



ВНУТРЕННИЙ ДОКУМЕНТ	
Наименование:	Политика применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан»
Владелец:	Департамент информационной безопасности
Утвержден:	Решением Правления (Протокол №103 от 06.09.2024г.)
Срок введения в действие:	6.09.2024
Внесение последних изменений/дополнений	Изменения и дополнения в Политику применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан», утвержденные решением Правления №5 от 20.01.2026
Отмененные/признанные утратившими силу документы (при наличии):	
Степень конфиденциальности:	Общедоступный

ОГЛАВЛЕНИЕ

ГЛАВА 1. ОБЩЕЕ ПОЛОЖЕНИЯ	4
РАЗДЕЛ 1. НАИМЕНОВАНИЕ И ИДЕНТИФИКАЦИЯ ДОКУМЕНТА.....	4
РАЗДЕЛ 2. ПОНЯТИЯ И СОКРАЩЕНИЯ	4
РАЗДЕЛ 3. УЦ.....	6
РАЗДЕЛ 4. ИСПОЛЬЗОВАНИЕ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ	7
РАЗДЕЛ 5. УПРАВЛЕНИЕ ДОКУМЕНТОМ	7
РАЗДЕЛ 6. ПУБЛИКАЦИЯ ИНФОРМАЦИИ	7
РАЗДЕЛ 7. ПЕРИОД ПУБЛИКАЦИИ ИНФОРМАЦИИ	7
РАЗДЕЛ 8. КОНТРОЛЬ ДОСТУПА К ПУБЛИЧНОЙ ИНФОРМАЦИИ	8
ГЛАВА 2. ШАБЛОНЫ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ, СОРС	8
РАЗДЕЛ 1. ОПИСАНИЕ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ	8
РАЗДЕЛ 2. ОПИСАНИЕ СОРС	11
РАЗДЕЛ 3. ОПИСАНИЕ ОССР	12
ГЛАВА 3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	12

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. № A0-08-13/198/ПТ/06092024**

РЕЕСТР

утвержденных изменений и дополнений
в Политику применения регистрационных свидетельств
удостоверяющего центра АО «Фридом Банк Казахстан»

№	Номер документа	Реквизиты решения Органа Банка об утверждении изменений и дополнений	Срок введения в действие утвержденных изменений и дополнений	Основание внесения изменений/дополнений
1	№A0-08- 13/198/ПТ/0609 2024	Протокол №5 от 20.01.2026	21.01.2026г	Изменения и дополнения для устранения замечаний уполномоченного органа
2				
3				
4				
5				
6				

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. № АО-08-13/198/ПТ/06092024**

ГЛАВА 1. ОБЩЕЕ ПОЛОЖЕНИЕ

1. Настоящая Политика применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан» (далее – Политика) определяет регламент и механизмы работы удостоверяющего центра АО «Фридом Банк Казахстан» в части управления регистрационными свидетельствами.

2. Требования Политики обязательны к исполнению для всех владельцев регистрационных свидетельств и работников УЦ.

3. Политика разработана в соответствии с законодательством Республики Казахстан в сфере ЭЦП и рекомендациями RFC 3647, а также внутренними и публичными документами УЦ.

4. Политика определяет виды регистрационных свидетельств, выпускаемых УЦ, процедуры их проверки, а также условия их применения.

5. Регистрационное свидетельство связывает значение открытого ключа ЭЦП с информацией, которая идентифицирует пользователя, использующего соответствующий закрытый ключ ЭЦП.

6. Регистрационное свидетельство применяется его пользователем или доверяющей стороной, которой необходимо задействовать открытый ключ ЭЦП из регистрационного свидетельства, для проверки ЭЦП.

7. Степень доверия к регистрационному свидетельству определяется следующими факторами:

- 1) Регламентом деятельности УЦ;
- 2) законодательством Республики Казахстан в сфере ЭЦП.

РАЗДЕЛ 1. НАИМЕНОВАНИЕ И ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

8. Наименование документа: Политика применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан».

Объектный идентификатор: 1.2.398.3.26.2 – Политика применения регистрационных свидетельств удостоверяющего центра АО «Фридом Банк Казахстан».

Актуальная редакция настоящего документа доступна по ссылке: <https://pki.bankffin.kz/policy/policy.pdf>.

РАЗДЕЛ 2. ПОНЯТИЯ И СОКРАЩЕНИЯ

9. Основные понятия и сокращения, используемые в настоящей Политике:

1) Аппаратный криптографический модуль (Hardware Security Module) (далее - HSM) - программно-аппаратный модуль, предназначенный для генерации, хранения, защиты и управления ключами УЦ, закрытыми ключами ЭЦП пользователей;

2) Банк – АО «Фридом Банк Казахстан»;

3) Владелец (пользователь) регистрационного свидетельства – физическое лицо или уполномоченный представитель юридического лица, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

4) Департамент информационной безопасности (далее – ДИБ) – структурное подразделение Банка, обеспечивающее контроль за состоянием защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

5) Документ из серии пронумерованных информационных документов Интернета, охватывающих технические спецификации и Стандарты, широко используемые сети Интернет (Request for Comments) (далее – RFC) 3647 – рекомендуемый стандарт из серии международных стандартов IETF, регулирующий требования к Инфраструктуре открытых ключей Internet X.509;

6) Документ из серии пронумерованных информационных документов Интернета, охватывающих технические спецификации и Стандарты, широко используемые сети

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. № А0-08-13/198/ПТ/06092024**

Интернет (Request for Comments) (далее – RFC) 2560 – рекомендуемый стандарт из серии международных стандартов IETF, регулирующий требования к протоколу для определения статуса регистрационного свидетельства;

7) Документ из серии пронумерованных информационных документов Интернета, охватывающих технические спецификации и Стандарты, широко используемые сети Интернет (Request for Comments) (далее – RFC) 5280 – рекомендуемый стандарт из серии международных стандартов IETF (Internet Engineering Task Force, открытое международное сообщество проектировщиков, ученых, сетевых операторов и провайдеров), регулирующий требования к структуре регистрационных свидетельств и СОРС;

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

9) Заявитель – физическое лицо или юридическое лицо, подавшее документы на выдачу или отзыв регистрационного свидетельства;

10) ИИН – индивидуальный идентификационный номер;

11) БИН – бизнес-идентификационный номер;

12) Интернет-ресурс УЦ – bankffin.kz;

13) Неотрекаемость – невозможность отказа отправителя (автора) Электронного документа от факта отправки (подписи) соответствующего документа или сообщения. Неотрекаемость предполагает, что Электронный документ является достоверным, он направлен и подтвержден Владелец регистрационного свидетельства (установлено авторство), содержание Электронного документа не имеет несанкционированных изменений после его подтверждения отправителем, автор Электронного документа, подтвердивший Электронный документ, согласен с содержанием подтвержденного им Электронного документа;

14) Носитель ключевой информации – 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»;

15) 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;

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

17) Работник УЦ – работник Департамента информационной безопасности, отвечающий за администрирование ПО УЦ, HSM УЦ, платформы, обеспечивающей функционирование ПО УЦ;

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

19) Сервер метки времени – служба для постановки метки времени на электронный документ. Служба работает на основе протокола меток времени – Time-Stamp Protocol (TSP);

20) Список отозванных регистрационных свидетельств (далее – СОРС) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования);

21) Средства криптографической защиты информации (далее – СКЗИ) – совокупность программно-технических средств, реализующих алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами и обеспечивающих применение электронной цифровой подписи и шифрование в

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. №А0-08-13/198/ПТ/06092024**

информационных системах. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение;

22) Удостоверяющий центр (далее – УЦ) – АО «Фридом Банк Казахстан», удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, подтверждающее достоверность регистрационного свидетельства;

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

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

25) 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;

26) хэш – преобразование массива входных данных произвольной длины в битовую сторону фиксированной длины;

27) блокчейн - Информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования.

РАЗДЕЛ 3. УЦ

10. УЦ

УЦ выполняет следующие функции:

- 1) получение и обработка запросов на выдачу и отзыв регистрационного свидетельства;
- 2) выдача, хранение, отзыв регистрационного свидетельства;
- 3) удостоверение соответствия Открытого ключа ЭЦП Закрытому ключу ЭЦП;
- 4) подтверждение достоверности регистрационных свидетельств;
- 5) выпуск, публикация и поддержка СОРС;
- 6) обработка запросов на сервис OCSP и его поддержка;
- 7) постановка штампа метки времени TSP;
- 8) генерация Открытых ключей ЭЦП и Закрытых ключей ЭЦП;
- 9) ведение реестра регистрационных свидетельств.

11. Хранилище и доступность публичной информации

УЦ обеспечивает публичную доступность 24 часа в сутки, 7 дней в неделю следующих материалов на Интернет-ресурсе УЦ:

- 1) Корневое регистрационное свидетельство УЦ по алгоритму ГОСТ;
- 2) Корневое регистрационное свидетельство Корневого удостоверяющего центра РК по алгоритму ГОСТ;
- 3) Регламент деятельности УЦ;
- 4) Политика применения регистрационных свидетельств УЦ;
- 5) СОРС;
- 6) Службы OCSP;
- 7) Служба TSP.

12. Доверяющая сторона

Доверяющая сторона – информационные системы, в которых будут применяться регистрационные свидетельства:

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. №А0-08-13/198/ПТ/06092024**

- 1) Интернет-банкинг для физических и/или юридических лиц (в том числе мобильные приложения, посредством которых клиенты пользуются банковскими услугами) Банка;
- 2) Система Certex Cloud (Облачная ЭЦП).

РАЗДЕЛ 4. ИСПОЛЬЗОВАНИЕ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ

13. Допустимое использование регистрационного свидетельства

Регистрационное свидетельство используется для подписания в ИС, утвержденных УЦ, электронных документов ЭЦП, для идентификации и/или аутентификации клиентов Банка в информационных системах, утвержденных УЦ, а также для проверки подлинности ЭЦП.

14. Ограничения использования регистрационных свидетельств

Регистрационные свидетельства не могут использоваться в иных случаях, не описанных в пункте 13 настоящего раздела Политики, а также по окончании их срока действия, в случае их отзыва или недействительности.

Тестовые регистрационные свидетельства должны использоваться только для подписания ЭЦП электронных документов, не имеющих юридической значимости.

РАЗДЕЛ 5. УПРАВЛЕНИЕ ДОКУМЕНТОМ

15. Организация, ответственная за содержание документа

АО «Фридом Банк Казахстан».

16. Контактная информация

АО «Фридом Банк Казахстан», Республика Казахстан, 050000, г. Алматы, Алмалинский район, ул. Курмангазы, дом 61А, телефон: 595, +7 776 159 55 95.

17. Орган, утверждающий изменения

Изменения в документе утверждаются Правлением АО «Фридом Банк Казахстан».

18. Процедура утверждения изменений

Официальным уведомлением владельцев регистрационных свидетельств об утверждении Политики в новой редакции или о внесении в нее изменений и дополнений является публикация Политики в новой редакции на Интернет-ресурсе УЦ по адресу: <https://pki.bankffin.kz/policy/policy.pdf>.

Все изменения, вносимые в Политику, вступают в силу и становятся обязательными к исполнению владельцами регистрационных свидетельств немедленно после их публикации.

Публикация Политики УЦ осуществляется в течении 3 (три) рабочих дней после ее утверждения.

РАЗДЕЛ 6. ПУБЛИКАЦИЯ ИНФОРМАЦИИ

19. СОРС УЦ предоставляется в электронной форме и формате, определенном рекомендациями RFC 5280 и настоящей Политикой. УЦ публикует СОРС для регистрационных свидетельств на алгоритме ГОСТ.

20. УЦ также предоставляет участникам ИС службу анонимной проверки статуса регистрационных свидетельств посредством службы OCSP.

21. УЦ предоставляет службу анонимной проверки поставки «Штампа времени» участникам ИС посредством службы TSP.

21-1. Протоколы событий ежедневно преобразуется в хэш, и данные хэш хранятся в цепочке событий блокчейн. Применяемая для этого блокчейн доступна в Интернет. <https://my.bankffin.kz/digital-signature/blockchain/?limit=100&offset=0>.

РАЗДЕЛ 7. ПЕРИОД ПУБЛИКАЦИИ ИНФОРМАЦИИ

22. Период публикации СОРС составляет 1 раз в сутки.

РАЗДЕЛ 8. КОНТРОЛЬ ДОСТУПА К ПУБЛИЧНОЙ ИНФОРМАЦИИ

23. В УЦ реализованы меры информационной и физической безопасности с целью предотвращения несанкционированного внесения изменений или удаления информации, содержащейся в СОРС и УЦ.

ГЛАВА 2. ШАБЛОНЫ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ, СОРС

РАЗДЕЛ 1. ОПИСАНИЕ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ

24. Версия регистрационного свидетельства

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

25. 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: Client Authentication, Secure e-mail, Time stamping, IPSec (Tunnel, User)
KeyUsage	Назначение ключа. Возможные значения: Подписание регистрационного свидетельства, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL), Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных
Basic constraints	Тип субъекта
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) регистрационных свидетельств
certificatePolicies	Политика регистрационных свидетельств
Authority Information Access (optional)	Способ получения информации о статусе регистрационного свидетельства

26. Объектные идентификаторы алгоритмов

УЦ использует следующие идентификаторы алгоритмов средства ЭЦП:

ГОСТ 34.310-2004	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)

27. Структура регистрационное свидетельства Корневого УЦ (Алгоритм ГОСТ

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. № A0-08-13/198/ПТ/06092024**

34.310-2004)

Название	Содержание
Версия	V3
Серийный номер	Уникальный серийный номер регистрационного свидетельства
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Поставщик	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Субъект	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Срок действия	действителен с: DDMMYYYYHHMMSSZ GMT действителен по: DDMMYYYYHHMMSSZ GMT
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде
Расширения регистрационного свидетельства	Дополнения регистрационного свидетельства
Подпись	ЭЦП

28. Структура регистрационного свидетельства владельца регистрационного свидетельства, использующего Облачное ЭЦП (Алгоритм ГОСТ 34.310-2004) для физических лиц

Название	Содержание
Версия	V3
Серийный номер	Уникальный серийный номер регистрационного свидетельства
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Поставщик	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Субъект	CN = Ф.И.О. (Фамилия Имя Отчество) SERIALNUMBER = ИИН (Индивидуальный Идентификационный Номер); OU = БИН (Бизнес-идентификационный Номер) – для юридического лица; O = Freedom Bank Kazakhstan JSC; C = KZ
Срок действия	действителен с DDMMYYYYHHMMSSZ GMT действителен по DDMMYYYYHHMMSSZ GMT
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде
Расширения регистрационного свидетельства	Дополнения регистрационного свидетельства
Подпись	ЭЦП

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. № A0-08-13/198/ПТ/06092024**

28-1. Структура регистрационного свидетельства владельца регистрационное свидетельства, использующего Облачное ЭЦП (Алгоритм ГОСТ 34.310-2004) для юридических лиц

Название	Содержание
Версия	V3
Серийный номер	Уникальный серийный номер регистрационного свидетельства
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Издатель	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Субъект	CN = Ф.И.О. (Фамилия Имя Отчество) SERIALNUMBER = IIN (Индивидуальный Идентификационный Номер); OU = BIN (Бизнес-идентификационный Номер) – для юридического лица; O = Freedom Bank Kazakhstan JSC; C = KZ
Срок действия	действителен с DDMMYYYYHHMMSSZ GMT действителен по DDMMYYYYHHMMSSZ GMT
Алгоритм открытого ключа	Объектный идентификатор алгоритма
Открытый ключ	Значение открытого ключа в бинарном виде
Расширения регистрационного свидетельства	Дополнения регистрационного свидетельства
Подпись	ЭЦП

29. 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 работника УЦ являются:

Common Name	Ф.И.О (Фамилия Имя Отчество)
SERIALNUMBER	ИИН (Индивидуальный Идентификационный Номер)
OU	БИН (Бизнес-идентификационный Номер)
Organization Unit	Название структурного подразделения Банка
Organization	Freedom Bank Kazakhstan (наименование места работы)
Country	KZ

Обязательными атрибутами поля идентификационных данных клиента Банка:

Common Name	Ф.И.О (Фамилия Имя Отчество)
SERIALNUMBER	ИИН (Индивидуальный Идентификационный Номер)
OU	БИН (Бизнес-идентификационный Номер)
Organization	Freedom Bank Kazakhstan JSC
Country	KZ

Обязательными атрибутами поля идентификационных данных владельца регистрационного свидетельства, являющегося пользователем Облачной ЭЦП являются:

**Политика применения регистрационных свидетельств удостоверяющего центра
АО «Фридом Банк Казахстан», рег. №А0-08-13/198/ПТ/06092024**

Common Name	Ф.И.О (Фамилия Имя Отчество)
SERIALNUMBER	ИИН (Индивидуальный Идентификационный Номер)
OU	БИН (Бизнес-идентификационный Номер)
Organization	Freedom Bank Kazakhstan JSC;
Country	KZ

30. Объектный идентификатор политики регистрационных свидетельств

УЦ выдает регистрационные свидетельства, соответствующие RFC 5280 (Регистрационное свидетельство X.509 версии 3). Выданные регистрационные свидетельства содержат поля, декларирующие, что для данного регистрационного свидетельства применялась одна или более политик регистрационных свидетельств. Политика регистрационного свидетельства, которую должны распознавать как выпускающий, так и владелец регистрационного свидетельства, представлена в регистрационном свидетельстве уникальным и зарегистрированным Object Identifier. Политика регистрационного свидетельства может применяться заинтересованным лицом 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 регистрационным свидетельствам, если требуемая политика отсутствует.

Для тестовых регистрационных свидетельств включается стандартная политика, указанная в настоящем документе. Тестовые регистрационные свидетельства, предназначенные для тестирования, выпускаются на тестовом оборудовании (HSM) УЦ, не обеспечивают юридической значимости электронных документов и могут использоваться доверяющей стороной исключительно в качестве тестовых регистрационных свидетельств в тестовых информационных/финансовых системах. Для получения тестовых регистрационных свидетельств заявителю необязательно проходить процедуру аутентификации.

РАЗДЕЛ 2. ОПИСАНИЕ СОРС

31. Номер версии

СОРС предоставляется в электронной форме и в формате определенном RFC 5280. СОРС заверяется корневым регистрационным свидетельством УЦ. Доступ к СОРС обеспечивается по протоколам LDAP и HTTP.

**32. Структура списка отозванных регистрационных свидетельств (СОРС)
(Алгоритм ГОСТ 34.310-2004)**

Название	Содержание
Версия	V2
Поставщик	CN = Freedom Root Certificate Authority; O = Freedom Bank Kazakhstan JSC; C = KZ
Дата выпуска	действителен с: DDMMYYYYHHMMSSZ GMT
Дата обновления	действителен по: DDMMYYYYHHMMSSZ GMT
Расширения СОРС	Дополнения СОРС
Отозванные регистрационные свидетельства	Последовательность следующего вида: <ul style="list-style-type: none">• CertificateSerialNumber (серийный номер регистрационного свидетельства)• Time (дата и время обработки заявления на отзыв регистрационного свидетельства)
Алгоритм подписи	Алгоритм подписи ГОСТ 34.310
Подпись	ЭЦП

РАЗДЕЛ 3. ОПИСАНИЕ OCSP

33. Протокол OCSP необходим доверяющим сторонам для определения статуса регистрационного свидетельства в текущем моменте времени – отозван или нет. OCSP может использоваться для обеспечения требований, касающихся получения более своевременной информации об отзыве регистрационных свидетельств, чем это возможно с использованием COPS.

34. Номер версии

Для проверки статуса регистрационного свидетельства УЦ использует версию 1 OCSP согласно рекомендациям RFC 2560 Online Certificate Status Protocol – OCSP.

35. Расширения OCSP

Расширения, обрабатываемые сервисом OCSP, а также их критичность соответствует рекомендациям RFC 2560 Online Certificate Status Protocol – OCSP.

ГЛАВА 3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

36. Внесение изменений и дополнений в Политику осуществляется в соответствии с требованиями внутренних нормативных документов УЦ.

37. Политика вступает в силу с момента ее публикации на Интернет-ресурсе и действует до публикации новой редакции Политики.

38. Ответственность за внесение изменений в Политику несет ДИБ.

39. Директор ДИБ несет ответственность за контроль соблюдения требований настоящей Политики.

40. Пересмотр настоящей Политики может быть как плановый, так и внеплановый – обусловленный изменениями в действующем законодательстве или в технологии работы подразделений Банка, предложениями и замечаниями аудиторов, рекомендациями внешних экспертов. Обязательный пересмотр настоящей Политики с целью анализа и актуализации изложенной в ней информации должен осуществляться не реже одного раза в два года.

41. Настоящая Политика обязательна для исполнения и ознакомления всеми работниками Банка и владельцам регистрационных свидетельств.