Утверждаю
Генеральный директор
ТОО «Вериграм»
Байгожин А.К.

«01» декабря 2024г.

РЕГЛАМЕНТ

ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

г. Алматы
2024г.

1 ВВЕДЕНИЕ

Настоящий Регламент (далее – Регламент) Удостоверяющего Центра (далее – УЦ) «Инфраструктура открытых ключей» ТОО «Вериграм» описывает порядок предоставления услуг, принадлежащего ТОО «Вериграм» удостоверяющего центра и правила его использования участниками информационных систем.

Регламент является средством официального информирования всех сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

Регламент подготовлен в соответствии с рекомендациями RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

Регламент разработан в соответствии с Законом РК от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи» и «Правилами 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», утвержденными приказом Министра по инвестициям и развитию РК от 23 декабря 2015 года № 1231

1.1 Участники УЦ

1.1.1 Центр сертификации

Центр сертификации – автоматизированный комплекс настраиваемых служб для выдачи сертификатов ключей и управления ими.

1.1.2 Центр Регистрации

Центр Регистрации – компонент УЦ, предназначенный для выполнения операций по идентификации, аутентификации и проверке полномочий заявителя.

1.1.3 Интернет-ресурс УЦ

Интернет-ресурс УЦ - сервис, включающий в себя систему Облачной ЭЦП, обеспечивающий идентификацию, аутентификацию пользователя, в том числе силами Центра регистрации.

1.1.4 Хранилище сертификатов

Для получения доступа к сертификатам, службе проверки сертификатов, хранения архивной информации и других функций, Центр Сертификации использует специализированный справочник – хранилище сертификатов и списков отозванных сертификатов.

1.1.5 Владелец сертификата

Владелец сертификата – физическое лицо/юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве

1.1.6 Пользователь сертификата

Пользователь сертификата – физическое лицо/юридическое лицо, правомерно владеющее закрытым ключом ЭЦП, обладающее правом на ее использование на электронном документе.

1.1.7 Доверяющая сторона

Доверяющая сторона – информационные системы, использующие полученные в Центре сертификации сведения о сертификате для проверки принадлежности ЭЦП владельцу сертификата.

1.1.8 Другие участники

Облачная ЭЦП – информационная система УЦ, позволяющая создавать, использовать и хранить закрытые ключи электронной цифровой подписи владельца в HSM УЦ, где доступ к закрытому ключу осуществляется владельцем посредством не менее двух факторов аутентификации, одним из которых является биометрическая.
Сервер метки времени – служба для постановки метки времени на электронный документ. Служба работает на основе протокола меток времени – Time-Stamp Protocol (TSP).
Сервер проверки статуса сертификата – служба определения статуса сертификата. Служба работает на основе протокола Online Certificate Status Protocol (OCSP).

1.2 Использование сертификатов

1.2.1 Допустимое использование сертификата

Сертификаты могут использоваться для электронной цифровой подписи при создании электронных документов, а также для аутентификации владельцев сертификатов, в соответствии со сведениями (политиками), указанными в этих сертификатах.

1.2.2 Область применения сертификата

Сертификаты УЦ применимы для следующих целей:

- подписание электронных документов электронной цифровой подписью;
- проверка электронной цифровой подписи;
- аутентификация пользователей в информационных системах

Тестовые сертификаты должны использоваться для электронной цифровой подписи электронных документов, не имеющих юридической значимости.

1.3 Управление документом

1.3.1 Организация, ответственная за содержание документа

ТОО «Вериграм»
Республика Казахстан, 050022
г. Алматы, ул. Сатпаева, 9Б

1.3.2 Контактные данные

Email: support@verigram.ai

1.3.3 Лица, утверждающие изменения

Изменения в документе утверждаются первым руководителем ТОО «Вериграм».

1.3.4 Процедура утверждения изменений

Официальным уведомлением участников информационных систем об утверждении изменений настоящего Регламента является его публикация на сайте: https://verigram.kz

Все изменения, вносимые в настоящий Регламент, вступают в силу и становятся обязательными к исполнению всеми участниками УЦ немедленно после их публикации.

1.4 Определения и сокращения

Сертификат – регистрационное свидетельство, электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным законодательством Республики Казахстан

Закрытый ключ электронной цифровой подписи (закрытый ключ ЭЦП) - последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи.

Компрометация ключа - утрата доверия к тому, что используемый владельцем ключ обеспечивает безопасность информации.

Метка времени - электронный документ, выдаваемый УЦ, содержащий информацию о времени создания электронного документа, подписанного ЭЦП.

Обработка заявления на изменение статуса сертификата - совокупность действий по внесению сведений об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата в хранилище УЦ и уведомлению владельца сертификата об аннулировании (отзыве) сертификата.

Открытый ключ электронной цифровой подписи (открытый ключ ЭЦП) - последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе.

Заявление - электронный документ на выдачу или отзыв сертификата, по форме, установленной законодательством Республики Казахстан;

Заявитель – это физическое или юридическое лицо, подающее запрос на выдачу сертификата через интернет-ресурс удостоверяющего центра (УЦ).

Регистрация участника УЦ - внесение регистрационной информации о владельце сертификата в хранилище сертификатов.

Средства криптографической защиты информации (СКЗИ) - совокупность программно-технических средств, реализующих алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами и обеспечивающих применение электронной цифровой подписи и шифрования в информационных системах. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Список отозванных сертификатов (СОС) – перечень всех сертификатов УЦ, отозванных на момент выпуска СОС.

Статус сертификата – составное понятие, отражающее результат проверки действительности сертификата. Например, просрочен – не просрочен, отозван – не отозван.

Хранилище сертификатов – общедоступный справочник всех сертификатов и СОС.

LDAP (Lightweight Directory Access Protocol) – протокол прикладного уровня для доступа к службе каталогов, разработанной на рекомендациях International Telecommunication Union – Telecommunication sector (далее – ITU-T) X.500.

Аппаратный криптографический модуль (Hardware Security Module - HSM) - аппаратный криптографический модуль, предназначенный для шифрования информации и управления открытыми и закрытыми ключами ЭЦП.

Хэш – преобразование массива входных данных произвольной длины в битовую строку фиксированной длины.

Облачная ЭЦП - информационная система УЦ позволяющая создавать, использовать и хранить закрытые ключи электронной цифровой подписи владельца в HSM УЦ, где доступ к закрытому ключу осуществляется владельцем посредством не менее двух факторов аутентификации, одним из которых является биометрическая

Личный кабинет – пространство на интернет-ресурсе УЦ, предназначенное для получения/отзыва и применения облачной ЭЦП;

2 ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1 Регламент УЦ

При внесении каких-либо изменений Регламент публикуется на сайт: https://verigram.kz

2.2 Хранилище сертификатов

УЦ ведет хранилище сертификатов и СОС, обеспечивает их актуальность и возможность свободного доступа к ним участников информационных систем. Хранение закрытых ключей электронной цифровой подписи в УЦ осуществляется в облачной ЭЦП в соответствии с правилами создания, использования и хранения закрытых ключей электронной цифровой подписи в УЦ.

2.3 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.

2.4 Время и частота публикаций хранилища сертификатов

Выданные сертификаты и СОС вносятся в хранилище сертификатов и публикуются не позднее даты начала их действия. Период обновления СОС составляет 7 (семь) календарных дней.

Сведения о статусе сертификата публикуются в соответствии с настоящим Регламентом.

2.5 Доступ к хранилищу сертификатов

Доступ к хранилищу сертификатов осуществляется по протоколу LDAP (RFC 2251 Lightweight Directory Access Protocol (v3)). УЦ осуществляет защиту от несанкционированного доступа к хранилищу сертификатов.

3 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1 Назначение имен

Имя сертификата идентифицирует участника, который является владельцем сертификата и соответствующего закрытого ключа.

3.1.1 Типы имен (наименований)

Центр Сертификации выдает сертификаты, соответствующие рекомендациям ITU-T X.509 версии 3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Выданные сертификаты содержат в полях «Субъект» и «Издатель» сведения, представленные в соответствии с рекомендациями ITU-T X.501 (Distinguished Names (далее - DN)).

3.1.2 Необходимость персональных данных

Указанное в сертификатах имя физического лица (ФИО) должно точно совпадать со сведениями, указанными в удостоверении личности гражданина или паспорте.

Для всех типов сертификатов атрибут C (Country) содержит двухбуквенный код страны (ISO 3166-1 alpha-2).

Атрибут CN (Common Name) содержит фамилию и имя физического лица – владельца сертификата (строго в указанном порядке). Чтобы исключить неоднозначность между различными физическими лицами с одним и тем же именем, атрибут CN сертификата может содержать другой дополнительный текст, кроме идентификационного имени физического лица. Дополнительный текст должен быть отформатирован так, чтобы его нельзя было перепутать с именем физического лица. Рекомендуется, чтобы текст следовал за именем физического лица после пробела в качестве разделителя и был заключен в круглые скобки. Центр Сертификации не проверяет содержимое атрибута CN, и поэтому доверяющим сторонам запрещается полагаться на содержание текста. Для сертификатов сервера атрибут CN содержит полное доменное имя сервера. Для сертификатов служб атрибут CN содержит название службы.

Атрибут Serial Number может быть использован для идентификации организации и физических лиц. Содержит идентификатор в соответствии с рекомендациями CWA 16036 (Cyber-Identity - Unique Identification Systems For Organizations and Parts Thereof).

Атрибут UID (Unique ID) может использоваться для различия имен (фамилии и имени физического лица), которые в ином случае были бы одинаковыми. Содержит идентификатор, присвоенный физическому лицу правительством или гражданской властью.

3.1.3 Использование псевдонимов

В случаях, когда сертификат явно не содержит фамилии, имени и отчества владельца в соответствующем поле, считается, что в этом сертификате указан псевдоним.

3.1.4 Правила интерпретации различных форм имен (наименований)

Не определено.

3.1.5 Уникальность имен (наименований)

Отличительное имя DN (distinguished name) должно быть уникальным для каждого заявителя. Если имя DN, представленное заявителем не уникально, то УЦ потребует, чтобы заявитель повторно представил запрос с некоторым изменением атрибута CN, чтобы обеспечить уникальность имени. Согласно настоящему документу два имени считаются идентичными, если они отличаются только регистром, количеством символов подчеркивания или пробелов между словами. Таким образом, регистр, символы подчеркивания или пробела не должны использоваться для различия имен. Сертификат должен относиться к уникальному лицу или ресурсу или службе. Сертификат должен использоваться только владельцем. УЦ гарантирует, что отличительное имя DN не будет использоваться повторно другим заявителем. Если физическое лицо запрашивает сертификат с таким же именем DN, как в уже существующем сертификате (независимо от статуса этого сертификата), и запрос не является запросом на изменение сертификата, то уполномоченный сотрудник УЦ может обратиться к персональной удостоверяющей информации, чтобы проверить, что физическое лицо – тот же субъект, который был идентифицирован при получении первоначального сертификата. Если эта идентичность не может быть установлена, имя DN не будет использоваться повторно. В случаях полного совпадения сведений, указываемых в нескольких сертификатах, принадлежащих разным владельцам, в них вносятся специальный атрибут (например, серийный номер), позволяющий однозначно идентифицировать их владельцев.

3.2 Процедура первичной регистрации

Первичная регистрация заявителя – это процесс, в результате которого конечный участник впервые сообщает о себе УЦ, до того, как будут выпущен сертификат для данного конечного участника. Конечным результатом данного процесса (если он успешен), является:

- выпуск, выдача и/или помещение сертификата для открытого ключа заявителя в хранилище сертификатов.

- выпуск закрытого ключа ЭЦП, который сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147-89, данное действие подтверждается согласием владельца на хранение закрытого ключа ЭЦП в облачной ЭЦП УЦ. В качестве секретных значений участвуют пароль, заданный владельцем, который в УЦ не хранится. УЦ, для проверки пароля от закрытого ключа владельца, хранит хэш пароля в HSM.

Первичная регистрация инициируется путем подачи заявления через интернет-ресурс УЦ. Выдача сертификата заявителю осуществляется через интернет-ресурс УЦ.

В случаях мошеннических действий со стороны пользователя Центр регистрации может принять меры по приостановлению выпуска сертификата и/или отозвать сертификат.

3.2.1 Способ доказательства факта владения закрытым ключом

Заявитель должен продемонстрировать факт обладания закрытым ключом, соответствующим открытому ключу следующим образом:

1) Наличие электронного экземпляра сертификата на интернет-ресурсе УЦ;
2) Подтверждение выполняемых подписантом действий в личном кабинете путем аутентификации личности при входе в интернет-ресурс УЦ и ввода пароля, заданного владельцем при получении сертификата

3.2.2 Идентификация при выпуске облачного сертификата физического лица

Подача заявлений на выпуск облачных сертификатов для физических лиц осуществляется через интернет-ресурс УЦ. В процессе запроса облачного сертификата заявитель должен:

- дать согласие на сбор и обработку персональных данных;
- пройти процедуру многофакторной аутентификации, включая биометрическую аутентификацию;
- предоставить документ или цифровые данные, удостоверяющие личность;
- дать согласие на хранение закрытого ключа облачной ЭЦП в модуле безопасности HSM облачного УЦ.

После создания, закрытый ключ облачной ЭЦП сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147-89. В качестве секретных значений используется пароль, который в УЦ не хранится.

3.2.3 Процедура при выпуске облачного сертификата юридического лица

Подача заявлений на выпуск облачных сертификатов для юридических лиц осуществляется через интернет-ресурс УЦ. Заявление на получение сертификата от юридического лица подается первым руководителем юридического лица или лицом,

исполняющим его обязанности. В процессе запроса облачного сертификата заявитель должен:

- дать согласие на сбор и обработку персональных данных;
- подать заявление на выдачу Регистрационного свидетельства от юридического лица через интернет-ресурс;
- предоставить документ или цифровые данные, удостоверяющие личность первого руководителя юридического лица или лица, исполняющего его обязанности;
- предоставить документ или цифровые данные, подтверждающий полномочия доверенного лица клиента на подачу заявлений на выпуск сертификата, подписание актов приема-передачи ключевой информации и сертификата;
- пройти процедуру многофакторной аутентификации, включая биометрическую аутентификацию;
- дать согласие на хранение закрытого ключа облачной ЭЦП в модуле безопасности HSM облачного УЦ.

После создания, закрытый ключ облачной ЭЦП сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147-89. В качестве секретных значений используется пароль, который в УЦ не хранится.

УЦ вправе отказать в выпуске ЭЦП в случаях:

1. истечения срока действия документа, удостоверяющего личность;
2. предоставления заявителем недостоверных сведений;
3. в соответствии со вступившим в законную силу решением суда.

При устранении заявителем причин отказа в оказании услуги, заявитель подает повторное заявление для получения услуги по выдаче и отзыву регистрационного свидетельства, в порядке, установленном настоящими Правилами.

3.2.4 Сведения, указанные в заявлении, не подвергающиеся проверке

Не определено.

3.2.5 Дополнительные условия аутентификации

УЦ оставляет за собой право осуществлять проверку сведений, указанных в заявлении на выдачу сертификата, а также требовать от заявителя представления дополнительных документов, подтверждающих сведения, указанные в заявлении.

3.2.6 Подтверждение полномочий владельца сертификата

Уполномоченный сотрудник УЦ проверяет полномочия на основе данных, предоставленных заявителем. В случае невозможности однозначно подтвердить полномочия заявителя, в выдаче сертификата может быть отказано.

3.2.7 Взаимодействие с владельцами сертификатов, выданными другими Центрами сертификации

Владельцы сертификатов могут быть участниками единого пространства доверия с владельцами сертификатов, выданными другими Центрами Сертификации в тех случаях, когда между Центрами Сертификации заключено соответствующее соглашение и приняты необходимые организационно-технические меры. Владельцы сертификатов могут быть участниками единого пространства доверия с владельцами сертификатов, выданными Центром Сертификации Национального Удостоверяющего Центра Республики Казахстан

3.3 Процедура аутентификация заявителя при смене ключей

При смене ключей заявитель проходит процедуру аналогичную процедуре первичной регистрации см. разделы 3.2.2 - 3.2.4 с обязательным прохождением удаленной двухфакторной аутентификации, одним из методов которой является биометрическая аутентификация

3.3.1 Процедура аутентификация запросов при плановой (очередной) замене ключей

Процедура аутентификации в случае плановой смены ключей может проводиться в порядке, описанном в подразделе 3.2, либо на основании электронного документа. В последнем случае запрос в электронной форме представляет собой электронный документ, подписанный действующими ключами электронной цифровой подписи.

3.3.2 Процедура аутентификация при смене ключей после отзыва (аннулирования) сертификата

Процедура проводится в порядке, описанном в подразделе 3.2.

3.3.3 Процедура аутентификации заявителя при отзыве (аннулировании) облачного сертификата

Подача заявлений на отзыв облачных сертификатов для юридических лиц осуществляется через интернет-ресурс. В процессе отзыва облачного сертификата владелец УЦ должен:

- дать согласие на удаление закрытого ключа облачной ЭЦП в модуле безопасности HSM.
- пройти процедуру многофакторной аутентификации, включая биометрическую аутентификацию;

4 ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1 Заявление на выдачу сертификата ЭЦП

4.1.1 Лица, имеющие право подавать заявления на выпуск сертификатов

Заявление на выдачу сертификата имеют право подавать:

- физические лица
- юридические лица
- уполномоченные работники УЦ.

4.1.2 Процедура и обязательства по регистрации

Регистрация владелеца в УЦ, осуществляется в соответствии с п. 3.2 настоящего Регламента.

4.2 Обработка заявления на выдачу сертификата

4.2.1 Процедура идентификации и аутентификации заявления

Процедуры идентификации и аутентификации осуществляются в порядке, описанном в подразделе 3.2.

4.2.2 Выдача или отказ в выдаче сертификата

УЦ выдает сертификат в случае успешного прохождения заявителем процедур идентификации и аутентификации, описанных в подразделе 3.2. после подтверждения факта владения ключом ЭЦП.

В регистрации сертификата может быть отказано в случае, если:

- заявителем не представлена (либо не полностью представлена) необходимая информация.

- заявителем представлена недостоверная информация.
- заявитель не достиг восемнадцати лет.

В случае отказа в регистрации сертификата производится официальное уведомление заявителя не позднее пяти рабочих дней.

4.2.3 Сроки рассмотрения заявления на выдачу сертификата

УЦ обрабатывает заявления на выдачу сертификата заявителей в течение 5 рабочих дней после завершения процедуры аутентификации.

4.3 Изготовление сертификата

4.3.1 Действия Центра Сертификации при изготовлении сертификата

Центр Сертификации изготавливает сертификаты в соответствии со сведениями, указанными при регистрации заявителя. Формат сертификата, основан на рекомендациях ITU-T X.509v3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile).

Запросы на выпуск облачных сертификатов принимаются от портала интернет-сервиса УЦ

4.3.2 Уведомление заявителя о факте изготовления сертификата

Официальным уведомлением пользователей УЦ о выдаче сертификата является его публикация в хранилище сертификатов.

4.4 Признание сертификата

4.4.1 Действия владельца сертификата, означающие признание сертификата

Следующие действия владельца сертификата означают признание сертификата:

- получение сертификата;
- отсутствие у владельца возражений (претензий) по содержанию сертификата;
- использование сертификата.

4.4.2 Публикация сертификата

Центр Сертификации публикует сертификат в хранилище сертификатов в соответствии с настоящим Регламентом. Публикация сертификата происходит сразу после подтверждения заявки в УЦ (или уполномоченным сотрудником УЦ).

4.4.3 Уведомление участника УЦ о выдаче сертификата

Официальным уведомлением пользователей УЦ о выдаче сертификата является его публикация в хранилище сертификатов.

4.5 Использование ключей и сертификатов

Ключ подписи используется для формирования электронной цифровой подписи с использованием средств электронной цифровой подписи. Ключ шифрования используется для аутентификации владельца сертификата в информационных системах.

Сертификат используется для подтверждения подлинности электронной цифровой подписи. Проверка производится путем предоставления сведений о статусе выданных сертификатов и сертификатов уполномоченных лиц Центра сертификации участникам информационных систем.

Вышеуказанные сведения позволяют, при использовании сертифицированных средств электронной цифровой подписи, получать подтверждение подлинности электронной цифровой подписи в электронном документе автоматически. Сертифицированные средства электронной цифровой подписи, также позволяют получать сведения о фактах несанкционированных изменений электронных документов и уведомлять пользователей об отсутствии доверия к некорректным электронным цифровым подписям.

4.5.1 Использование закрытого ключа и сертификата их владельцем

Использование владельцем закрытого ключа и сертификата допускается только после признания сертификата. Использование закрытого ключа возможно только в соответствии с настоящим Регламентом.

4.5.2 Использование открытого ключа и сертификата пользователем

Пользователь сертификата должен использовать сертификат строго в соответствии с указанными в нем сведениями и настоящим Регламентом. Получение дополнительных сведений и гарантий, помимо сведений, указанных в сертификате, осуществляется участниками УЦ самостоятельно.

4.6 Обновление сертификата

Обновление сертификата – процедура получения сертификата с новыми сведениями и сроками действия без изменения открытого ключа, указанного в действующем сертификате.

4.7 Смена ключей

Смена ключей – процедура выдачи нового сертификата. Данная процедура подразумевает изготовление нового закрытого ключа и соответствующего ему сертификата.

Процедура подачи заявления и выдачи сертификата при смене ключей полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки.

4.7.1 Основания для замены ключей в сертификате

Ключи в сертификате могут быть заменены, если до истечения срока действия сертификата осталось менее чем 31 календарный день.

4.7.2 Обработка запросов на замену ключей в сертификате

Замена ключей до истечения срока действия сертификата может быть выполнена при предоставлении запроса, подписанного личным ключом, который соответствует действующему сертификату участника УЦ. При замене ключей в сертификате по истечению срока действия используется такая же процедура аутентификации как при получении первоначального сертификата.

4.8 Изменение сведений, указанных в сертификате

Процедура подачи заявления и выдачи сертификата при изменении сведений, указанных в сертификате, полностью аналогична процедурам подачи заявления на выдачу сертификата и его обработки.

4.9 Отзыв и приостановление действия сертификата

4.9.1 Основания для отзыва сертификата

УЦ может отозвать сертификат и осуществить публикацию его в СОС в следующих случаях:

- по требованию владельца сертификата.
- установления факта предоставления недостоверных сведений при получении сертификата.
- смерти владельца сертификата.
- изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца сертификата.

- смены наименования, реорганизации, ликвидации юридического лица – владельца сертификата.
- при подозрении на компрометацию ключа
- по вступившему в законную силу решению суда.

4.9.2 Лица, уполномоченные подавать заявления на отзыв сертификатов

Заявление на отзыв сертификата может подавать его владелец, сотрудник подразделения ИБ.

4.9.3 Процедура идентификации и аутентификации заявления

Процедура идентификации владельца сертификата при обработке электронного запроса на смену статуса сертификата, выполняется на основании данных, указанных в заявлении на отзыв сертификата.

4.9.4 Процедура подачи заявления на отзыв сертификата

Заявление на отзыв сертификата в УЦ направляется владельцем сертификата, сотрудником подразделения ИБ. Электронный запрос на отзыв сертификата заверяется подписью владельца сертификата. В случае получения электронного запроса УЦ автоматически обрабатывает его.

В случае утери сертификата запрос на отзыв сертификата направляется с электронного адреса владельца сертификата (указанном в сертификате).

Запрос на отзыв сертификата от сотрудника подразделения ИБ направляется по электронной почте.

4.9.5 Срок подачи заявления на отзыв сертификата

Заявление на отзыв сертификата следует подавать в течение минимально возможного времени после появления такой необходимости (например, в случае компрометации закрытого ключа).

4.9.6 Срок обработки заявления на отзыв сертификата

УЦ обрабатывает заявку на отзыв сертификата в течение одного рабочего дня.

4.9.7 Требования к осуществлению проверки факта отзыва сертификата

Пользователь сертификата должен самостоятельно проверять факт отзыва сертификата, полагаясь на достоверность которого он собирается действовать. Проверка факта отзыва может осуществляться с использованием СОС или сервиса проверки

статуса сертификатов в режиме online, сведения о порядке доступа, к которым указаны в каждом выданном сертификате и настоящем Регламенте.

4.9.8 Частота выпуска списков отозванных сертификатов

СОС обновляется по мере поступления запросов на смену статуса сертификатов.

Отозванные сертификаты с истекшим сроком действия, как правило, удаляются из СОС.

4.9.9 Задержка публикации списков отозванных сертификатов

Информация об отзыве сертификата публикуется автоматически, после включения серийного номера сертификата, времени и причин отзыва в СОС.

4.9.10 Возможность проверки статуса сертификата в режиме online

Информацию о статусе сертификата можно получить по протоколу проверки статуса сертификатов в режиме online (Online Certificate Status Protocol - OCSP). Сведения о порядке доступа к сервису проверки статуса сертификата в режиме online опционально включаются в расширение сертификатов.

4.9.11 Требования к осуществлению проверки факта отзыва сертификата в режиме online

Владелец сертификата должен самостоятельно осуществлять проверку статуса сертификата, полагаясь на достоверность которого он собирается действовать. В тех случаях, когда для определения степени доверия к сертификату недостаточно использования СОС, пользователь должен использовать сервис проверки статуса сертификатов в режиме online (OCSP).

4.9.12 Другие способы извещения участников информационных систем о фактах отзыва сертификатов

Официальным уведомлением участников УЦ об отзыве сертификата является публикация СОС в хранилище сертификатов.

4.9.13 Срок хранения отозванных сертификатов

Срок хранения отозванных сертификатов в хранилище сертификатов составляет не менее пяти лет.

4.9.14 Особые требования в случае компрометации секретных ключей

УЦ прилагает все, коммерчески оправданные усилия для оповещения участников информационных систем, в случае компрометации ключей уполномоченных лиц Центра Сертификации.

4.9.15 Условия приостановления действия сертификата

Не определено.

4.9.16 Лица, уполномоченные подавать заявления на приостановление действия сертификатов

Не определено.

4.9.17 Процедура подачи заявления на приостановление действия сертификата

Не определено.

4.9.18 Ограничение срока приостановления действия сертификата

Не определено.

4.10 Сервис проверки статуса сертификата в режиме online

4.10.1 Эксплуатационные характеристики

Информация о статусах сертификатов доступна с использованием списков отозванных сертификатов и сервиса проверки статуса сертификатов в режиме online.

Список отозванных сертификатов предоставляется в электронной форме в формате, определенном RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Список заверяется ЭЦП Центра Сертификации. Доступ к списку отозванных сертификатов обеспечивается по протоколам LDAP (RFC 2251 Lightweight Directory Access Protocol (v3)) и HTTP.

Сервис проверки статуса сертификата в режиме online соответствует требованиям, описанным в RFC 2560 (Online Certificate Status Protocol - OCSP). Квитанции с результатом проверки сертификата в режиме online заверяются ЭЦП сервера OCSP.

4.10.2 Доступность службы проверки статусов сертификатов

Информация о статусах сертификатов доступна постоянно за исключением запланированных перерывов в работе УЦ.

4.10.3 Дополнительные возможности

Не определено.

4.11 Окончание пользования услугами УЦ

Участник информационной системы может закончить использование услуг УЦ путем отзыва своего набора ключевой информации или отказа от смены ключей после окончания их срока действия.

4.12 Депонирование и восстановление ключей

Не определено.

5 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для обеспечения безопасности УЦ применяются приведенные ниже меры, включающие в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установлением соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты от несанкционированного доступа.

Защита персональных данных в УЦ выполняется в соответствии с требованиями внутренних нормативных документов по информационной безопасности.

5.1 Физические меры обеспечения безопасности

5.1.1 Размещение Центра Сертификации

Центр Сертификации, обрабатывающий запросы участников УЦ, расположен в специализированном для размещения серверов и оборудования помещении.

5.1.2 Физический доступ

Все помещения УЦ оборудованы системой контроля и управления доступом с идентификацией по смарт-картам, исполнительными устройствами системы контроля доступа электромеханического типа.

5.1.3 Электроснабжение и кондиционирование воздуха

Технические средства Центра Сертификации подключены к общегородской сети электроснабжения с использованием оборудования бесперебойного питания. Помещения УЦ оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Республики Казахстан.

5.1.4 Подверженность воздействию влаги

Защита оборудования УЦ от влаги обеспечивается его размещением в специальных серверных шкафах.

5.1.5 Противопожарные меры безопасности и защита от возгорания

Помещения УЦ оборудованы средствами пожаротушения в соответствии с требованиями, установленными законодательством Республики Казахстан.

5.1.6 Хранение архивных документов и электронных носителей

Документальный архив УЦ хранится в соответствии с действующим законодательством Республики Казахстан.

5.1.7 Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками УЦ, обеспечивающими документирование.

Сменные носители информации физически уничтожаются перед утилизацией.

5.1.8 Резервное копирование вне сети

Не определено.

5.2 Организационные меры обеспечения безопасности

5.2.1 Разграничение ролей (полномочий)

Среди сотрудников УЦ выделяют роли администратора, оператора, аудитора и системного администратора.

5.3 Требования к персоналу

5.3.1 Требования к квалификации и стажу работы

Сотрудники УЦ должны иметь высшее профессиональное образование, с предпочтительно трехлетним опытом работы в области информационных технологий.

5.3.2 Требования к повышению квалификации персонала

Обязательное обучение проходят вновь принятые сотрудники УЦ.

В случае переноса средств УЦ на новое оборудования или программное обеспечение, персонал Центра Сертификации проходит курс обучения работе с новыми средствами.

5.3.3 Частота и последовательность смены деятельности сотрудников

Не определено.

5.3.4 Ответственность за нарушения

Персонал УЦ несет ответственность за свои действия в соответствии с законодательством Республики Казахстан.

5.3.5 Требования к независимым подрядчикам

В исключительных случаях, когда для выполнения работ требуются услуги независимых подрядчиков, специалисты подрядчиков проводят работы только под наблюдением и с разрешения сотрудников УЦ.

5.3.6 Документация, предоставляемая персоналу

Деятельность сотрудников УЦ регламентирована внутренними инструкциями.

5.4 Порядок ведения записей аудита

5.4.1 Типы событий, подлежащих аудиту

Программно-аппаратный комплекс УЦ регистрирует следующие виды событий:

- системные события общесистемного программного обеспечения.
- принятие запроса на выпуск сертификата.
- выпуск сертификата.
- помещение запроса на сертификат.

- принятие запроса на сертификат.
- отклонение запроса на сертификат.
- выпуск/перевыпуск списка отозванных сертификатов.
- невыполнение внутренней операции программной компоненты.

Структуры записей событий соответствуют эксплуатационной документации программного обеспечения реализации целевых функций УЦ и общесистемного программного обеспечения.

5.4.2 Частота анализа журналов аудита

Журналы аудита еженедельно анализируются с целью обнаружения нарушений в работе программного и аппаратного обеспечения Центра Сертификации, анализа производительности систем, а также по мере поступления запросов/жалоб от информационных систем, использующих УЦ.

В процессе анализа журналов аудита проводится расследование всех значительных нарушений работы, и принимаются адекватные меры реагирования, которые в последствии находят отражения в новых версиях ПО.

5.4.3 Срок хранения журналов аудита

Журналы аудита подлежат архивированию по истечении двух месяцев после окончания их анализа.

5.4.4 Защита журналов аудита

Журналы аудита защищены от несанкционированного просмотра, модификации и удаления средствами прикладного и общесистемного программного обеспечения.

5.4.5 Резервное копирование журналов аудита

Журналы аудита подлежат резервному копированию ежедневно.

5.4.6 Условия сбора данных для аудита

События аудита автоматически записываются в журналы средствами прикладного и общесистемного программного обеспечения.

5.4.7 Уведомление субъекта события, вносимого в журнал аудита

При записи события в журнал аудита уведомление субъекта этого события не требуется.

5.4.8 Анализ уязвимостей

События, записываемые в журнал аудита, также служат для анализа уязвимостей УЦ. УЦ постоянно проводит анализ технических уязвимостей и предотвращает их возможные проявления. Все найденные уязвимости и принятые меры по их устранению включаются в ежегодный отчет об аудите.

5.5 Ведение архива

5.5.1 Типы регистрируемых событий

УЦ ведет архив:

- журналов аудита в соответствии с подразделом 5.4.
- соглашений с владельцами сертификатов, договоров.
- заявлений на выдачу и отзыв сертификатов.
- личных копий идентификационных данных.
- сертификатов пользователей УЦ, срок действия которых истек.
- отозванных сертификатов пользователей УЦ.
- списков отозванных сертификатов УЦ.
- протоколов работы программного обеспечения УЦ.
- протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемая для этого блокчейн доступна в Интернет.

5.5.2 Срок хранения архива

УЦ хранит архив на протяжении всего срока работы.

5.5.3 Защита архива

УЦ обеспечивает хранение архивных документов в соответствии с законодательством Республики Казахстан.

5.5.4 Резервное копирование архива

Электронные носители архива подлежат резервному копированию ежедневно.

5.5.5 Требования к простановке времени создания архивных записей

Не определено.

5.5.6 Условия архивирования

УЦ обеспечивает ведение архива в соответствии с законодательством Республики Казахстан.

5.5.7 Порядок получения и проверки информации, хранящейся в архиве

Доступ к архиву имеют только уполномоченные сотрудники Центра Сертификации.

5.6 Смена ключей Центра Сертификации

Заблаговременно, до окончания срока действия закрытого ключа уполномоченного лица Центра Сертификации, администратор Центра производит формирование нового закрытого ключа и сертификата уполномоченного лица Центра Сертификации и публикует его в соответствующий раздел хранилища сертификатов.

По окончании действия закрытого ключа, носители ключевой информации с закрытым ключом и его копиями уничтожаются по акту.

Все владельцы и пользователи сертификатов обязаны получить новый сертификат Центра Сертификации и добавить его в справочники сертификатов без удаления действующего сертификата Центра Сертификации.

5.7 Восстановление в случае компрометации или сбоев

5.7.1 Действия по предотвращению компрометации и сбоев

Для предотвращения потери данные Центра Сертификации (хранилище выпущенных сертификатов, ключи Центра Сертификации) архивируются и помещаются в специально предназначенные для этих целей хранилища. Архивирование хранилища выпущенных сертификатов и СОС осуществляется не реже одного раза в сутки.

5.7.2 Случаи повреждения оборудования, программных и/или аппаратных сбоев

В случае повреждения оборудования, программных и/или аппаратных сбоев, сведения о происшествии поступают к руководству Центра Сертификации, которое расследует происшествие и принимает необходимые меры по устранению последствий и недопущению повторения подобных инцидентов.

Восстановительные работы проводятся в соответствии с внутренним планом аварийного восстановления.

5.7.3 Компрометация ключа участника информационной системы

В случае если секретный ключ потерян или есть основания полагать, что информация о секретном ключе стала доступной третьим лицам, требуется немедленно направить в УЦ запрос на отзыв сертификата.

5.7.4 Восстановление работоспособности после аварии

В случае технических сбоев в работе УЦ отзыв сертификатов приостанавливается до восстановления работы УЦ.

5.8 Разрешение конфликтных ситуаций

5.8.1 Некорректность входящего электронного документа или электронной цифровой подписи, а также непризнание отправителем электронного документа факта отправки документа

Не определено.

5.8.2 Непризнание отправителем/получателем электронного документа его целостности и подлинности

Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон и уполномоченных лиц УЦ.

5.8.3 Процедура проверки ЭЦП документа

Процедура проверки ЭЦП электронного документа включает в себя проверку действительности использования сертификата на момент подписания, проверку подлинности ЭЦП и проверку соответствия использования ЭЦП сведениям в сертификате.

5.9 Прекращение работы УЦ

В случае прекращения работы УЦ принимает все меры по минимизации влияния указанного процесса на участников информационных систем в соответствии с действующим законодательством Республики Казахстан.

В случае принятия решения о прекращении своей деятельности удостоверяющий центр обязан за тридцать календарных дней до прекращения деятельности проинформировать об этом всех участников обслуживаемых им систем электронного документооборота и уполномоченный орган в сфере обеспечения информационной безопасности.

При прекращении деятельности удостоверяющего центра выданные им сертификаты и соответствующие ключи электронной цифровой подписи, сведения о владельцах сертификатов передаются в другие удостоверяющие центры по согласованию с владельцем сертификата.

6 ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1 Изготовление и установка ключевой пары

6.1.1 Изготовление ключей и используемые алгоритмы

Изготовление закрытых (секретных) ключей ЭЦП проводится лицом, подавшим заявление на выпуск сертификата самостоятельно с использованием сертифицированных средств, рекомендованных в данном Регламенте.

Ключи ЭЦП Центра Сертификации, формируются в сертифицированном криптографическом модуле и не могут быть извлечены в незащищенном виде.

Ключи ЭЦП формируются в соответствии с алгоритмом ГОСТ 34.310-2004.

6.1.2 Передача открытого ключа подписи в Центр Сертификации

При наличии действующего сертификата, владелец сертификата формирует запрос PKCS#10 на получение нового сертификата, содержащий открытый ключ. Запрос передается в формате PKCS#7 и содержит ЭЦП владельца действующего сертификата. DN имя владельца сертификата в запросе должно совпадать с именем в выпускаемом сертификате.

6.1.3 Передача открытых ключей подписей участникам информационных систем

УЦ публикует сертификаты и списки отозванных сертификатов в соответствии с порядком, описанном в настоящем Регламенте.

До начала использования сертификата участник информационной системы должен скачать и установить сертификаты уполномоченных лиц УЦ.

Скачав и установив сертификаты уполномоченных лиц Центра Сертификации, пользователь подтверждает свое полное и безоговорочное согласие с условиями использования сервисов УЦ.

6.1.4 Размеры ключей

При использовании криптографического преобразования по алгоритму СТ РК ГОСТ 34.310-2004:

- закрытый ключ – 256 бит.

открытый ключ – 512 бит.

6.1.5 Параметры генерации и проверки качества закрытого ключа

Определяются сертифицированным в соответствии с СТ РК 1073–2007 СКЗИ автоматически.

6.1.6 Цели использования ключа (порядок заполнения поля key usage сертификата x.509v3)

Заполняются в соответствии с политикой сертификата.

6.2 Защита закрытого ключа, требования к носителям ключевой информации и криптографическим модулям

Все действия с носителями ключевой информации должны осуществляться строго в соответствии с инструкциями по их эксплуатации и требованиями безопасности.

6.2.1 Контроль закрытого ключа (n из m), контролируемый несколькими держателями

В соответствии с эксплуатационной документацией средства криптографической защиты информации.

6.2.2 Депонирование закрытого ключа

См. в подразделе 4.12.

6.2.3 Резервное копирование закрытого ключа

Резервное копирование закрытого ключа пользователя не предусмотрено.

Резервное копирование закрытого ключа Центра Сертификации происходит в соответствии с эксплуатационной документацией средства криптографической защиты информации по схеме n из m. Резервная копия закрытого ключа Центра Сертификации хранится отдельно от криптографического модуля в зашифрованном архиве.

6.2.4 Архивирование закрытого ключа

Закрытые ключи с истекшим сроком действия подлежат уничтожению в соответствии с эксплуатационной документацией средства криптографической защиты информации. Архивное хранение закрытых ключей не допускается.

6.2.5 Запись закрытого ключа в криптографический модуль (носитель ключевой информации)

Производится штатными средствами модуля криптографической защиты информации в соответствии с эксплуатационной документацией.

Закрытые ключи ЭЦП создаются УЦ в облачной ЭЦП. Закрытые ключи ЭЦП облачной ЭЦП генерируются строго внутри HSM. Закрытый ключ не извлекается из HSM в открытом виде

6.2.6 Хранение закрытого ключа в криптографическом модуле (носителе ключевой информации)

После создания, закрытый ключ ЭЦП сохраняется в HSM в зашифрованном виде с использованием стандарта ГОСТ 28147-89. В качестве секретных значений участвуют пароль, заданный владельцем, который в УЦ не хранится. УЦ, для проверки пароля от закрытого ключа владельца, хранит хэш пароля в HSM.

6.2.7 Способы активации закрытого ключа

В соответствии с требованиями эксплуатационной документации средства криптографической защиты информации и действующим законодательством.

6.2.8 Способы деактивации закрытого ключа

Закрытый ключ деактивируется средством криптографической защиты информации автоматически, после выполнения связанных с его использованием операций или после выхода из личного кабинета на интернет-ресурсе УЦ.

6.2.9 Способы уничтожения закрытого ключа

Уничтожение закрытого ключа производится в соответствии с эксплуатационной документацией средства криптографической защиты информации.

6.2.10 Оценка криптографического модуля (носителя ключевой информации)

Носителем ключевой информации является специализированный носитель, в котором для защиты хранящихся закрытых ключей электронной цифровой подписи используется СКЗИ, имеющее сертификат соответствия требованиям стандарта СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования». Для записи сертификата УЦ использует облачную ЭЦП. HSM облачной ЭЦП:

1) соответствует не ниже третьего уровня безопасности в соответствии с требованиями, установленными СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования";

2) спроектирован с физической защитой периметра (защита от вскрытия корпуса), использующей датчики для определения факта вскрытия корпуса и последующего удаления ключевой информации, необходимой для HSM.

3) соответствует нормам эффективности защиты и методикам оценки защищенности информации и технических средств согласно требованиям действующего законодательства Республики Казахстан.

6.3 Другие особенности использования ключей

6.3.1 Архивирование открытых ключей подписей

Все сертификаты архивируются в соответствии с порядком резервного копирования, установленным в УЦ.

6.3.2 Распространение открытого ключа Центра Сертификации

Предоставление открытого ключа Центра Сертификации реализовано посредством публикации его сертификата в хранилище.

Безопасность сертификата Центра Сертификации реализована путем предоставления информации о серийном номере сертификата и его хеш-значения, с предоставлением доверяющим сторонам возможности его проверки.

В случае смены ключей подписи Центра Сертификации и выпуска нового сертификата Центра Сертификации, его распространение может производиться с использованием механизма кросс-сертификации.

6.3.3 Сроки действия сертификатов и ключей

Начало периода действия сертификата Центра Сертификации исчисляется с даты и времени его генерации. Срок действия корневого сертификата УЦ составляет 20 (двадцать) лет.

Срок действия пользовательского сертификата устанавливается УЦ, но не более 3 лет. Начало периода действия закрытого ключа владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата владельца сертификата.

6.3.4 Ограничения на использования ключей

Закрытый ключ Центра Сертификации используется для формирования ЭЦП сертификатов открытых ключей пользователей и списков отозванных сертификатов.

Закрытые ключи пользователей УЦ используются для формирования ЭЦП электронных документов и авторизации на интернет-ресурсах информационных систем.

6.4 Данные активации закрытых ключей

6.4.1 Генерация и установка данных активации закрытого ключа

Защита закрытого ключа обеспечивается несколькими защитными процессами:

- биометрическая аутентификация,
- вод кода доступа, сформированного владельцем сертификата.

6.4.2 Защита данных активации закрытого ключа

Запрещается передавать коды доступа третьим лицам и публиковать где-либо. Запрещается использование функции автоматического сохранения ключа в используемых средствах безопасности.

6.4.3 Особенности данных активации закрытого ключа

Не определено.

6.5 Средства управления компьютерной безопасностью

6.5.1 Специфические технические требования к компьютерной безопасности

Компьютеры, работающие в УЦ, удовлетворяют следующим требованиям:

- компьютеры для подписи сертификатов изолированы для неавторизованного доступа.
- операционные системы поддерживаются на высоком уровне защиты, при регулярном применении всех рекомендованных и соответствующих пакетов защиты, в том числе антивирусов.
- мониторинг осуществляется для обнаружения несанкционированных программных изменений.
- количество запущенных системных служб сведено к минимуму.

6.5.2 Оценка компьютерной безопасности

Не определено.

6.6 Технические средства управления жизненным циклом

6.6.1 Контроль работы системы

Не определено.

6.6.2 Средства управления безопасностью

Не определено.

6.6.3 Управление безопасностью жизненного цикла

Не определено.

6.7 Средства управления сетевой безопасностью

Безопасность аппаратных средств Центра Сертификации обеспечивается антивирусами и межсетевыми экранами.

6.8 Списание оборудования

Не определено.

7 ШАБЛОНЫ СЕРТИФИКАТОВ И СОС

7.1 Описание сертификата

7.1.1 Версия сертификата

Центр Сертификации выдает сертификаты в электронной форме в формате, основанном на рекомендациях ITU-T X.509v3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile).

7.1.2 Расширения сертификата

Сертификаты могут содержать следующие дополнения:

authorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
subjectKeyIdentifier	Идентификатор ключа владельца сертификата
ExtendedKeyUsage	Область (области) использования ключа, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение. Возможные значения:

	• Server Authentication • Client Authentication • Secure e-mail • Time stamping • IPSec (Tunnel, User)
KeyUsage	Назначение ключа. Возможные значения: • Цифровая подпись • Неотрекаемость • Шифрование ключей, • Шифрование данных.
Basic constraints (optional)	Тип субъекта
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов
certificatePolicies	Политика сертификата
Authority Information Access (optional)	Способ получения информации о статусе сертификата

7.1.3 Объектные идентификаторы алгоритмов

Центр Сертификации использует следующие идентификаторы алгоритмов средства электронной цифровой подписи:

ГОСТ 34.10-2004	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) sign(2)
ГОСТ 28147-89	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) enc(4)
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

7.1.4 Структура сертификата Корневого Центра Сертификации (Алгоритм ГОСТ 34.310-2004)

Название	**Содержание**
Версия	V3
Серийный номер	Уникальный серийный номер сертификата
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004
Поставщик	CN = Verigram O = Verigram Limited Liability Partnership C = KZ
Субъект	CN = Verigram O = Verigram Limited Liability Partnership C = KZ
Срок действия	действителен с действителен по
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде
Расширения сертификатов	Дополнения сертификатов (см. пункт 7.1.10)
Подпись	ЭЦП

7.1.5

7.1.6 Структура сертификата участника УЦ - физическое лицо (Алгоритм ГОСТ 34.310-2004)

Название	**Содержание**
Версия	V3
Серийный номер	Уникальный серийный номер сертификата

Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004
Поставщик	CN = Verigram O = Verigram Limited Liability Partnership C = KZ
Субъект	SERIALNUMBER = ИИН CN = ФИО C = KZ Phone = номер телефона
Срок действия	действителен с действителен по
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде
Расширения сертификатов	Дополнения сертификатов (см. пункт 7.1.10)
Подпись	ЭЦП

7.1.7 Структура сертификата участника УЦ - юридическое лицо (Алгоритм ГОСТ 34.310-2004)

Название	**Содержание**
Версия	V3
Серийный номер	Уникальный серийный номер сертификата
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004
Поставщик	CN = Verigram O = Verigram Limited Liability Partnership C = KZ

Субъект	SERIALNUMBER = ИИН CN = ФАМИЛИЯ ИМЯ OU = БИН O = НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ C = KZ Phone = номер телефона Title = Должность (Первый руководитель/Сотрудник с правом подписи/ Сотрудник организации) DN = Департамент
Срок действия	действителен с действителен по
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде
Расширения сертификатов	Дополнения сертификатов (см. пункт 7.1.10)
Подпись	ЭЦП

7.1.8 Ограничения, накладываемые на имена (идентификационные данные)

На идентификационные данные налагаются ограничения по содержанию, длинам строк и используемым символам в соответствии с ITU-T X.501 (Distinguished Names).

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

Serial Number	ИИН пользователя

Обязательными атрибутами поля идентификационных данных владельца сертификата являются:

Serial Number	ИИН/номер паспорта

OU	БИН для юридического лица

7.1.9 Объектный идентификатор политики сертификата

Подробно представлено в документе «Политика применения сертификатов ТОО «Вериграм».

7.1.10 Использование расширения Policy Constraints

Не определено.

7.1.11 Использование расширения Policy Qualifier

Не определено.

7.1.12 Порядок обработки расширений Certificate Policies, имеющих пометку critical

Решение о доверии к сертификату принимается участником УЦ самостоятельно.

7.2 Описание COC

7.2.1 Номер версии

УЦ формирует COC в электронной форме в формате, основанном на рекомендациях ITU-T X.509v3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile).

7.2.2 Расширения COC

Центр Сертификации может использовать следующие дополнения:

CRL number	Порядковый номер COC
Authority Key Identifier	Идентификатор ключа уполномоченного лица УЦ
Reason Code	Код причины отзыва сертификата. Возможные значения: ● Компрометация ключа пользователя ● Компрометация ключа Центра Сертификации ● Прекращение действия сертификата

7.2.3 Структура списка отозванных сертификатов (Алгоритм ГОСТ 34.310-2004)

Название	Содержание
Версия	V2
Поставщик	CN = Verigram O = Verigram Limited Liability Partnership C = KZ
Дата выпуска	действителен с
Дата обновления	действителен по
Расширения COC	Дополнения COC (см. пункт 7.2.2)
Отозванные сертификаты	Последовательность следующего вида: ● CertificateSerialNumber (серийный номер сертификата) ● Time (время обработки заявления на отзыв)
Алгоритм подписи	Алгоритм подписи СТ РК ГОСТ Р 34.310-2015
Подпись	ЭЦП

7.3 Описание OCSP

Протокол OCSP необходим доверяющим сторонам для определения статуса указанного сертификата в текущий момент времени. OCSP может использоваться для обеспечения требований, касающихся получения более своевременной информации об отмене, чем это возможно с использованием COC.

7.3.1 Номер версии

УЦ формирует квитанции OCSP в электронной форме версии 1 в соответствии с RFC 2560 Online Certificate Status Protocol - OCSP.

7.3.2 Расширения OCSP

Не определено.

8 ПРОВЕРКА СООТВЕТСТВИЯ И ДРУГИЕ ОЦЕНКИ

8.1 Частота или основания проведения оценки

Не определено.

8.2 Идентификация/квалификации эксперта

Не определено.

8.3 Отношение эксперта к оцениваемому объекту

Не определено.

8.4 Темы, затрагиваемые при проведении оценки

Не определено.

8.5 Действия, предпринимаемые в результате несоответствия функционирования УЦ данному документу

При выявлении нарушений в функционировании УЦ, разрабатывается план действий по устранению выявленных нарушений. Если выявленные нарушения привели к выдаче сертификатов, нарушающих безопасность УЦ, эти сертификаты будут немедленно отозваны. В случае выявления нарушений в функционировании, УЦ сообщит о действиях, которые необходимо предпринять для восстановления надлежащего функционирования. Если в процессе изготовления сертификатов Центр Сертификации функционировал с нарушениями, выпущенные в это время сертификаты должны быть отозваны.

8.6 Сообщение о результатах

Не определено.

9 ДРУГИЕ КОММЕРЧЕСКИЕ И ЮРИДИЧЕСКИЕ ВОПРОСЫ

9.1 Конфиденциальность коммерческой информации

9.1.1 Пределы конфиденциальной информации

Участники УЦ признают, что информация, доступ к которой ограничивается в соответствии с законодательством Республики Казахстан и представляющая собой коммерческую, служебную или личную тайны, рассматривается в качестве конфиденциальной информации.

9.1.2 Информация вне пределов конфиденциальной информации

Участники УЦ, признают, что содержимое сертификатов, информация об их отзыве или иная информация о статусе сертификатов, публичная часть хранилища и содержащаяся в них информация не рассматриваются в качестве конфиденциальной информации. Информация, не перечисленная в пункте 9.2.2, не рассматривается как конфиденциальная, если иное не предусмотрено действующим законодательством Республики Казахстан.

9.1.3 Обязательства по защите конфиденциальной информации

Участники УЦ обязаны хранить в тайне информацию, рассматриваемую в качестве конфиденциальной.

9.2 Конфиденциальность личной информации

УЦ обеспечивает защиту сведений о владельцах сертификатов и раскрывает их только в случаях, предусмотренных законодательством Республики Казахстан. Сведения о владельцах сертификатов, являющиеся конфиденциальными в соответствии с соглашением сторон, не включаются в общедоступный справочник.

9.2.1 План по обеспечению конфиденциальности

УЦ в своей деятельности руководствуется действующим законодательством Республики Казахстан по вопросам защиты персональных данных. В частности, УЦ не разглашает информацию, идентифицирующую заявителей на выпуск сертификатов, за исключением информации, перечисленной в пункте 9.2.3

УЦ собирает и обрабатывает персональные данные владельцев и пользователей сертификатов в соответствии с требованиями законодательства Республики Казахстан.

9.2.2 Информация, рассматриваемая как конфиденциальная

Идентификационные данные (материалы заявлений на регистрацию) пользователей УЦ (включая секретное слово (пароль) для доступа к услугам).

Протоколы работы служб УЦ, отчеты о проверках деятельности (внутренних и аудиторских) УЦ, планы восстановления после чрезвычайных происшествий и сбоев, меры безопасности, контролирующие функционирование аппаратного и программного обеспечения, администрирование служб сертификатов и регистрации.

Закрытые ключи электронной цифровой подписи и пароли сотрудников УЦ.

Закрытые ключи электронной цифровой подписи, шифрования и пароли пользователей услуг УЦ.

9.2.3 Информация не являющаяся конфиденциальной

Информация, которая не считается конфиденциальной:

- списки отозванных сертификатов.
- статус сертификата участника УЦ.
- сертификат участника УЦ.

Статистика относительно выдачи и отзыва сертификатов не содержит никакой личной информации и не считается конфиденциальной.

9.2.4 Обязательства по защите конфиденциальной информации

Участник УЦ обязуется:

✓ Не разглашать конфиденциальную информацию и использовать ее только в целях, для которых она была передана (получена).

✓ Соблюдать и принимать установленные УЦ меры по охране конфиденциальной информации, переданной (полученной) на материальных носителях:

- хранение и использование конфиденциальной информации должно осуществляться участником УЦ в местах, обеспечивающих физическую сохранность конфиденциальной информации и авторизацию доступа.
- на устройствах, являющихся материальным носителем ключевой информации, должны быть установлены пароли, с целью обеспечить сохранность данной информации и исключить доступ к конфиденциальной информации всех лиц, кроме лица, уполномоченного владеть доступом к носителю.
- любая попытка извлечения конфиденциальной информации за пределы мест ее хранения/использования не допускается.
- запрещается оставлять конфиденциальную информацию без присмотра.
- конфиденциальную информацию, во время работы (выполнения действий, операций) использовать так, чтобы исключить возможность ознакомления с нею лиц, не уполномоченных на такое ознакомление (доступ).
- копирование или иное воспроизведение конфиденциальной информации и/или ее материальных носителей, включая любые выписки и цитаты, допускается лишь с письменного согласия УЦ. При этом неудачные или ненужные копии и иные результаты воспроизведения конфиденциальной информации (ее материальных носителей) подлежат обязательному уничтожению с помощью специальных механических устройств или вручную. В отношении копий и иных результатов воспроизведения конфиденциальной информации и/или ее материальных

носителей участник УЦ обязан придерживаться тех же мер защиты, как и в отношении оригиналов. Единовременное использование одного и того же экземпляра ключевой информации на разных устройствах строго запрещается.

- при утере (повреждении) или разглашении, подозрении либо угрозе разглашения (компрометации) конфиденциальной информации, а также при обнаружении признаков незаконного получения (использования) конфиденциальной информации третьими лицами, незамедлительно сообщить об этом УЦ, отправив запрос на отзыв сертификатов.
- при предоставлении конфиденциальной информации в установленных законодательством случаях органу государственной власти, иным государственным органам, органам местного самоуправления одновременно с таким предоставлением уведомить об этом УЦ.

9.2.5 Предупреждение об использовании и разрешение на использование конфиденциальной информации

Не определено.

9.2.6 Разглашение информации в случаях, установленных законодательством

Деятельность УЦ регулируется законодательством Республики Казахстан. УЦ обязуется использовать конфиденциальную и личную информацию для установления полномочий в соответствии с установленным порядком.

9.2.7 Другие основания разглашения информации

Не определено.

9.3 Права на интеллектуальную собственность

Регламент описывает порядок предоставления услуг УЦ, принадлежащей ТОО «Вериграм», и правила их использования участниками информационных систем. ТОО «Вериграм» оставляет за собой права интеллектуальной собственности на сертификаты, которые выпускает УЦ, и на информацию об их статусе. При этом не запрещается копирование и распространение сертификатов на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования сертификатов в соответствии с настоящим Регламентом. ТОО «Вериграм» также не запрещает использование информации о статусе сертификатов для выполнения функций доверяющей стороны в соответствии с настоящим Регламентом. Участники УЦ сохраняют все свои права на все торговые и тому подобные марки и имена,

содержащиеся в заявлениях на выпуск сертификатов и отличительные (DN-)имена в выпущенных сертификатах.

Ключевые пары, которые соответствуют сертификатам, выпущенным УЦ, составляют собственность (в том числе интеллектуальную) владельцев сертификатов в независимости от физических носителей, на которых хранятся эти ключевые пары и которыми они защищаются.

При составлении настоящего документа использовались следующие материалы:

- LDAP (RFC 2251 Lightweight Directory Access Protocol (v3)).
- RFC 3647 Certificate Policy and Certification Practices Framework.
- RFC 2560 Online Certificate Status Protocol – OCSP.
- RFC 3161 Time-Stamp Protocol – TSP.
- RFC 4210 Public Key Infrastructure Certificate Management Protocol.
- RFC 5280 Certificate and Certificate Revocation List (CRL) Profile.

9.4 Обязанности

9.4.1 Обязанности Центра Сертификации

Центр Сертификации ответственен за изготовление сертификатов и последующее управление ими в соответствии с настоящим Регламентом, в частности, он:

- обрабатывает запросы на выдачу сертификатов и издает новые сертификаты, в соответствии с запрашиваемой областью применения (политикой).
- подтверждает запросы на выдачу сертификатов от участников УЦ, запрашивающих сертификаты согласно процедурам, описанным в данном документе.
- издает сертификаты на основе запросов от аутентифицированных заявителей.
- посылает уведомление о статусе выпущенных сертификатов по запросам заявителей.
- обеспечивает доступ к хранилищу сертификатов.
- публикует информацию о выпущенных сертификатах в хранилище сертификатов.
- публикует корневой сертификат Центра Сертификации в хранилище сертификатов.
- обрабатывает запросы на отзыв сертификатов.

- подтверждает запросы на отзыв сертификатов от заявителей согласно процедурам, описанным в данном документе.
- выпускает СОС.
- публикует информацию об отозванных сертификатах.

9.4.2 Обязанности владельца сертификата

Направляя запрос на выдачу сертификата, заявители соглашаются:

- предоставить достоверную и точную информацию при регистрации в УЦ.
- своевременно уведомлять УЦ об изменении своих учетных данных, предоставленных в документах при регистрации.
- использовать сервисы УЦ в соответствии с настоящим Регламентом.
- применять для формирования ЭЦП только действующий закрытый ключ ЭЦП, соответствующий открытому ключу ЭЦП, указанному в сертификате участника УЦ.
- применять секретные ключи и соответствующие им сертификаты в соответствии с областью применения и политиками, указанными в сертификате.
- использовать сложный пароль длиной не менее 8 символов для защиты личного ключа.
- не использовать секретные ключи и соответствующие им сертификаты по истечении срока их действия.
- не использовать секретные ключи и соответствующие им сертификаты в случае их отзыва.
- немедленно направить в УЦ запрос на отзыв сертификата в случае, если секретный ключ потерян или есть основания полагать, что информация о секретном ключе стала доступной третьим лицам.
- не позднее, чем за 14 (четырнадцать) рабочих дней до истечения срока действия сертификата, отправить электронный запрос на выпуск соответствующего нового сертификата.

9.4.3 Обязанности доверяющих сторон

При использовании сертификата, выданного УЦ, доверяющие стороны соглашаются:

- принять условия и следовать процедурам, описанным в настоящем Регламенте.

- проверить сроки действия, ЭЦП и политики сертификата.
- не использовать секретные ключи и соответствующие им сертификаты по истечении срока их действия.
- проверить статус сертификата, используя списки отозванных сертификатов и/или службу проверки статуса сертификата в режиме online.
- не использовать секретные ключи и соответствующие им сертификаты в случае их отзыва.
- использовать сертификат в соответствии с настоящим Регламентом, политиками сертификатов и действующим законодательством.

Сертификат не может быть использован до наступления срока действия или после истечения срока действия, в случае неверной ЭЦП и/или после приостановления/отзыва.

9.4.4 Обязанности других участников

Не определено.

9.5 Отзыв гарантий

УЦ не несет ответственности за последствия, возникшие в результате нарушения пользователями и/или доверяющими сторонами положений настоящего Регламента и/или действующего законодательства.

9.6 Ограничения ответственности

УЦ гарантирует обработку запросов на выдачу сертификата согласно процедурам, описанным в настоящем Регламенте.

УЦ гарантирует обработку запросов на отзыв согласно процедурам, описанным в настоящем Регламенте.

УЦ гарантирует отсутствие в сертификатах ключей умышленных искажений данных участников УЦ.

Претензии к УЦ ограничиваются указанием на несоответствие ее действий настоящему Регламенту.

9.7 Срок действия и прекращение действия

9.7.1 Срок действия

Регламент вступает в силу с момента его публикации на сайте https://verigram.kz и действует до публикации новой редакции Регламента на сайте https://verigram.kz.

9.7.2 Прекращение действия

Регламент прекращает действие в случае замены на новую редакцию Регламента.

9.7.3 Последствия прекращения действия и положения, остающиеся действительными

С момента прекращения действия настоящего Регламента участники УЦ остаются связанными его условиями по всем сертификатам до момента истечения периода их действия.

9.8 Индивидуальные уведомления и сообщения участникам

Не определено.

9.9 Поправки

9.9.1 Внесение поправок

Участников УЦ не уведомляют заранее о внесении поправок в настоящий Регламент. Поправки утверждают прежде, чем новый документ будет опубликован на сайте https://verigram.kz.

Механизм и период уведомления

УЦ оставляет за собой право без предварительного уведомления вносить изменения и дополнения в Регламент, включая, но не ограничиваясь: исправлением опечаток, изменением адресов ссылок и контактной информации.

9.9.2 Основания, при которых номер версии документа должен быть изменен

Версия документа обновляется всякий раз, когда в документ вносятся поправки.

9.10 Условия разрешения споров

Разрешение юридических споров, являющихся результатом функционирования УЦ, осуществляется в соответствии с законодательством Республики Казахстан.

9.11 Действующее законодательство

Юридическая сила, толкование данного документа осуществляется в соответствии с действующим законодательством Республики Казахстан.

9.12 Соответствие действующему законодательству

УЦ осуществляет свою деятельность в соответствии с действующим законодательством Республики Казахстан.

9.13 Различные положения

9.13.1 Полнота соглашения

Не определено.

9.13.2 Передача прав

Не предусматривается.

9.13.3 Независимость разделов документов

В случае если часть положений настоящего Регламента будет признана неосуществимой судом или уполномоченным государственным органом, остальная ее часть сохраняет силу.

9.13.4 Взыскание (юридические издержки и освобождение от обязательств)

Не определено.

9.13.5 Форс - мажор

УЦ освобождается от ответственности за неисполнение либо ненадлежащее исполнение своих обязательств в соответствии с настоящим Регламентом, если оно явилось следствием наступления обстоятельств непреодолимой силы.

9.14 Прочие положения

Не определено.