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

BTS·Digital

ПОЛИТИКА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ЭЦП УДОСТОВЕРЯЮЩЕГО ЦЕНТРА «ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ ТОО «BTS Digital»

Астана, 2023

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Настоящий документ описывает общие правила применения регистрационных свидетельств Удостоверяющего Центра «Инфраструктура открытых ключей» ТОО «BTS Digital» (далее – УЦ), принадлежащего ТОО «BTS Digital», участниками информационных систем.

Настоящий документ является документом, определяющим порядок действий и обязательства вовлеченных сторон, возникающих в процессе предоставления и использования услуг УЦ.

Настоящий документ подготовлен в соответствии с рекомендациями RFC 3647.

Для конечных владельцев регистрационных свидетельств используется краткая инструкция пользователя.

1.1 Определения и сокращения

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 используемые владельцем ключи обеспечивают безопасность информации.

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.

Политика применения регистрационного свидетельства –внутренний документ, определяющий регламент и механизмы работы удостоверяющего центра в части управления регистрационными свидетельствами.

Регистрация участника УЦ – внесение регистрационной информации о владельце регистрационного свидетельства в хранилище УЦ.

Регистрационное свидетельство – документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным законодательством Республики Казахстан.

Список отозванных регистрационных свидетельств (СОС) – перечень всех регистрационных свидетельств подписчиков УЦ, отозванных на момент выпуска СОС.

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

Хранилище регистрационных свидетельств – справочник всех регистрационных свидетельств и СОС.

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

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

1.2 Обзор

Настоящий документ определяет виды регистрационных свидетельств, выпускаемых УЦ, процедуры их проверки и их применимость. Регистрационное свидетельство связывает значение открытого ключа Электронной Цифровой Подписи (далее - ЭЦП) с информацией, которая идентифицирует пользователя, использующего соответствующий закрытый ключ ЭЦП. Регистрационное свидетельство применяется пользователем регистрационного свидетельства или доверяющей стороной, которой необходимо задействовать открытый ключ из регистрационного свидетельства для проверки ЭЦП. Степень доверия к регистрационному свидетельству определяется следующими факторами:

- документом Регламент Удостоверяющего Центра «Инфраструктура открытых ключей ТОО «BTS Digital» (далее – Регламент), которому следует УЦ при аутентификации субъекта и выпуске регистрационного свидетельства;
- Выполнением требований законодательства УЦ.

1.3 Наименование и идентификация документа

Наименование документа: Политика применения регистрационных свидетельств ТОО «BTS Digital»

Версия документа: 1.0

Номер документа: 0021

Актуальная редакция настоящего документа доступна по ссылке https://passport.aitu.io/assets/resources/pdf/ca/certification-key-policy.pdf

1.4 Участники УЦ

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

1.5 Использование регистрационных свидетельств ключей

Допустимое использование регистрационного свидетельства

Регистрационные свидетельства могут использоваться для электронной цифровой подписи при создании электронных документов, а также для аутентификации владельцев регистрационных свидетельств, в соответствии со сведениями указанными в этих регистрационных свидетельствах.

1.6 Управление документом

1.6.1 Организация, ответственная за содержание документа

ТОО «BTS Digital»
Республика Казахстан, 010000
г. Астана, район Алматы, пр. Рақымжан Қошқарбаев, ¼

1.6.2 Контактное лицо

Байгаскин Жаслан,
Ведущий менеджер продуктов
Email: zhaslan.baygaskin@btsdigital.kz

1.6.3 Лица, утверждающие изменения

Изменения в документе утверждаются Генеральным директором ТОО «BTS Digital».

1.6.4 Процедура уведомления об изменении

Официальным уведомлением участников информационных систем об утверждении изменений политики является публикация по ссылке https://passport.aitu.io/assets/resources/pdf/ca/certification-key-policy.pdf.

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

2. ПУБЛИКАЦИЯ И ХРАНЕНИЕ СВЕДЕНИЙ

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1 Назначение имен

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

3.2 Процедура первичной регистрации

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

3.3 Идентификация и аутентификация заявителя при смене ключей

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

4.1 Заявление на выдачу регистрационного свидетельства

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.2 Обработка заявления на выдачу регистрационного свидетельства

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.3 Изготовление регистрационного свидетельства

Регистрационное свидетельство изготавливается Центром сертификации в соответствии со сведениями, указанными в заявлении. Формат регистрационного свидетельства основан на рекомендациях ITU-T X.509v3 и RFC 5280. Требования к полям расширения регистрационных свидетельств описаны в подразделе 7.1.

4.4 Признание регистрационного свидетельства

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.5 Использование ключей и регистрационных свидетельств

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.6 Обновление регистрационного свидетельства

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.7 Смена ключей подписи

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.8 Изменение сведений, указанных в регистрационном свидетельстве

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.9 Отзыв регистрационного свидетельства

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.10 Сервис проверки статуса регистрационного свидетельства в режиме on-line

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.11 Окончание пользования услугами УЦ

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

4.12 Депонирование и восстановление ключей

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для обеспечения безопасности УЦ применяются организационно-технические и

административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление 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.

Этот контроль периодически выполняется сотрудниками подразделения информационной безопасности (ИБ) на основе требований документации на средства защиты от несанкционированного доступа, а также оценки рисков ИБ.

5.1 Физические меры обеспечения безопасности

5.1.1 Размещение Центра сертификации

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.2 Организационные меры обеспечения безопасности

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.3 Требования к персоналу

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.4 Порядок ведения записей аудита

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.5 Ведение архива

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.6 Смена ключей Центра сертификации

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.7 Восстановление в случае компрометации или сбоев

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

5.8 Разрешение конфликтных ситуаций

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

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.

6. ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

6.1 Изготовление и установка ключевой пары

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

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

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

6.3 Другие особенности использования ключей

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

6.4 Данные активации закрытых ключей

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

6.5 Средства управления компьютерной безопасностью

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

6.6 Технические средства управления жизненным циклом

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

6.7 Средства управления сетевой безопасностью

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

6.8 Списание оборудования

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7. ШАБЛОНЫ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ, COC И OCSP

7.1 Описание регистрационного свидетельства

7.1.1 Версия регистрационного свидетельства

Центр Сертификации выдает регистрационные свидетельства в электронной форме в формате, основанном на рекомендациях ITU-T X.509v3 и RFC 5280.

7.1.2 Расширения регистрационного свидетельства

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7.1.3 Объектные идентификаторы алгоритмов

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7.1.4 Структура регистрационного свидетельства Центра сертификации (Алгоритм ГОСТ 34.310-)

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7.1.5 Структура регистрационного свидетельства пользователя УЦ

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7.1.6 Структура регистрационного свидетельства пользователя УЦ (Алгоритм ГОСТ 34.310)

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

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:

Common Name	**Фамилия, имя, или Псевдоним**
Organization	**Наименование места работы**
Country	**KZ**

Обязательными атрибутами поля идентификационных данных владельца регистрационного свидетельства являются:

Serial Number	**ИИН/номер паспорта**
Country	**ISO 3166-1 alpha-2**
Organization	**Значение поля – полное наименование организации**

7.1.8 Объектный идентификатор политики регистрационного свидетельства

Центр Сертификации выдает регистрационные свидетельства, соответствующие RFC 5280 (Регистрационное свидетельство X.509 версии 3). Выданные регистрационные свидетельства содержат поля, декларирующие, что для данного регистрационного свидетельства применялись одна или более политик регистрационного свидетельства. Политика регистрационного свидетельства, которую должны распознавать как выпускающий, так и пользователь регистрационного свидетельства, представлена в регистрационном свидетельстве уникальным зарегистрированным Object Identifier. Политика регистрационного свидетельства может применяться пользователем регистрационного свидетельства при решении вопроса о том, может ли доверять регистрационному свидетельству и содержащейся в нем информации для конкретной информационной системы. Доверяющая сторона заранее конфигурирует свое ПО так,

что оно «знает», какая политика ему требуется и, соответственно, не доверяет регистрационного свидетельствам, если требуемая политика отсутствует.

Зарегистрированный объектный идентификатор удостоверяющего центра “BTS Digital” - 1.2.398.3.17

7.1.8.1 Тестовые регистрационные свидетельства

Политика включается в регистрационные свидетельства, предназначенные для тестирования. Регистрационные свидетельства с этой политикой не обеспечивают юридической значимости электронных документов и могут использоваться доверяющей стороной исключительно в качестве тестовых регистрационных свидетельств в действующих информационных системах. Для получения тестовых регистрационных свидетельств заявителю не обязательно проходить процедуру аутентификации, см. пункты 3.2.2 – 3.3.4 Регламента.

7.1.8.2 Администратор Центра Сертификации

Политика включается в регистрационные свидетельства уполномоченного лица УЦ для получения привилегированных прав в системе.

7.1.9 Использование расширения Policy Constraints

Нет условий.

7.1.10 Использование расширения Policy Qualifier

Нет условий.

7.1.11 Порядок обработки расширений Certificate Policies, имеющих пометку critical

Решение о доверии к регистрационному свидетельству принимается пользователем самостоятельно.

7.2 Описание COC

7.2.1 Номер версии

Центр Сертификации формирует COC в электронной форме в формате, основанном на рекомендациях ITU-T X.509v3 и RFC 5280.

7.2.2 Расширения COC

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7.2.3 Структура списка отозванных регистрационных свидетельств (Алгоритм ГОСТ 34.310-2004)

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

7.3 Описание OCSP

7.3.1 Номер версии

УЦ формирует квитанции OCSP в электронной форме версии 1 в соответствии с RFC 2560.

7.3.2 Расширения OCSP

Не определены.

8. ПРОВЕРКА СООТВЕТСТВИЯ И ДРУГИЕ ОЦЕНКИ

8.1 Частота или основания проведения оценки

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

8.2 Темы, затрагиваемые при проведении оценки

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

8.3 Действия, предпринимаемые в результате несоответствия функционирования УЦ данному документу

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

8.4 Сообщение о результатах

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

9. ДРУГИЕ КОММЕРЧЕСКИЕ И ЮРИДИЧЕСКИЕ ВОПРОСЫ

9.1 Финансовая ответственность

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

9.2 Конфиденциальность коммерческой информации

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

9.3 Конфиденциальность личной информации

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

9.4 Права на интеллектуальную собственность

Настоящий документ описывает общие правила, определяющие применимость регистрационных свидетельств УЦ. ТОО «BTS Digital» оставляет за собой права интеллектуальной собственности на регистрационные свидетельства, которые выпускает УЦ и на информацию об их статусе. При этом не запрещается копирование и распространение регистрационных свидетельств на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования регистрационных свидетельств в соответствии с Регламентом. Также, не запрещается использование информации о статусе регистрационных свидетельств для выполнения функций доверяющей стороны в соответствии с Регламентом.

При составлении настоящего документа использовались следующие материалы:

- 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 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ГОСТ 34.310-2004 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

9.5 Обязанности

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

9.6 Отзыв гарантий

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

9.7 Ограничения ответственности

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).

9.8 Срок действия и прекращение действия

Настоящий Документ вступает в силу с момента его публикации по ссылке https://passport.aitu.io/assets/resources/pdf/ca/certification-key-policy.pdf и действует до публикации новой редакции Документа.

9.9 Индивидуальные уведомления и сообщения участникам

Не определены.

9.10 Поправки

Участникам УЦ не сообщат заранее о внесении поправок в настоящий Документ. Поправки утверждают прежде, чем новый документ будет опубликован по ссылке https://passport.aitu.io/assets/resources/pdf/ca/certification-key-policy.pdf. Обновленная версия настоящего документа публикуются по ссылке https://passport.aitu.io/assets/resources/pdf/ca/certification-key-policy.pdf.

9.11 Условия разрешения споров

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

9.12 Действующее законодательство

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

9.13 Соответствие действующему законодательству

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

9.14 Прочие положения

Подробно представлено в Регламенте (https://passport.aitu.io/assets/resources/pdf/ca/regulation.pdf).