АКЦИОНЕРНОЕ ОБЩЕСТВО "FORTEBANK"

Утверждена
решением Совета директоров
АО "ForteBank"
(протокол заседания №33 (з)
от 15.10.2020 года)
Регистрационный номер
№01-010873-ВДБП/135
Введена в действие

с ____ _____ 2020 года

ПОЛИТИКА

ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

РАЗРАБОТЧИК:
Направление по разработке розничных продуктов и процессов

г. Нур-Султан
2020 г.

Настоящая Политика разработана в соответствии с законодательством Республики Казахстан и определяет регламент и механизмы работы удостоверяющего центра АО "ForteBank", в части управления процессом выдачи регистрационных свидетельств, общие правила применения, процедуры проверки, способы использования регистрационных свидетельств.

Статья 1. Общие положения

1. Настоящая Политика определяет порядок изготовления и применения регистрационных свидетельств при подписании электронных документов.

2. Действие настоящей Политики распространяется на всех работников Банка, применяющих ее в работе.

3. В настоящей Политике используются следующие понятия, условные обозначения и сокращения:

1) **владелец регистрационного свидетельства** – клиент Банка-физическое лицо, на имя которого удостоверяющим центром выдано регистрационное свидетельство, при наличии технической возможности;

2) **закрытый ключ ЭЦП** – последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

3) **заявитель** – клиент Банка-физическое лицо, подавший документы в удостоверяющий центр для выдачи или отзыва регистрационного свидетельства;

4) **заявление** – документ на выдачу или отзыв регистрационного свидетельства, по форме, установленной законодательством Республики Казахстан;

5) **корневой УЦ РК** - удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров;

6) **открытый ключ ЭЦП** – последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

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

8) **СОРС** – список отозванных регистрационных свидетельств, часть регистра регистрационных свидетельств, содержащий сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва;

9) **удостоверяющий центр (УЦ)** – АО "ForteBank", удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационных свидетельств;

9) **участник УЦ** – владельцы регистрационных свидетельств и АО "ForteBank", участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения электронных документов в рамках деятельности Банка;

10) **хранилище регистрационных свидетельств** – регистр всех регистрационных свидетельств, в том числе, СОРС, доступный участникам удостоверяющего центра, в порядке, установленном внутренними документами удостоверяющего центра;

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

Иные специфические термины и сокращения, используемые по тексту Политики, применяются в соответствии со значением, закрепленном в законодательстве Республики Казахстан, во внутренних документах удостоверяющего центра или принятым в международной банковской практике.

Статья 2. Цель и задачи.

1. Целью настоящей Политики является поддержание общих правил применения, процедур проверки, способов использования регистрационных свидетельств в соответствии с требованиями законодательства Республики Казахстан.

2. Задачами Политики является осуществление контроля:

1) за соблюдением требований законодательства и внутренних документов Банка при осуществлении деятельности УЦ;

2) за надлежащим применением ЭЦП при подписании электронных документов владельцами регистрационных свидетельств.

Статья 3. Принципы применения регистрационных свидетельств

1. Применение регистрационных свидетельств УЦ должно осуществляться в соответствии со следующими принципами:

1) принцип законности. Соблюдение законодательства Республики Казахстан при применении регистрационных свидетельств;

2) принцип целостности информации. Организация безопасного хранения и использования ЭЦП в соответствии с требованиями настоящей Политики.

Статья 4. Использование Регистрационных свидетельств

1. Регистрационные свидетельства используются Владельцами регистрационных свидетельств при подписании электронных документов, а также для аутентификации Владельцев регистрационных свидетельств, в соответствии со сведениями, указанными в этих Регистрационных свидетельствах.

2. Сферой применения ЭЦП Владельца регистрационного свидетельства являются отношения между ним и АО "ForteBank": для подписания Владельцем регистрационного свидетельства заявлений, согласий, договоров банковского обслуживания и иных документов в рамках правоотношений с АО "ForteBank", получения услуг АО "ForteBank" дистанционным способом, с учетом норм внутренних документов АО "ForteBank".

Иные способы использования ЭЦП не допускаются.

3. Регистрационное свидетельство связывает значение Открытого ключа ЭЦП с информацией, которая идентифицирует пользователя, использующего соответствующий Закрытый ключ ЭЦП. Регистрационное свидетельство применяется Владельцем регистрационного свидетельства, которому необходимо задействовать Открытый ключ ЭЦП из Регистрационного свидетельства для проверки ЭЦП. Степень доверия к Регистрационному свидетельству определяется требованиями:

1) Регламентом деятельности Удостоверяющего центра;

2) Политикой;

3) Законодательством Республики Казахстан.

Статья 5. Содержание Регистрационного свидетельства

1. Регистрационное свидетельство содержит следующие сведения:

1) номер регистрационного свидетельства и срок его действия;

2) данные, позволяющие идентифицировать владельца ЭЦП;

3) открытый ключ ЭЦП;

4) информацию о сферах применения и ограничениях применения ЭЦП;

5) реквизиты УЦ.

2. Удостоверяющий центр по согласованию с участником информационной системы может включать в Регистрационное свидетельство дополнительную информацию, необходимую для электронного документооборота.

3. 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).

4. Указанные в Регистрационном свидетельстве личные данные Владельца регистрационного свидетельства, должны точно совпадать со сведениями, указанными в документах, удостоверяющих его личность.

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

6. Для Регистрационных свидетельств физических лиц, атрибут CN (Common Name) содержит фамилию и имя 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 третьим лицам, использующим сведения о Регистрационном свидетельстве, полученные в УЦ, для проверки принадлежности ЭЦП Владельцу Регистрационного свидетельства запрещается полагаться на содержание текста. Для Регистрационных свидетельств сервера атрибут CN содержит ROOTCA. Для Регистрационных свидетельств служб атрибут CN содержит название службы.

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

8. Атрибут UID (Unique ID) может использоваться для различия имен (фамилии и имени физического лица), которые в ином случае были бы одинаковыми. Содержит идентификатор, присвоенный физическому лицу уполномоченными государственными органами.

9. Дополнительно, могут использоваться атрибуты OU (Organization Unit), L (Locality) и E (email).

10. DN должно быть уникальным для каждого Заявителя. Если DN, представленное Заявителем не уникально, то УЦ требует Заявителя повторно представить запрос с изменением атрибута CN, для обеспечения уникальности DN. Согласно настоящему документу два DN 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 DN. Регистрационное свидетельство должно относиться к уникальному физическому лицу. Регистрационное свидетельство должно использоваться только Владельцем регистрационного свидетельства. УЦ гарантирует, что DN не будет использоваться повторно другим физическим лицом. Если Заявитель запрашивает Регистрационное свидетельство с таким же 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 Заявитель является тем же субъектом, который был идентифицирован при получении первоначального Регистрационного свидетельства. Если идентичность не может быть установлена, DN не будет использоваться повторно. В случаях полного совпадения сведений, указываемых в нескольких Регистрационных свидетельствах, принадлежащих разным Владельцам регистрационных свидетельств, в них вносится специальный атрибут (например, SN), позволяющий однозначно идентифицировать их владельцев.

11. Выданные Регистрационные свидетельства и СОРС вносятся в Хранилище регистрационных свидетельств. УЦ обеспечивает публикацию СОРС на Forte.kz, с указанием серийного номера, даты и причины отзыва регистрационного свидетельства в СОРС.

12. Сведения о статусе Регистрационных свидетельств публикуются в соответствии с Регламентом деятельности Удостоверяющего центра.

(В подпункт 11 статьи 5 внесены изменения согласно решению Совета Директоров №37(з) от 29.10.2021г.)

Статья 6. Изготовление Регистрационных свидетельств и установка ключевой пары

1. УЦ изготавливает Регистрационные свидетельства в соответствии со сведениями, указанными в Заявлении.

2. Открытый и Закрытый ключи ЭЦП формируются с применением сертифицированного СКЗИ, в соответствии с алгоритмом ГОСТ 34.310-2004.

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

Статья 7. Расширения Регистрационных свидетельств

1. 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 ЭЦП будет иметь юридическое значение. Возможные значения: Server Authentication, Client Authentication, Secure e-mail, Time stamping, IPSec (Tunnel, User).
KeyUsage	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных.
Basic constraints (optional)	Тип субъекта
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) Регистрационных свидетельств
certificatePolicies	Политика Регистрационных свидетельств: Договоры банковского обслуживания, заявления, согласия и иные документы в рамках правоотношений с АО "ForteBank", в целях получения банковских услуг дистанционным способом
Authority Information Access (optional)	Способ получения информации о статусе Регистрационных свидетельств

Статья 8. Объектные идентификаторы алгоритмов

1. УЦ использует следующие идентификаторы алгоритмов средства ЭЦП:

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 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)}

(В пункт 1 статьи 8 внесены изменения согласно решению Совета Директоров №44 (з) от 08.12.2021г.)

Статья 9. Структура Регистрационного свидетельства корневого УЦ РК (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 = ROOTCA O = JSC ForteBank
	C = KZ

Субъект	CN = ROOTCA O = JSC ForteBank C = KZ
Срок действия	действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC
Открытый ключ	Значение открытого ключа в бинарном виде

Статья 10. 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 = ROOTCA O = JSC ForteBank C = KZ
Субъект	Физические лица: CN = Полное ФИО SERIALNUMBER = IIN123456789012 C = KZ Где IIN123456789012 – ИИН Физического лица
Срок действия	действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC
Открытый ключ	Значение открытого ключа в бинарном виде

Статья 11. Описание СОРС

1. 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).

Расширения СОРС

1. 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): Компрометация ключа пользователя; Компрометация ключа УЦ; Прекращение действия Регистрационного свидетельства.

Структура СОРС (Алгоритм ГОСТ 34.310-2004)

Название	Содержание
Версия	V2
Поставщик	CN = ROOTCA O = JSC ForteBank
	C = KZ
Дата выпуска	действителен с: YYMMDDHHMMSSZ UTC
Дата обновления	действителен по: YYMMDDHHMMSSZ UTC
Отозванные Регистрационные свидетельства	Последовательность следующего вида: □ CertificateSerialNumber (серийный номер Регистрационного свидетельства) Time (дата и время обработки заявления на отзыв)
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310-2004

Подпись	Цифровая подпись.

Статья 12. Заключительные положения

1. Структура настоящей Политики разработана в соответствии с внутренним документом Банка, регламентирующим порядок разработки, оформления и утверждения внутренних документов Банка.

2. Политика вступает в силу с момента ее публикации на сайте www.forte.kz и действует до публикации в новой редакции.

3. УЦ имеет право в одностороннем внесудебном порядке вносить изменения/дополнения в Политику, путем размещения изменений/дополнений (в том числе новой редакции) на сайте www.forte.kz.

4. Официальным уведомлением Участников УЦ об утверждении изменений/дополнений в Политику является ее публикация на сайте www.forte.kz.

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

6. За не соблюдение требований Политики Участники УЦ несут ответственность в соответствии с законодательством Республики Казахстан и внутренними документами УЦ.

7. Вопросы, порядок урегулирования которых не определен Политикой, подлежат разрешению в соответствии с требованиями законодательства Республики Казахстан и внутренних документов УЦ.