми ключами, посредством которых решаются указанные задачи
Компрометация ключей	Утрата владельцем регистрационного свидетельства уверенности в том, что

электронной цифровой подписи	конкретные ключи электронной цифровой подписи обеспечивают безопасность защищаемой с их помощью информации
Корневой удостоверяющий центр Республики Казахстан	Удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров
Многофакторная аутентификация	Способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации)
Облачная ЭЦП	Информационная система УЦ позволяющая создавать, хранить, использовать и удалять закрытые ключи электронной цифровой подписи владельца в модуле HSM УЦ, при котором доступ к закрытому ключу осуществляется владельцем посредством не менее двух факторов аутентификации, одним из которых является биометрическая
Облачный сертификат	Регистрационное свидетельство УЦ, выданное владельцу ключа облачной ЭЦП
Объектный идентификатор (OID)	Уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов
Открытый ключ электронной цифровой подписи	Последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе
Отозванное регистрационное свидетельство	Регистрационное свидетельство, аннулированное в порядке, который установлен правовым актом по вопросам выдачи, хранения, отзыва регистрационных свидетельств, изданным уполномоченным органом в сфере информатизации
Подписчик УЦ	Владелец регистрационного свидетельства, физическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющий закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве
Политика применения регистрационных свидетельств	Внутренний документ, утвержденный удостоверяющим центром, определяющий регламент и механизмы работы удостоверяющего центра в части управления регистрационными свидетельствами
Приложение ВСС	Мобильные приложения/цифровые платформы Банка, предоставляющие услуги дистанционного банковского обслуживания для физических лиц
Регистрационное свидетельство	Электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом “Об электронном документе и электронной цифровой подписи”
Регламент деятельности удостоверяющего центра	Нормативный документ, который определяет порядок организации основной деятельности удостоверяющего центра, осуществляемой в соответствии с политикой регистрационных свидетельств, включая течение основных процессов удостоверяющего центра
Сертификат	Регистрационное свидетельство
Список отозванных регистрационных свидетельств (сертификатов)	Часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования)
Средство криптографической защиты информации	Средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами
Удостоверяющий центр (УЦ)	Удостоверяющий центр Банка. Юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства
Электронная цифровая подпись (ЭЦП)	Набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания

Электронный документ	Документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи

1.2 Перечень сокращений

Аббревиатура	Определение
ИОК	Инфраструктура открытых ключей
СКЗИ	Средство криптографической защиты информации
HSM	Модуль безопасности CERTEX HSM
DN	Distinguished Names
COC	Список отозванных сертификатов
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
LDAP	Lightweight Directory Access Protocol v3

1.3 Обзор

Политика определяет требования к процедурам и условиям предоставления услуг подписчикам УЦ, связанных с жизненным циклом регистрационных свидетельств УЦ. Политика обязательна к применению всем участникам ИОК Банка, использующим регистрационные свидетельства УЦ.

1.4 Наименование и идентификация документа

Наименование документа: Политика применения регистрационных свидетельств Удостоверяющего центра АО «Банк ЦентрКредит».
Объектный идентификатор: 1.2.398.3.24.1.1.1
Версия документа: 2.1.
Адрес сервера для публикации Политики: https://www.bcc.kz/product/pki/?tab=DPP

1.5 Участники ИОК Банка

1.5.1 Центр Сертификации

Центр Сертификации - программно-аппаратный комплекс для выдачи, обслуживания и отзыва сертификатов ключей, действующий в соответствии с утвержденными правилами и сертифицированный по ГОСТ РК 1073–2007.
Центр Сертификации осуществляет следующие функции ИОК:
- обработка запросов на выдачу и отзыв регистрационных свидетельств;
- публикация COC и промежуточных списков отзыва сертификатов;
- обработка запросов к службе OCSP на проверку состояния сертификата;
- обработка запросов к службе TSP на формирование метки времени.

Центры Сертификации УЦ Банка:
- Центр сертификации: CN=Certification Authority
- Облачный центр сертификации: CN=CA Cloud

1.5.2 Центр Регистрации

Функцию центров регистрации выполняют информационные системы Банка, ответственные за прием и проверку документов на выпуск или отзыв сертификатов, а также идентификацию и аутентификацию подписчиков.

1.5.3 Подписчик УЦ

Подписчик УЦ - владелец регистрационного свидетельства УЦ, физическое, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве.

1.5.4 Доверяющие стороны

Доверяющая сторона – информационная система использующая полученные в УЦ сведения о сертификате для проверки принадлежности электронной цифровой подписи владельцу сертификата.

Доверяющими сторонами УЦ являются:
- Корневой Удостоверяющий центр Республики Казахстан
- Физические лица, граждане РК
- Информационные системы Банка, использующие регистрационные свидетельства Удостоверяющего центра Банка

1.6 Использование регистрационных свидетельств УЦ Банка

1.6.1 Допустимое использование сертификата

Сертификаты УЦ применимы для следующих целей:
- подписание электронных документов электронной цифровой подписью;
- проверка электронной цифровой подписи.

1.6.2 Ограничения использования сертификата

Способы использования сертификатов УЦ не должны противоречить действующему законодательству Республики Казахстан, а также требованиям настоящей Политики.

1.7 Управление Политикой

Все изменения, вносимые в настоящий документ, вступают в силу и становятся обязательными к исполнению всеми участниками УЦ немедленно после их публикации.
Изменения в Политику утверждаются Советом директоров Банка.

2 ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1 Доступность публичной информации

УЦ обеспечивает публикацию и доступность следующей информации на интернет-ресурсах.
Обеспечивается доступность сервисов из приложения ВСС:
- CA https://bcc-app.bank.corp.centercredit.kz:62305/
- RA https://bcc-app.bank.corp.centercredit.kz:62310/
- OCSP https://bcc-app.bank.corp.centercredit.kz:62301/
- TSP https://bcc-app.bank.corp.centercredit.kz:62302/

Доступны для скачивания и ознакомления:
- Регламент УЦ https://www.bcc.kz/product/pki/?tab=DPP
- Политика применения регистрационных свидетельств УЦ https://www.bcc.kz/product/pki/?tab=DPP
- СОС https://uc.bcc.kz/cgi/crl

2.2 Публикация хранилища сертификатов

Центр Сертификации публикует для доступа участникам УЦ хранилище сертификатов и СОС. Официальным уведомлением участников УЦ о выпуске сертификата и СОС является публикация сертификата и СОС в хранилище сертификатов.

2.3 Время и частота публикаций хранилища сертификата

Выданные сертификаты и СОС вносятся в хранилище сертификатов и публикуются не позднее даты начала их действия. Период обновления СОС составляет 7 календарных дней, публикация СОС производится по мере появления отозванных сертификатов.
Сведения о статусе сертификата публикуются в соответствии с настоящей Политикой.

2.4 Доступ к хранилищу сертификатов

Доступ к хранилищу сертификатов осуществляется по протоколу LDAP RFC 2251. УЦ осуществляет защиту от несанкционированного доступа к хранилищу сертификатов. Сведения, публикуемые на сайте УЦ, предоставляются участникам информационных систем в режиме свободного доступа с правами «только для чтения».

3 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1 Присваивание имён

УЦ выдает сертификаты, соответствующие рекомендациям X.509 ITU-T версии 3 и RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile». Сертификат содержит отличительное DN имя в формате, рекомендуемом стандартами X.501 ITU-T в поле «Subject». DN имя сертификата содержит персональные данные, позволяющие идентифицировать подписчика УЦ. DN имя определяет владельца сертификата и соответствующего закрытого ключа, а также область применения сертификата УЦ.
Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

3.2 Идентификация и аутентификация

3.2.1 Идентификация при выпуске и отзыве облачного сертификата

Подача заявлений на выпуск и отзыв облачных сертификатов осуществляется в режиме онлайн через систему дистанционного банковского обслуживания (приложение ВСС) с применением многофакторной аутентификации, включая биометрическую.
Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

3.2.2 Идентификация при выпуске и отзыве сертификата

Выпуск и отзыв регистрационных свидетельств осуществляется на основании заявления через дистанционный канал (приложение ВСС).
Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4 ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1 Заявление на выдачу сертификата

Заявление на выдачу сертификата имеют право подавать физические лица, граждане РК.

4.2 Обработка заявления на выпуск сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.3 Выдача сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.4 Признание сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.5 Использование ключей и сертификатов

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.6 Обновление сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.7 Смена ключей

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.8 Изменение сведений, указанных в сертификате

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.9 Отзыв и приостановление действия сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.10 Сервис проверки статуса сертификата в режиме онлайн

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

4.11 Окончание срока действия сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5 УПРАВЛЕНИЕ, ОПЕРАЦИОННЫЙ И ФИЗИЧЕСКИЙ КОНТРОЛЬ

5.1 Физические меры обеспечения безопасности

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.2 Организационные меры обеспечения безопасности

УЦ обеспечивает меры информационной безопасности персонала в соответствии с:
- внутренними нормативными документами Банка;
- должностными инструкциями работников Банка;
- законодательством Республики Казахстан.

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.3 Требования к персоналу

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.4 Порядок ведения записей аудита

УЦ обеспечивает протоколирование следующих событий:
- запрос на выпуск сертификата;
- запрос на отзыв сертификата;
- формирование закрытого ключа облачной ЭЦП;
- использование закрытого ключа облачной ЭЦП;
- удаление (стирание) закрытого ключа облачной ЭЦП.

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.5 Ведение архива

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.6 Смена ключей Центра Сертификации

УЦ осуществляет выпуск ключевых пар и регистрационных свидетельств по истечении срока действия корневого регистрационного свидетельства или в случае компрометации ключевых пар.
Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.7 Восстановление в случае компрометации или сбоев

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

5.8 Разрешение конфликтных ситуаций

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

6 ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1 Изготовление и установка ключевых пар УЦ и подписчиков

УЦ выпускает ключи и сертификаты в соответствии с алгоритмами ГОСТ 34.310–2004. Более подробная информация изложена в Регламенте удостоверяющего центра Банка.

6.2 Защита закрытого ключа, требования к носителям ключевой информации

Закрытые ключи центров сертификации создаются в модулях безопасности HSM, сертифицированных на соответствие стандарту Республики Казахстан СТ РК 1073–2007 по уровню не ниже второго.

Закрытые ключи облачных сертификатов создаются в модулях безопасности HSM, сертифицированных на соответствие стандарту Республики Казахстан СТ РК 1073–2007 по уровню не ниже третьего.
Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

6.3 Другие особенности использования ключей

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

6.4 Данные активации закрытых ключей

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

6.5 Средства управления компьютерной безопасностью

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

6.6 Технические средства управления жизненным циклом

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

7 ШАБЛОНЫ СЕРТИФИКАТОВ И COC

7.1 Описание сертификата

Центр Сертификации выдает сертификаты, соответствующие рекомендациям X.509 ITU-T версии 3 и RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile».

7.2 Объектные идентификаторы алгоритмов

Центр Сертификации использует объектные идентификаторы Республики Казахстан (OID РК)
https://root.gov.kz/oid/

7.3 Объектный идентификатор политики сертификата

7.3.1 Пользователь BCC KZ

Политика включается в сертификаты физических лиц пользователей информационной системы "BCC KZ";
Идентификатор (OID) политики 1.2.398.3.24.3.2.2

7.4 Структура сертификата

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

7.5 Описание COC

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.

7.6 Профиль OCSP

Более подробная информация изложена в Регламенте Удостоверяющего центра Банка.