Утверждено
приказом Генерального директора
ТОО «BTS Digital»
№2023/0016-п от «12 » октября 2023 года

BTS·Digital

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА «ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ ТОО «BTS Digital»

Астана, 2023

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Настоящий Регламент (далее – Регламент) Удостоверяющего Центра (далее – УЦ) «Инфраструктура открытых ключей» ТОО «BTS Digital» описывает порядок предоставления услуг принадлежащего ТОО «BTS Digital» 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»
- «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.
- “Правилами создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре”, утвержденными приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ

1.1 Обзор

Регламент определяет правила, механизмы и условия предоставления и использования услуг УЦ, включая права, обязанности и ответственность участников УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, включая, но, не ограничивая такие операции, как выпуск, использование и отзыв сертификатов открытых ключей.

1.2 Наименование и идентификация документа

Наименование документа: Регламент Удостоверяющего Центра «Инфраструктура открытых ключей ТОО «BTS Digital».

Объектный идентификатор: 1.2.398.3.17.1 – Регламент Удостоверяющего Центра «Инфраструктура открытых ключей ТОО «BTS Digital».

Версия документа: 4.0.

Актуальная редакция настоящего документа доступна по ссылке: https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf

1.3 Участники УЦ

1.3.1 Центр сертификации

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

1.3.2 Центр Регистрации

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

Центр регистрации – структурное подразделение удостоверяющего центра или действующее на основании договора с удостоверяющим центром юридическое лицо, ответственные за идентификацию заявителя, и/или прием документов на выдачу или отзыв регистрационных свидетельств и предоставление заявителю готовых регистрационных свидетельств

1.3.3 Интернет-ресурс Удостоверяющего центра

Интернет-ресурс УЦ, расположенный по адресу https://passport.aitu.io/ - сервис, включающий в себя систему Облачной ЭЦП, обеспечивающий идентификацию, аутентификацию пользователя, в том числе силами Центра регистрации

1.3.4 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.

1.3.5 Владелец сертификата

Владелец сертификата – физическое лицо, на имя которого Центром Сертификации выпущен сертификат, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в сертификате.

1.3.6 Пользователь сертификата

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

1.3.7 Доверяющая сторона

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

1.3.8 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 Online Certificate Status Protocol (OCSP).

1.4 Использование сертификатов

1.4.1 Допустимое использование сертификата

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

1.5 Управление документом

1.5.1 Организация, ответственная за содержание документа

ТОО «BTS Digital»
Республика Казахстан, 010000
г. Астана, район Алматы, пр. Рақымжан Қошқарбаев, 1/4

1.5.2 Контактное лицо

Байгаскин Жаслан
Менеджер продукта
Email: zhaslan.baygaskin@btsdigital.kz

1.5.3 Лица, утверждающие изменения

Изменения в документе утверждаются первым руководителем ТОО «BTS Digital» либо уполномоченным им лицом.

1.5.4 Процедура утверждения изменений

Официальным уведомлением участников информационных систем об утверждении изменений настоящего Регламента является его публикация по адресу: https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf.

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

1.6 Определения и сокращения

Электронная цифровая подпись (далее - ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

УЦ - удостоверяющий центр;

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

Закрытый ключ ЭЦП - последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

Средства электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

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

Метка времени – электронный документ, выпускаемый 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 в хранилище УЦ и уведомлению владельца сертификата об аннулировании (отзыве) сертификата.

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

Сертификат – регистрационное свидетельство, электронный документ, выпускаемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи».

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 подписчиков УЦ, отозванных на момент выпуска СОС. Список отозванных сертификатов публикуется по адресу: https://passport.aitu.io/revoked-esigns

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

2. ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

2.1 Публикация регламента УЦ

При внесении каких-либо изменений Регламент публикуется по адресу: https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf.

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

Выпущенные сертификаты и СОС вносятся в хранилище сертификатов и публикуются не позднее даты начала их действия. Срок действия 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 ко всей конфиденциальной информации.

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 выпускает сертификаты, соответствующие рекомендациям ITU-T X.509 версии 3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Выпущенные 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

Указанный в сертификатах ИИН физического лица или номер паспорта для физических лиц нерезидентов Республики Казахстан должен точно совпадать со сведениями, указанными в удостоверении личности этого физического лица или паспорте физического лица.

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

Для сертификатов юридических лиц атрибут O (Organization) содержит название юридического лица.

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).

UID (Unique ID) может содержать уникальный символ и/или номер. Дополнительно, могут использоваться атрибуты OU (Organization Unit), L (Locality)

3.1.3 Использование псевдонимов

Не определено.

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 Центр регистрации может добавить UID, 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 или юридическое 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 или юридическое 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, номер UID), позволяющий однозначно идентифицировать их владельцев.

3.1.6 Использование торговых марок

Не определено.

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 регистрационного свидетельства 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 Регистрационного свидетельства 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 Процедура аутентификации физического лица

Для получения Регистрационного свидетельства, заявитель посредством Центра регистрации подтверждает свою аутентичность и подлинность предоставленных им биометрических и персональных данных (цифровых данных, удостоверяющих личность) путем прохождения двухфакторной аутентификации, одной из которых является биометрическая аутентификация.

Далее заявитель через интернет-ресурс УЦ предоставляет заявление на выдачу Регистрационного свидетельства от физического лица (Приложение 1).

УЦ вправе отказать в выпуске ЭЦП в случаях:

- истечения срока действия документа, удостоверяющего личность;
- предоставления заявителем недостоверных сведений;
- в соответствии со вступившим в законную силу решением суда;
- либо недостижения заявителем шестнадцатилетнего возраста.

3.2.3 Процедура аутентификации юридического лица

Для получения Регистрационного свидетельства, заявитель от юридического лица, его филиала или представительства (либо его представитель по доверенности) посредством Центра регистрации подтверждает свою аутентичность и подлинность предоставленных им

биометрических и персональных данных (цифровых данных, удостоверяющих личность) путем прохождения двухфакторной аутентификации, одной из которых является биометрическая аутентификация.

Далее юридическое лицо его филиал или представительство (либо его представитель по доверенности) предоставляет в Центр регистрации документы или копии документов при получении через интернет-ресурс удостоверяющего центра :

- заявление на выдачу Регистрационного свидетельства от юридического лица (Приложение 4);
- справку либо свидетельство о государственной регистрации (перерегистрации) юридического лица заявителя в качестве юридического лица (либо копию, удостоверенную нотариально в случае непредставления оригиналов);
- доверенность на представителя юридического лица, с указанием полномочия представлять документы на выдачу регистрационных свидетельств удостоверяющего центра и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью. При отсутствии печати организации, доверенность на представителя заявителя заверяется нотариально, с указанием полномочий представлять документы на выдачу регистрационного свидетельства и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью;
- для первого руководителя юридического лица или лица, исполняющего его обязанности, взамен доверенности представляется справка с места работы, либо заверенная печатью юридического лица (при ее наличии) копия приказа (решения, протокола) о назначении на должность первого руководителя или лица, исполняющего его обязанности.

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, не подвергающиеся проверке

Не определено.

3.2.5 Дополнительные условия аутентификации

УЦ оставляет за собой право осуществлять проверку сведений, переданных УЦ, а также требовать от заявителя представления дополнительных документов, подтверждающих личность заявителя.

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 аутентификации 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 аутентификации запросов при плановой (очередной) замене ключей

Процедура аутентификации в случае плановой смены ключей может проводиться в порядке, описанном в подразделе 3.2.

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

Процедура аутентификации при смене ключей после отзыва (аннулирования) сертификата проводится в порядке, описанном в подразделе 3.2.

3.3.3 Процедура аутентификации заявителя при отзыве (аннулировании) сертификата

Для отзыва Регистрационного свидетельства физического лица, заявитель через интернет-ресурс УЦ предоставляет в УЦ Заявление на отзыв Регистрационного свидетельства (Приложение 2).

Для отзыва регистрационного свидетельства, владелец регистрационного свидетельства – юридическое лицо, его филиал или представительство (либо его представитель по доверенности) нарочно предоставляет следующие документы в центр регистрации, либо электронные копии документов при осуществлении отзыва через интернет-ресурс удостоверяющего центра:

1) заявление на отзыв регистрационного свидетельства от юридического лица по форме, согласно приложению __ к настоящему регламенту;

2) документ, удостоверяющий личность, для идентификации;

3) доверенность на представителя заявителя.

Юридическое лицо отзывает регистрационное свидетельство, выданное на его филиал и/или представительство при предоставлении доверенности на представителя заявителя от юридического лица. При этом подпись лица, указанного в заявлении на отзыв регистрационного свидетельства, в доверенности не требуется.

При отсутствии печати организации, доверенность на представителя заявителя заверяется нотариально, с указанием полномочия представлять документы на отзыв регистрационного свидетельства и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью.

Для первого руководителя юридического лица не требуется предоставление доверенности для отзыва регистрационного свидетельства.

Для отзыва регистрационного свидетельства, владелец регистрационного свидетельства – юридическое лицо, его филиал или представительство через интернет-ресурс УЦ предоставляет Заявление на отзыв регистрационного свидетельства от юридического лица (Приложение 5).

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА

4.1 Заявление на выпуск сертификата ЭЦП

4.1.1 Лица, имеющие право подавать заявления на выпуск сертификатов

Процесс получения сертификата инициируется самим физическим лицом.

4.1.2 Процедура и обязательства по регистрации

Физическое лицо, инициируя процесс получения регистрационного свидетельства, подтверждает свое полное и безоговорочное присоединение к настоящему Регламенту.

4.2 Обработка заявления на выпуск сертификата

4.2.1 Процедура идентификации и аутентификации заявления

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

4.2.2 Выпуск или отказ в выпуске сертификата

4.2.3 УЦ выпускает сертификат в случае успешного прохождения заявителем процедур идентификации и аутентификации, описанных в подразделе 3.2.

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 выпуске регистрационного свидетельства, производится официальное уведомление заявителя не позднее пяти рабочих дней посредством каналов связи.

Порог чувствительности и достоверность распознавания в пределах допущений исходя из False Positive Ratio (FPR) и False Negative Ratio (FNR).

FPR – ложно-положительная доля, вероятность ложного принятия положительного решения. Считается как доля количества негативных событий, ошибочно отнесенных к положительным, к общему фактическому количеству негативных событий. FPR показывает, какую долю из объектов

отрицательного класса алгоритм предсказал неправильно, и показатель FPR в Системе составляет 0,0001% по результатам проверки в Национальном институте стандартов и технологий NIST.

False Negative Ratio (FNR) - представляет собой статистический показатель, полученный в ходе проверки и оценки эффективности биометрической системы с использованием данных, предоставленных Национальным институтом стандартов и технологий (NIST), FNR в Системе составляет 0.83%.

4.2.4 Сроки рассмотрения заявления на выпуск сертификата

УЦ обрабатывает заявления на выпуск сертификата заявителей в течение 5 рабочих дней после завершения процедуры идентификации и 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).

4.3.2 Уведомление заявителя о факте изготовления сертификата

Сертификат активируется Центром регистрации по установленному ключу и публикуется в хранилище сертификатов Центра Сертификации.

4.4 Признание сертификата

4.4.1 Действия владельца сертификата, означающие признание сертификата

Получение сертификата в личном кабинете владельцем сертификата означает признание сертификата.

4.4.2 Публикация сертификата

Центр Сертификации публикует сертификат в хранилище сертификатов в соответствии с настоящим Регламентом. Публикация сертификата происходит сразу после активации.

4.4.3 Уведомление участника УЦ о выпуске сертификата

Официальным уведомлением пользователей УЦ о выпуске сертификата является его публикация в хранилище сертификатов и его передача пользователю УЦ.

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 выпущенных сертификатов и сертификатов уполномоченных лиц Центра сертификации участникам информационных систем. Каждый сертификат, выпущенный УЦ, содержит ссылку на списки отозванных сертификатов.

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.

4.5.3 Хранение закрытого ключа владельцем

Владелец регистрационного свидетельства обязан принимать меры для защиты принадлежащего ему закрытого ключа электронной цифровой подписи от неправомерного доступа и использования. Закрытые ключи электронной цифровой подписи хранятся в облачной ЭЦП в удостоверяющем центре согласно правилам создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре.

4.6 Обновление сертификата

Обновление сертификата не предусмотрено.

4.7 Смена ключей

Не предусмотрено.

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 сертификата

4.9.1 Основания для отзыва сертификата

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

- по требованию владельца сертификата;
- установления факта предоставления недостоверных сведений при получении сертификата;
- наличия вступившего в законную силу решения суда;
- при подозрении на компрометацию ключа.

4.9.2 Лица, уполномоченные подавать заявления на отзыв сертификатов

Заявление на отзыв сертификата может подавать его владелец и/или сотрудник подразделения ИБ.

4.9.3 Процедура идентификации и аутентификации заявления

Процедура идентификации владельца сертификата при обработке 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. Запрос на отзыв сертификата заверяется подписью владельца сертификата.

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 посредством входа в личный кабинет на интернет-ресурсе УЦ, 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.

СОС обновляется по окончанию его срока действия (по умолчанию – 1 неделя).

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 Требования к осуществлению проверки действительности ЭЦП

УЦ предоставляет интернет-ресурс для осуществления проверки действительности ЭЦП по адресу: https://passport.aitu.io/e-sign-verification

Проверка ЭЦП на электронном документе осуществляется путем использования открытого ключа ЭЦП, который содержится в регистрационном свидетельстве подписывающей стороны.

Проверка ЭЦП осуществляется в обратном порядке, по которому производилась подпись документа, по следующей схеме:

1) с помощью открытого ключа ЭЦП отправителя дешифруется хэш сообщения (подпись отправителя);

2) с помощью хэш-функции вычисляется контрольная сумма оригинального сообщения.

Производится сверка двух контрольных сумм, если они равны, то ЭЦП считается верной (определен положительный результат проверки ЭЦП), если не равны, то ЭЦП считается не действительной (определен отрицательный результат проверки ЭЦП).

4.9.13 Другие способы извещения участников информационных систем о фактах отзыва сертификатов

Официальным уведомлением участников УЦ об отзыве сертификата является публикация СОС в хранилище сертификатов, для пользователя сертификата - отображение статуса действия в личном кабинете пользователя на интернет-ресурсе УЦ, уведомление с помощью SMS.

4.9.14 Срок хранения отозванных сертификатов

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

4.9.15 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.

4.9.16 Условия 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;
- наличия вступившего в законную силу решения суда;
- при подозрении на компрометацию ключа.

4.9.17 Лица, уполномоченные подавать заявления на отзыв сертификата

Запрос на отзыв сертификата в УЦ направляется владельцем сертификата и/или сотрудником подразделения ИБ. Запрос на отзыв сертификата заверяется ЭЦП владельца сертификата.

4.9.18 Процедура подачи заявления на отзыв сертификата

Процедура отзыва сертификата осуществляется посредством интернет-ресурса УЦ с личного кабинета пользователя.

4.9.19 Ограничение срока отзыва 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. Статус действия ЭЦП также можно проверить посредством интернет-ресурса УЦ в личном кабинете пользователя.

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 и законодательства Республики Казахстан.

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

Помещение Центра Сертификации оборудовано 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.

Электрические сети и электрооборудование, используемые в Центре Сертификации, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

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

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

5.1.7 Уничтожение документированной информации

Решение 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

Резервное копирование выполняется один раз в сутки в соответствии с требованиями внутренних нормативных документов по информационной безопасности.

5.2 Организационные меры обеспечения безопасности

5.2.1 Разграничение ролей (полномочий)

В центре регистрации интегрируется модуль или подсистема или система которая будет проверять валидность данных пользователей, администратора, 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 оборудование 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.
- 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.

Серверы «CA SERVER» и «STORE SERVER» регистрируют события операционной системы.

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 впоследствии находят отражения в новых версиях ПО.

5.4.3 Срок хранения журналов аудита

Журналы аудита подлежат архивированию 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.

Журналы протоколирования событий удостоверяющего центра оперативно передаются в систему управления событиями ИБ, используемую в Компании в соответствии с «Инструкцией по мониторингу событий и управлению инцидентами ИБ».

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.
- заявлений на выдачу и отзыв сертификатов.
- сертификатов пользователей УЦ, срок действия которых истек.
- отозванных сертификатов пользователей УЦ.
- списков отозванных сертификатов УЦ.
- протоколов работы программного обеспечения УЦ.
- служебных электронных документов.

УЦ обеспечивает протоколирование следующих событий:

- формирование закрытого ключа ЭЦП облачной ЭЦП;
- использование закрытого ключа ЭЦП облачной ЭЦП;
- удаление (стирание) закрытого ключа ЭЦП облачной ЭЦП.

Срок хранения протоколов работы составляет один год с даты истечения срока действия регистрационного свидетельства. При протоколировании действий записывается следующая информация:

- идентификатор владельца;
- дата, время;
- событие.

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

Срок хранения архива УЦ составляет от 5 до 15 лет и зависит от типа регистрируемых событий согласно требованиям действующего законодательства Республики Казахстан.

5.5.3 Защита архива

УЦ обеспечивает хранение электронных 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 электронного архива в соответствии с законодательством Республики Казахстан.

5.5.7 Порядок получения и проверки информации, хранящейся в архиве

Доступ к электронному 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. Для этого используются механизмы кросс-сертификации Удостоверяющего центра и публикация сертификата Центра Сертификации в хранилище Удостоверяющего центра.

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 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.

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 УЦ на основании заявления на выпуск сертификата 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 СТ РК ГОСТ 34.310-2004.

6.1.2 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.

6.1.3 Размеры ключей

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

- закрытый ключ – 256 бит.
- открытый ключ – 512 бит.

6.1.4 Параметры генерации и проверки качества закрытого ключа

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

6.1.5 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. Закрытые ключи хранятся в Облачной ЭЦП.

6.2.1 Требования к носителям ключевой информации

Не определено.

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

В соответствии с эксплуатационной документацией средства криптографической защиты информации.

6.2.3 Депонирование закрытого ключа

Не определено. (п.4.12)

6.2.4 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.

6.2.5 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.

Архивирование ключевой информации с HSM возможно только в зашифрованном виде и только с разделением ключа шифрования по схеме M из N (не менее 3 из 5). Ключи шифрования по схеме M из N хранятся на защищенных токенах. Защищенные токены используются только при восстановлении архива на резервном HSM.

6.2.6 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.

6.2.7 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.

6.2.8 Способы активации закрытого ключа

Все владельцы сертификатов обязаны защищать доступ к своему личному кабинету на интернет-ресурсе УЦ и не передавать установленные защитные коды третьим лицам. В случае передачи защитных кодов третьим лицам, пользователь сам несет ответственность за сохранность и передачу личных данных, а также использование ЭЦП.

6.2.9 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.

6.2.10 Способы уничтожения закрытого ключа

Уничтожение закрытого ключа производится в соответствии с эксплуатационной документацией средства криптографической защиты информации. Перед уничтожением закрытого ключа УЦ будет уведомлять пользователя с помощью интернет-ресурса УЦ.

6.2.11Оценка 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 Регистрационного свидетельства 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 сертификата УЦ составляет 10 (десять) лет.

Срок действия пользовательского сертификата, от трех месяцев до трех лет, устанавливается УЦ. 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:
- видеоидентификация с помощью liveness detection,
- биометрическая аутентификация,
- ввод 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 выпускает 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
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)
СТ РК ГОСТ Р 34.11-2015	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) hash(1)
ГОСТ 28147-89	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) enc(4)

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

Название	**Содержание**
Версия	V3
Серийный номер	Уникальный серийный номер сертификата
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Поставщик	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) C = KZ
Субъект	CN = BTSD CA O = BTS Digital 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 Структура сертификата участника УЦ (Алгоритм СТ РК ГОСТ 34.310-2004)

Название	**Содержание**
Версия	V3
Серийный номер	Уникальный серийный номер сертификата
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Поставщик	CN = BTSD CA O = BTS Digital C = KZ
Субъект	SERIALNUMBER = ИИН/номер паспорта

Название	**Содержание**
	UID = текст и/или номер присвоенный УЦ
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)
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Подпись	ЭЦП

7.1.6 Структура сертификата участника УЦ юридического лица (Алгоритм СТ РК ГОСТ 34.310-2004)

Название	**Содержание**
Версия	V3
Серийный номер	Уникальный серийный номер сертификата
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Поставщик	CN = BTSD CA O = BTS Digital C = KZ
Субъект	SERIALNUMBER = ИИН/номер паспорта O = название организации (места работы) OU = BINбизнесидентификационный номер C = страна UID
Срок действия	действителен с действителен по
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде

Название	**Содержание**
Расширения сертификатов	Дополнения сертификатов (см. пункт 7.1.10)
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Подпись	ЭЦП

7.1.7 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, БИН для юридического лица

7.1.8 Объектный идентификатор политики сертификата

Подробно представлено в документе «Политика применения регистрационных свидетельств ТОО «BTS Digital» (https://passport.aitu.io/assets/resources/pdf/ca/certification-key-policy.pdf).

7.1.9 Использование расширения Policy Constraints

Не определено.

7.1.10 Использование расширения Policy Qualifier

Не определено.

7.1.11 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 ● Отзыв сертификата ● Инициирование запроса от пользователя ● По решению УЦ

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

Название	**Содержание**
Версия	V2
Поставщик	CN = BTSD CA O = BTS Digital 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)

Название	**Содержание**
Алгоритм подписи	Алгоритм подписи СТ РК ГОСТ Р 34.310-2004
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

В рамках аудита рассматривается полнота и качество выполнения требований в отношении финансово-хозяйственной деятельности и программно-технического комплекса, в том числе:

- раскрытие бизнес-практик УЦ.
- целостность услуг.

8.5 Действия, предпринимаемые в случае несоответствия функционирования УЦ данному документу

При выявлении нарушений в функционировании УЦ, разрабатывается план действий по устранению выявленных нарушений. Если выявленные нарушения привели к выпуску 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 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 выпуска 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 интернет-ресурс УЦ.
- 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 сертификата.
- 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 с помощью обращения техническую поддержку интернет-ресурса 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, принадлежащего ТОО «BTS Digital», и правила их использования участниками информационных систем. ТОО «BTS Digital» оставляет за собой права интеллектуальной собственности на сертификаты, которые выпускает УЦ, и на информацию об их статусе. ТОО «BTS Digital» 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 марки и имена, содержащиеся в заявлениях на выпуск сертификатов и отличительные (DN-) имена в выпущенных сертификатах.

Ключевые пары, которые соответствуют сертификатам, выпущенным УЦ, являются собственностью (в том числе интеллектуальной) владельцев сертификатов независимо от материальных носителей, на которых хранятся эти ключевые пары и которыми они защищаются.

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 выпуск сертификатов и издает новые сертификаты, в соответствии с запрашиваемой областью применения (политикой).
- подтверждает запросы на выпуск сертификата 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 Центра регистрации

Центр регистрации (модуль или подсистема или система) ответственен за проведение процедур идентификации и аутентификации, описанных в подразделе 3.2, в частности:

- проверяет информацию, предоставленную заявителем при участии Центра идентификации и верификации в процессе регистрации в УЦ, на полноту, достоверность и точность.
- передает запросы на выпуск сертификатов по защищенному каналу в УЦ.
- осуществляет консультацию заявителей, посредством пользовательского интерфейса, на предмет прохождения процедур идентификации и аутентификации в УЦ.

9.4.3 Обязанности владельца сертификата

Направляя запрос на выдачу сертификата, заявители соглашаются:

- предоставить достоверную и точную информацию при регистрации в УЦ.
- своевременно загружать действующий документ, удостоверяющий личность.
- использовать интернет-ресурс 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.
- обеспечивать сохранность доступа к своему личному кабинету на интернет-ресурсе УЦ и не допускать неправомерного распространения информации о своем закрытом ключе.
- принимать разумные меры для предотвращения доступа, раскрытия или несанкционированного использования личного ключа, в том числе, но, не ограничиваясь, поддерживать на высоком уровне защиту операционной системы, при регулярном применении всех рекомендованных и соответствующих пакетов защиты, в том числе антивирусов и межсетевых экранов.
- немедленно направить в УЦ запрос на отзыв сертификата в случае, если есть основания полагать, что информация о секретном ключе стала доступной третьим лицам.

9.4.4 Обязанности доверяющих сторон

При использовании сертификата, выпущенного УЦ, доверяющие стороны соглашаются:

- принять условия и следовать процедурам, описанным в настоящем Регламенте.
- проверить сроки действия документа удостоверяющего личность, 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.
- 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, а также в случае неверной ЭЦП и/или после отзыва.

9.4.5 Обязанности других участников

Нет

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 его действий настоящему Регламенту.

9.7 Срок действия и прекращение действия

9.7.1 Срок действия

Регламент вступает в силу с момента его публикации по адресу https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf и действует до публикации новой редакции Регламента.

9.7.2 Прекращение действия

Регламент прекращает действие в случае замены на новую редакцию Регламента.

9.7.3 Последствия прекращения действия и положения, остаются 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 по ссылке https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf. Поправки также публикуются по ссылке https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf.

9.9.2 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.

9.9.3 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.

10. ПРИЛОЖЕНИЯ

Приложение №1 - Форма “Заявление на выдачу регистрационных свидетельств (от физического лица)”

Приложение №2 Форма “Заявление на отзыв регистрационных свидетельств” (от физического лица)

Приложение №3 - Форма “Регистрационное свидетельство в форме электронного документа”

Приложение № 4 - Форма “Заявление на выдачу регистрационных свидетельств (от юридического лица)”

Приложение 5 - Форма "Заявление на отзыв регистрационных свидетельств (от юридического лица)"

Приложение 1 **Форма**

Заявление на выдачу регистрационных свидетельств (от физического лица)

Выпуск регистрационного свидетельства для электронной цифровой подписи

**Срок действия регистрационных свидетельств: 3 года.*

Идентификационные данные физического лица, на имя которого выдаются регистрационные свидетельства:

Фамилия: _____
Имя: _____
Отчество (при наличии): _____
Для резидентов РК
ИИН: _____
Для нерезидентов РК

Номер документа , удостоверяющего личность: _____
Дата выдачи документа :_____
Орган выдачи : _____
Страна выдачи : _____

Телефон: _____

С политикой применения соответствующих регистрационных свидетельств Удостоверяющего центра BTS Digital ознакомлен, возражений не имею. Настоящим даю согласие на хранение закрытого ключа ЭЦП в облачной ЭЦП УЦ.

Данные о средствах ЭЦП, используемых для создания соответствующего закрытого ключа ЭЦП, обозначение стандарта алгоритма ЭЦП и длины открытого ключа: СКЗИ Certex (ЭЦП - СТ РК ГОСТ 34.310-2004, 256 Бит).

Открытый ключ: :_____

Место для дополнительной информации: _____

С пользовательским соглашением на интернет-ресурсе Удостоверяющего центра BTS Digital ознакомлен и подтверждаю свое согласие на обработку моих персональных данных в целях выпуска электронной цифровой подписи.

Дата "___" _____ 20 __г.

Приложение 2 **Форма**

Заявление на отзыв регистрационных свидетельств (от физического лица)

Идентификационные данные физического лица, на имя которого выданы регистрационные свидетельства:

Фамилия: _____
Имя: _____
Отчество (при наличии): _____
Для резидентов РК
ИИН: _____
Для нерезидентов РК

Номер документа , удостоверяющего личность: _____
Дата выдачи документа (не обязательно к заполнению):_____
Орган выдачи (не обязательно к заполнению): _____
Страна выдачи (не обязательно к заполнению): _____

Телефон: _____

Идентификационные данные регистрационного свидетельства:

Серийный номер:_____

С пользовательским соглашением Удостоверяющего центра BTS Digital ознакомлен и подтверждаю свое согласие на обработку моих персональных данных в целях их передачи.

Дата обращения к услугодателю "___" _____ 20 __г.

Приложение 3 **Форма**

Регистрационное свидетельство в форме электронного документа

Регистрационное Свидетельство № _____

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 _____

Индивидуальный идентификационный номер: _____

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:

Средство ЭЦП: _____

Регистрационное свидетельство в формате: _____

ЭЦП издателя под настоящим регистрационным свидетельством: _____

"___" _____ 20__ г.

Приложение 4 **Форма**

Заявление на выдачу регистрационных свидетельств (от юридического лица)

Выпуск регистрационного свидетельства для электронной цифровой подписи

**Срок действия регистрационных свидетельств: 3 года.*

Идентификационные данные юридического лица:

Номер регистрационного свидетельства : _____

Наименование организации: _____

Для резидентов РК
Бизнес-идентификационный номер: _____
Для нерезидентов РК
Регистрационный номер плательщика НДС: _____
Страна регистрации: _____

Идентификационные данные представителя юридического лица, на имя которого выдаются регистрационные свидетельства:

Для резидентов РК
Индивидуальный идентификационный номер: _____

Для нерезидентов РК
Индивидуальный идентификационный номер (при наличии): _____
Номер документа, удостоверяющего личность:_____
Дата выдачи: _____

Фамилия: _____
Имя: _____
Отчество (при наличии): _____

С политикой применения соответствующих регистрационных свидетельств Удостоверяющего центра BTS Digital ознакомлен, возражений не имею. Настоящим даю согласие на хранение закрытого ключа ЭЦП в облачной ЭЦП УЦ.

Данные о средствах ЭЦП, используемых для создания соответствующего закрытого ключа ЭЦП, обозначение стандарта алгоритма ЭЦП и длины открытого ключа: СКЗИ Certex (ЭЦП - RSA 2048 Бит).

Открытый ключ подписи:_____

С пользовательским соглашением на интернет-ресурсе Удостоверяющего центра BTS Digital ознакомлен и подтверждаю свое согласие на обработку моих персональных данных в целях выпуска электронной цифровой подписи.

Дата "__" _____ 20__ г.

Приложение 5 **Форма**

Заявление на отзыв регистрационных свидетельств (от юридического лица)

Идентификационные данные юридического лица (представителя), на которого выданы регистрационные свидетельства:

Бизнес-идентификационный номер:_____
Для нерезидентов – регистрационный номер плательщика налог на добавленную стоимость с указанием страны регистрации:
_____
Наименование организации:_____
Идентификационные данные сотрудника юридического лица на имя которого выдается регистрационные свидетельства:
Индивидуальный идентификационный номер: _____
Для нерезидентов - номер документа, удостоверяющего личность, дата его выдачи, наименование выдавшего органа с указанием государства выдачи или уникальный номер: _____
Фамилия: _____
Имя: _____
Отчество: _____
Идентификационные данные регистрационного свидетельства:
Серийный номер: _____

С пользовательским соглашением Удостоверяющего центра BTS Digital ознакомлен и подтверждаю свое согласие на обработку моих персональных данных в целях их передачи.

Дата "__" _____ 20__ года.