УТВЕРЖДЕНЫ
Решением Совета директоров
ДБ АО «Банк Хоум Кредит»
Протокол № 36/2020
от «26» октября 2020г.

Политика
применения регистрационных свидетельств
Удостоверяющего центра
ДБ АО «Банк Хоум Кредит»

Politics application of registration certificates
Certification Authority SB JSC "Bank Home Credit"

DIN PP00204

Алматы 2020 год

Справочная информация

Название:	**Политика применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит»**
Версия:	**4.00**
Подразделение – ответственный разработчик:	Департамент продаж
Уровень доступа:	**Общий**

Отв. разработчик:	**Должность**	**Ф.И.О.**	**Подпись**	**Дата**	**Конт. тел.**
	Менеджер по оптимизации процессов продаж	Реброва И.			2360

Хронология изменений и дополнений в документ

Ф.И.О. исполнителя	**Версия**	**Описание**	**Дата**
Реброва И.	1	Политика применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит»	17.04.2020г.
Реброва И.	2	Политика применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит»	13.07.2020г.
Реброва И.	3	Политика применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит»	17.09.2020г.

ОГЛАВЛЕНИЕ

1. Основные понятия

1. В настоящей Политике применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит» используются следующие термины и сокращения:

1) **Банк** – ДБ АО «Банк Хоум Кредит»;

2) **Владелец Регистрационного свидетельства** – физическое лицо, на имя которого выдано Регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в Регистрационном свидетельстве;

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

4) **Заявитель** – физическое лицо, обратившееся в Удостоверяющий центр для выпуска Регистрационного свидетельства;

5) **Заявление** – документ на выпуск Регистрационного свидетельства;

6) **Закон** – Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи»;

7) **Личный кабинет** – интерфейс в мобильном приложении, предназначенный для предоставления Клиенту электронных банковских услуг и иных целей, предусмотренных Договором банковского обслуживания, в рамках мобильного банкинга;

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

9) **Политика** – настоящая Политика применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит»;

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

11) **СКЗИ** – средства криптографической защиты информации, 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;

12) **СОРС** – Список отозванных Регистрационных свидетельств, перечень всех Регистрационных свидетельств, содержащих сведения о Регистрационном свидетельстве, действие которых прекращено, их серийные номера, дату и причину отзыва;

13) **Статус Регистрационного свидетельства** – результат проверки действительности Регистрационного свидетельства;

14) **Удостоверяющий центр (УЦ)** – Банк или иное юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность Регистрационного свидетельства;

15) **Участник УЦ** – Владельцы Регистрационных свидетельств, государственные органы, партнеры Банка участвующие в процессах сбора, обработки, хранения электронных документов в рамках детальности Банка;

16) **Хранилище Регистрационных свидетельств** – справочник всех Регистрационных свидетельств и СОРС;

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

18) **Home Credit Bank Kazakhstan/ Home Credit Agent (HCA)** - мобильное приложение/ приложение Банка, доступное для скачивания в Google Play и AppStore для платформ Android и iOS соответственно.

2. Общие положения

2. Настоящая Политика определяет общие правила применения Регистрационных свидетельств и является неотъемлемой частью Регламента деятельности Удостоверяющего центра ДБ АО «Банк Хоум Кредит».

3. Настоящая Политика разработана в соответствии с Законом и 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.

3. Использование Регистрационных свидетельств

4. 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.

5. ЭЦП используется для подписания Договоров, Заявлений и прочих документов в ДБ АО «Банк Хоум Кредит» (подписания документов между физическим лицом и ДБ АО «Банк Хоум Кредит»).

6. Регистрационное свидетельство связывает значение Открытого ключа ЭЦП с информацией, которая идентифицирует пользователя, использующего соответствующий Закрытый ключ ЭЦП.

7. УЦ предоставляет пользователю Закрытого ключа ЭЦП, хранимого в защищенной системе Банка, доступ к информации о всех подписанных электронных документах через личный кабинет/НСА Банка. Срок хранения информации обо всех подписанных электронных документах составляет не менее пятнадцати лет после истечения срока действия Регистрационного свидетельства пользователя.

4. Содержание Регистрационного свидетельства

8. 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.

9. Указанные в Регистрационных свидетельствах личные данные физического лица, должны точно совпадать со сведениями, указанными в документах, удостоверяющих личность.

10. УЦ выпускает Регистрационные свидетельства, соответствующие рекомендациям ITU-T X.509 версии 3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Выпущенные Регистрационные свидетельства содержат в полях «Субъект» и «Издатель» сведения, представленные в соответствии с рекомендациями ITU-T X.501 (Distinguished Names (далее - DN)).

11. Для Регистрационных свидетельств атрибут C (Country) содержит двухбуквенный код страны (ISO 3166-1 alpha-2).

12. Для Регистрационных свидетельств атрибут O может содержать название юридического лица – владельца информационной системы, для которой предназначено Регистрационное свидетельство.

13. Для Регистрационных свидетельств атрибут CN (Common Name) содержит фамилию и имя 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.

14. Атрибут Serial Number 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).

15. Дополнительно, могут использоваться атрибут E (email).

16. 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 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 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 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.

17. Выпущенные 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.

18. Сведения о Статусе Регистрационных свидетельств публикуются в соответствии с Регламентом деятельности УЦ.

5. Изготовление Регистрационных свидетельств и установка ключевой пары

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

20. Ключи ЭЦП УЦ, формируются с применением сертифицированного СКЗИ.

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

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

6. Расширения Регистрационных свидетельств

23. 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).
KeyUsage	Назначение ключа. Возможные значения: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных.
Basic constraints (optional)	Тип субъекта
cRLDistributionPoint	Точка распространения списка аннулированных (отозванных) Регистрационных свидетельств
certificatePolicies	Политика Регистрационных свидетельств
Authority Information Access (optional)	Способ получения информации о статусе Регистрационных свидетельств

6.1. Объектные идентификаторы алгоритмов

24. 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)}

6.2. 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 = homecredit.kz Root Certificate Authority O = Subsidiary Bank Joint-Stock Company Home Credit Bank C=KZ
Субъект	CN = homecredit.kz Root Certificate Authority O = Subsidiary Bank Joint-Stock Company Home Credit Bank C=KZ
Срок действия	действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC
Открытый ключ	Значение открытого ключа в бинарном виде
Подпись	ЭЦП

6.3. 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 = homecredit.kz Root Certificate Authority

	O = Subsidiary Bank Joint-Stock Company Home Credit Bank 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
Подпись	Цифровая подпись.

7. Описание СОРС

25. 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).

7.1. Расширение СОРС

26. 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.

7.2. Структура СОРС (Алгоритм ГОСТ 34.310-2004)

Название	Содержание
Версия	V2
Поставщик	CN = homecredit.kz Root Certificate Authority O = Subsidiary Bank Joint-Stock Company Home Credit Bank 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.

8. Заключительные положения

27. Политика вступает в силу с даты ее утверждения уполномоченным органом Банка и публикации на сайте ДБ АО «Банк Хоум Кредит» (https://homecredit.kz/) и действует до публикации новой редакции Политики.

28. Политика прекращает действие в случае замены на новую редакцию Политики.

29. Официальным уведомлением Участников УЦ об утверждении изменений Политики является публикация на интернет-сайте УЦ по адресу: (https://homecredit.kz/).

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

31. С даты вступления в силу настоящей Политики, считать утратившим силу Политику применения регистрационных свидетельств Удостоверяющего центра ДБ АО «Банк Хоум Кредит» (утвержденного решением Совета директоров ДБ АО «Банк Хоум Кредит», протокол № 31/2020 от 17.09.2020 г.).