Kaspi Bank» АҚ/АО «Kaspi Bank»
Нормативтік құжат / Нормативный документ
№ ___
күні/дата 28.11.23г.

Приложение № 3
К приказу «Об утверждении документов
Удостоверяющего центра АО «Kaspi Bank»»
«28» 11 2023 года № _____

Политика применения Регистрационных свидетельств Удостоверяющего центра АО «Kaspi Bank»

Политика применения Регистрационных свидетельств Удостоверяющего Центра АО «Kaspi Bank» (далее – Политика) описывает общие правила применения Регистрационных свидетельств, Участниками УЦ. Политика подготовлена в соответствии с рекомендациями RFC 3647.
Политика является неотъемлемой частью Регламента деятельности Удостоверяющего Центра АО «Kaspi Bank» (далее – Регламент) и определяет виды Регистрационных свидетельств, выпускаемых УЦ, процедуры их проверки и их применимость.

1. Использование Регистрационных свидетельств

1.1. Регистрационные свидетельства используются для ЭЦП при создании электронных документов, а также для аутентификации Владельцев Регистрационных свидетельств, в соответствии со сведениями, указанными в этих Регистрационных свидетельствах.
1.2. Сфера применения ЭЦП Владельца Регистрационного свидетельства определена в Регламенте.
1.3. Регистрационное свидетельство связывает значение Открытого ключа ЭЦП с информацией, которая идентифицирует пользователя, использующего соответствующий Закрытый ключ ЭЦП. Регистрационное свидетельство применяется Владельцем Регистрационных свидетельств или Доверяющей стороной, которой необходимо задействовать Открытый ключ ЭЦП из Регистрационного свидетельства для проверки ЭЦП. Степень доверия к Регистрационному свидетельству определяется следующими факторами:
1) Регламентом;
2) Политикой;
3) Законодательством Республики Казахстан.

2. Содержание Регистрационного свидетельства

2.1. УЦ выдает Регистрационные свидетельства, соответствующие рекомендациям ITU-T X.509 версии 3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Выданные Регистрационные свидетельства содержат в полях «Субъект» и «Издатель» сведения, представленные в соответствии с рекомендациями ITU-T X.501 (Distinguished Names (далее - DN)).
2.2. Указанные в Регистрационных свидетельствах личные данные физического лица или представителя юридического лица по доверенности, должны точно совпадать со сведениями, указанными в документах, удостоверяющих личность.
2.3. Для всех типов Регистрационных свидетельств, атрибут C (Country) содержит двухбуквенный код страны (ISO 3166-1 alpha-2).
2.4. Для Регистрационных свидетельств юридических лиц атрибут O (Organization) содержит название юридического лица. Для Регистрационных свидетельств физических лиц атрибут O может содержать название юридического лица – владельца информационной системы, для которой предназначено Регистрационное свидетельство.
2.5. Для Регистрационных свидетельств физических и юридических лиц, атрибут CN (Common Name) содержит фамилию, имя и отчество (при наличии) физического лица – Владельца Регистрационного свидетельства (строго в указанном порядке). Чтобы исключить неоднозначность между различными физическими лицами с одним и тем же именем, атрибут CN Регистрационного свидетельства может содержать другой дополнительный текст, кроме идентификационного имени физического лица. Дополнительный текст должен быть отформатирован так, чтобы его нельзя было перепутать с именем физического лица. Рекомендуется, чтобы текст следовал за именем физического лица после пробела в качестве разделителя и был заключен в круглые скобки. УЦ не проверяет содержимое атрибута CN, и поэтому доверяющим сторонам запрещается полагаться на содержание текста. Для Регистрационных

свидетельств сервера атрибут CN содержит полное доменное имя сервера. Для Регистрационных свидетельств служб атрибут CN содержит название службы.

2.6. 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).

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

2.8. Дополнительно, могут использоваться атрибуты OU (Organization Unit), L (Locality) и E (e-mail).

2.9. Отличительное имя DN должно быть уникальным для каждого Заявителя. Если имя DN, представленное Заявителем не уникально, то УЦ требует Заявителя повторно представить запрос с изменением атрибута CN, для обеспечения уникальности 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. Регистрационное свидетельство должно относиться к уникальному физическому/юридическому лицу или ресурсу, или службе. Регистрационное свидетельство должно использоваться только Владельцем Регистрационного свидетельства. УЦ гарантирует, что отличительное имя DN не будет использоваться повторно другим Заявителем. Если физическое или юридическое лицо запрашивает Регистрационное свидетельство с таким же именем DN, как в уже существующем Регистрационном свидетельстве (независимо от статуса этого Регистрационного свидетельства), и запрос не является запросом на изменение Регистрационного свидетельства, то уполномоченный работник УЦ может обратиться к персональной удостоверяющей информации, чтобы проверить, что физическое/юридическое лицо – тот же субъект, который был идентифицирован при получении первоначального Регистрационного свидетельства. Если идентичность не может быть установлена, имя DN не будет использоваться повторно. В случаях полного совпадения сведений, указываемых в нескольких Регистрационных свидетельствах, принадлежащих разным Владельцам Регистрационных свидетельств, в них вносятся специальный атрибут (например, серийный номер), позволяющий однозначно идентифицировать их владельцев.

2.10. Выданные Регистрационные свидетельства и COPC вносятся в Хранилище Регистрационных свидетельств и публикуются не позднее даты начала их действия. Срок действия COPC составляет 7 (семь) календарных дней, публикация COPC производится по мере появления отозванных (приостановленных) Регистрационных свидетельств.

2.11. Сведения о Статусе Регистрационных свидетельств публикуются в соответствии с Регламентом.

3. Изготовление Регистрационных свидетельств и установка ключевой пары

3.1. УЦ изготавливает Регистрационные свидетельства в соответствии со сведениями, указанными в Заявлении. Формат Регистрационных свидетельств основан на рекомендациях ITU-T X.509v3 и RFC 5280.

3.2. Ключи ЭЦП УЦ формируются с применением сертифицированного СКЗИ.

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

3.4. Параметры генерации и проверки качества Закрытого ключа ЭЦП определяются сертифицированным СКЗИ в соответствии с СТ РК 1073–2007 автоматически.

3.5. Закрытые ключи ЭЦП в облачной ЭЦП хранятся в течение срока действия Регистрационных свидетельств.

4. Расширения Регистрационных свидетельств

Регистрационные свидетельства могут содержать следующие дополнения:

authorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
subjectKeyIdentifier	Идентификатор ключа Владельца Регистрационного свидетельства
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), ▪ 1.2.398.3.14.9 - Хранилище ключей ◦ 1.2.398.3.14.9.1 – Файловое хранилище ◦ 1.2.398.3.14.9.2 - Облачное хранилище ▪ 1.2.398.3.14.10 - Пользователи ◦ 1.2.398.3.14.10.1 - Физическое лицо

	◦ 1.2.398.3.14.10.2 - Юридическое лицо • 1.2.398.3.14.10.2.1 - Первый руководитель юридического лица • 1.2.398.3.14.10.2.2 - Лицо, наделенное правом подписи
KeyUsage	Назначение ключа. Возможные значения: Подписание Регистрационных свидетельств, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL), Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей.
Basic constraints (optional)	Тип субъекта
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) Регистрационных свидетельств
certificatePolicies	1.2.398.3.14.2 - Политика Регистрационных свидетельств
Authority Information Access (optional)	Способ получения информации о статусе Регистрационных свидетельств

4.1. Объектные идентификаторы алгоритмов

ГОСТ 34.10-2004	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) sign(2)
ГОСТ 34.311-95	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) hash(1)
ГОСТ 34.310-2004	1.2.398.3.10.1.1.1.2 Подпись ГОСТ 34.310-2004
ГОСТ 34.311-95	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)
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

4.2. Структура Регистрационного свидетельства Корневого УЦ (Алгоритм ГОСТ 34.310-2004)

Название	Содержание
Версия	V3
Серийный номер	Уникальный серийный номер Регистрационного свидетельства
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004
Поставщик	CN = Kaspi.kz Root Certificate Authority O = АО «Kaspi Bank» C = KZ
Субъект	CN = Kaspi.kz Root Certificate Authority O = АО «Kaspi Bank» C = KZ
Срок действия	действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC
Открытый ключ	Значение открытого ключа в бинарном виде

4.3. Структура Регистрационного свидетельства Участника УЦ (Алгоритм ГОСТ 34.310-2004)

Название	Содержание
Версия	V3
Серийный номер	Уникальный серийный номер Регистрационного свидетельства
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004
Поставщик	CN = Kaspi.kz Root Certificate Authority O = АО «Kaspi Bank» C = KZ
Субъект	Физические лица: CN = Полное ФИО SERIALNUMBER = IIN123456789012 C = KZ Где IIN123456789012 – ИИН Физического лица, Юридические лица: CN = Полное ФИО работника

	SERIALNUMBER = IIN123456789012 O = Название организации OU = BIN123456789012 C = KZ Где IIN123456789012 – ИИН Физического лица, BIN123456789012 – БИН Юридического лица
Срок действия	действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC
Открытый ключ	Значение открытого ключа в бинарном виде

5. Описание СОРС

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

5.1. Расширения СОРС

УЦ может использовать следующие дополнения:

CRL number	Порядковый номер СОРС
Authority Key Identifier	Идентификатор ключа уполномоченного лица УЦ
Reason Code	Код причины отзыва Регистрационного свидетельства. Возможные значения (включая, но не ограничивая): 1 - Компрометация ключей 3 - Имя пользователя или другая информация в сертификате изменена 4 - Сертификат заменен другим 5 - Сертификат более не нужен для целей, которых он выдавался.

5.2. Структура СОРС (Алгоритм ГОСТ 34.310-2004)

Название	Содержание
Версия	V2
Издатель	CN = Kaspi.kz Root Certificate Authority O = АО «Kaspi Bank» C = KZ
Действителен с	действителен с: YYMMDDHHMMSSZ UTC
Следующее обновление	действителен по: YYMMDDHHMMSSZ UTC
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004
Номер CRL	Номер CRL
Идентификатор ключа центра сертификатов	Идентификатор ключа Поставщик сертификата: Адрес каталога: CN = Kaspi.kz Root Certificate Authority O = АО «Kaspi Bank» C = KZ Серийный номер сертификата
Отпечаток	Хэш сертификата
Отозванные Регистрационные свидетельства	Последовательность следующего вида: Серийный номер Дата отзыва Код причины списка отзыва (CRL)

6. Информация об УЦ

6.1. Политика вступает в силу с момента его публикации на сайте www.kaspibank.kz и действует до публикации новой редакции Политики.

6.2. Официальным уведомлением Участников УЦ об утверждении изменений Политики является публикация на интернет-сайте УЦ по адресу: www.kaspibank.kz/?ft=1&type=32

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

***