2020 жылғы 26 қазандағы
«Банк Хоум Кредит» АҚ ЕБ
Директорлар кеңесі
шешімінің
№ 36/2020 хаттамасымен
БЕКІТІЛГЕН

«Банк Хоум Кредит» АҚ ЕБ
Куәландыру орталығының тіркеу куәліктерін қолдану саясаты

DIN PP00204

Алматы 2020 жыл

Анықтамалық ақпарат

Атауы:	**«Банк Хоум Кредит» АҚ ЕБ Куәландыру орталығының тіркеу куәліктерін қолдану саясаты**
Нұсқасы:	**4.00**
Жауапты құрылымдық бөлімше:	Сату департаменті
Қолжетімділік деңгейі:	**Жалпы**

Жауапты әзірлеуші:	**Лауазымы**	**Аты-жөні**	**Қолы**	**Күні**	**Ішкі нөмірі**
	Сату процестерін оңтайландыру менеджері	Реброва И.			2360

Құжатқа енгізілген өзгерістер мен толықтырулардың хронологиясы

Орындаушының аты-жөні	**Нұсқасы**	**Сипаттамасы**	**Күні**
Реброва И.	1	«Банк Хоум Кредит» АҚ ЕБ Куәландыру орталығының тіркеу куәліктерін қолдану саясаты	17.04.2020 ж.
Реброва И.	2	«Банк Хоум Кредит» АҚ ЕБ Куәландыру орталығының тіркеу куәліктерін қолдану саясаты	13.07.2020 ж.
Реброва И.	3	«Банк Хоум Кредит» АҚ ЕБ Куәландыру орталығының тіркеу куәліктерін қолдану саясаты	17.09.2020 ж.

МАЗМҰНЫ

1. Негізгі ұғымдар

1. Осы «Банк Хоум Кредит» АҚ ЕБ Куәландырушы орталығының тіркеу куәліктерін қолдану саясатында төмендегі терминдер мен қысқартулар пайдаланылады:

1) **Банк** – «Банк Хоум Кредит» АҚ ЕБ;

2) **Тіркеу куәлігінің иесі** - оның атына тіркеу куәлігі берілген, тіркеу куәлігінде көрсетілген ашық кілтке сәйкес келетін жабық кілтті заңды түрде иеленетін жеке тұлға;

3) **Электрондық сандық қолтаңбаның жабық кілті** - электрондық сандық қолтаңба құралдарын пайдалана отырып, электрондық сандық қолтаңбаны жасауға арналған электрондық сандық нышандар дәйектілігі;

4) **Өтініш беруші** - Тіркеу куәлігін шығару үшін Куәландырушы орталығына жүгінген жеке тұлға;

5) **Өтініш** - Тіркеу куәлігін шығаруға өтініш;

6) **Заң** - Қазақстан Республикасының 2003 жылғы 7 қаңтардағы «Электрондық құжат және электрондық сандық қолтаңба туралы» заңы, № 370-II;

7) **Жеке кабинет** - Клиентке электрондық банк қызметтерін ұсынуға және мобильді банкинг шеңберінде банктік қызмет көрсету шартында көзделген өзге де мақсаттарға арналған мобильді қосымшадағы интерфейс;

8) **Электрондық сандық қолтаңбаның ашық кілті** – кез келген тұлғаға қолжетімді және электрондық құжаттағы электрондық сандық қолтаңбаның төлнұсқалығын растауға арналған электрондық сандық нышандар дәйектілігі;

9) **Саясат** - осы «Банк Хоум Кредит» АҚ ЕБ Куәландырушы орталығының тіркеу куәліктерін қолдану саясаты;

10) **Тіркеу куәлігі** - электрондық сандық қолтаңбаның Қазақстан Республикасының заңнамасында белгіленген талаптарға сәйкестігін растау үшін Куәландырушы орталық беретін электрондық құжат;

11) **АКҚҚ** - ақпаратты криптографиялық қорғау құралдары, криптографиялық түрлендіру алгоритмдерін, кілттерді генерациялауды, қалыптастыруды, бөлуді немесе басқаруды жүзеге асыратын және ақпараттық жүйелерде электрондық сандық қолтаңба мен шифрлауды қолдануды қамтамасыз ететін бағдарламалық-техникалық құралдардың жиынтығы. АКҚҚ тәуелсіз бағдарламалық модульдер түрінде де, қолданбалы бағдарламалық жасақтамаға енгізілген құралдар түрінде де қолданылады;

12) **ҚТКТ** - Кері қайтарып алынған тіркеу куәліктерінің тізімі, қолданылуы тоқтатылған Тіркеу куәлігі туралы мәліметтерді қамтитын барлық Тіркеу куәліктерінің тізбесі, олардың сериялық нөмірлері, кері қайтарып алу күні мен себебі;

13) **Тіркеу куәлігінің мәртебесі** - тіркеу куәлігінің жарамдылығын тексеру нәтижесі;

14) **Куәландырушы орталығы (КО)** – электрондық сандық қолтаңбаның ашық кілтінің электрондық сандық қолтаңбаның жабық кілтіне сәйкестігін куәландыратын, сондай-ақ Тіркеу куәлігінің нақтылығын растайтын Банк немесе өзге де заңды тұлға;

15) **КО қатысушысы** - Банктің нақтылығы шеңберінде электрондық құжаттарды жинау, өңдеу, сақтау процестеріне қатысатын Тіркеу куәліктерінің иелері, мемлекеттік органдар, Банктің серіктестері;

16) **Тіркеу куәліктерінің қоймасы** - барлық Тіркеу куәліктерінің анықтамалығы және ҚТКТ;

17) **Электрондық сандық қолтаңба (ЭСҚ)** - Электрондық сандық қолтаңбаның көмегімен құрылған және электрондық құжаттың құрамының дұрыстығын, шынайылығын және өзгермейтіндігін растайтын электрондық сандық символдардың жиынтығы;

18) **Home Credit Bank Kazakhstan/ Home Credit Agent (HCA)** - Android және iOS платформалары үшін Google Play және AppStore дүкендерінде қолжетімді Банктің мобильді қосымшасы/қосымшасы.

2. Жалпы ережелер

2. Осы Саясат Тіркеу куәліктерін қолданудың жалпы қағидаларын айқындайды және «Банк Хоум Кредит» АҚ ЕБ Куәландырушы орталығының қызметі регламентінің ажырамас бөлігі болып табылады.

3. Осы Саясат Заңға және Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 23 желтоқсандағы № 1231 бұйрығымен бекітілген Қазақстан Республикасының Түбірлік куәландырушы орталығын, мемлекеттік органдардың куәландырушы орталығын, Қазақстан Республикасының Ұлттық куәландырушы орталығын және Қазақстан Республикасының сенім білдірілген үшінші тарапын қоспағанда, куәландырушы орталығының Тіркеу куәліктерін беру, сақтау, кері қайтарып алу және электрондық сандық қолтаңбаның ашық кілтінің тиесілілігі мен жарамдылығын растау қағидаларына сәйкес әзірленді.

3. Тіркеу куәліктерін пайдалану

4. Тіркеу куәліктері электрондық құжаттарды жасау кезінде ЭСҚ үшін, сондай-ақ осы тіркеу куәліктерінде көрсетілген мәліметтерге сәйкес Тіркеу куәліктерінің иелерін сәйкестендіру үшін пайдаланылады.

5. ЭСҚ «Банк Хоум Кредит» АҚ ЕБ-де шарттарға, өтініштерге және өзге де құжаттарға қол қою үшін (жеке тұлға мен «Банк Хоум Кредит» АҚ ЕБ арасында құжаттарға қол қою) пайдаланылады.

6. Тіркеу куәлігі ЭСҚ ашық кілтінің мәнін ЭСҚ-ның тиісті жабық кілтін пайдаланатын пайдаланушыны сәйкестендіретін ақпаратпен байланыстырады.

7. КО Банктің қорғалған жүйесінде сақталатын ЭСҚ жабық кілтін пайдаланушыға Банктің жеке кабинеті/HCA арқылы барлық қол қойылған электрондық құжаттар туралы ақпаратқа кіруге рұқсат береді. Барлық қол қойылған электрондық құжаттар туралы ақпаратты сақтау мерзімі пайдаланушының Тіркеу куәлігінің қолданылу мерзімі өткеннен кейін кемінде он бес жылды құрайды.

4. Тіркеу куәлігінің мазмұны

8. Тіркеу куәлігі төмендегі мәліметтерді қамтиды:

1) Тіркеу куәлігінің нөмірі және оның қолданылу мерзімі;

2) ЭСҚ иесін сәйкестендіруге мүмкіндік беретін деректер;

3) ЭСҚ ашық кілті;

4) ЭСҚ қолдану салалары және қолдану шектеулері туралы ақпарат;

5) КО деректемелері.

9. Тіркеу куәліктерінде көрсетілген жеке тұлғаның жеке деректері жеке басты куәландыратын құжаттарда көрсетілген мәліметтермен дәл сәйкес келуі тиіс.

10. КО ITU-T X. 509 3 нұсқасының және RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile) ұсынымдарына сәйкес келетін Тіркеу куәліктерін шығарады. Шығарылған Тіркеу куәліктері «Субъект» және «Баспагер» жолақтарында ITU-T X. 501 (Distinguished Names (бұдан әрі - DN)) ұсынымдарына сәйкес ұсынылған мәліметтерді қамтиды.

11. Тіркеу куәліктері үшін C (country) белгісі елдің екі әріптік кодын қамтиды (ISO 3166-1 alpha-2).

12. Тіркеу куәліктері үшін O белгісінде заңды тұлғаның – Тіркеу куәлігі арналған ақпараттық жүйе иесінің атауы болуы мүмкін.

13. Тіркеу куәліктері үшін CN (Common Name) белгісінде Тіркеу куәлігі иесінің тегі мен аты (қатаң көрсетілген тәртіппен) болады. Аты бірдей әр түрлі жеке тұлғалар арасындағы бірмәнсіздікті болдырмау үшін Тіркеу куәлігінің CN белгісінде жеке тұлғаның сәйкестендіру атауынан басқа қосымша мәтін болуы мүмкін. Қосымша мәтін жеке тұлғаның атымен шатастырмау үшін пішімделуі тиіс. Мәтін бөлгіш ретінде бос орыннан кейін жеке тұлғаның атынан кейін тұруы және жақшаға алынуы тиіс.

14. Serial Number белгісін ұйым мен жеке тұлғаларды сәйкестендіру үшін пайдалануға болады. Құрамында CWA 16036 (CyberIdentity - Unique Identification Systems For Organizations and Parts Thereof) ұсыныстарына сәйкес идентификатор бар.

15. Сонымен қатар, E белгісі (email) пайдаланылуы мүмкін.

16. DN ерекше атауы әр Өтініш беруші үшін ерекше болуы керек. Егер Өтінім беруші ұсынған DN атауы бірегей болмаса, онда КО Өтінім берушіден атаудың бірегейлігін қамтамасыз ету үшін CN белгісін өзгерту арқылы сұранысты қайта ұсынуды талап етеді. Егер екі атау тек регистрмен, астын сызу таңбаларының санымен немесе сөздер арасындағы бос орындармен ерекшеленсе, олар

осы құжатқа сәйкес бірдей деп саналады. Осылайша, есімдерді ажырату үшін регистр, астын сызу немесе бос орын таңбаларын қолдануға болмайды. Тіркеу куәлігі бірегей жеке тұлғаға немесе ресурсқа немесе қызметке қатысты болуы тиіс. Тіркеу куәлігін тек Тіркеу куәлігінің иесі ғана пайдалануы тиіс. КО DN ерекше атауын басқа өтініш беруші қайта пайдаланбайтынына кепілдік береді. Егер жеке тұлға қолданыстағы Тіркеу куәлігіндегідей DN атауы бар Тіркеу куәлігін сұраса (осы Тіркеу куәлігінің мәртебесіне қарамастан) және сұрау Тіркеу куәлігін өзгерту бойынша болмаса, онда КО – ның уәкілетті қызметкері жеке тұлғаның - бастапқы тіркеу куәлігін алу кезінде сәйкестендірілген субъект екенін тексеру үшін жеке куәландыру ақпаратын пайдалана алады. Егер жеке басын анықтау мүмкін болмаса, DN атауы қайта пайдаланылмайды. Әртүрлі Тіркеу куәліктерінің иелеріне тиесілі бірнеше Тіркеу куәліктерінде көрсетілетін мәліметтер толық сәйкес келген жағдайларда, оларға олардың иелерін бір мәнді сәйкестендіруге мүмкіндік беретін арнайы белгі (мысалы, сериялық нөмір) енгізіледі.

17. Шығарылған Тіркеу куәліктері мен ҚТКТ тіркеу куәліктерінің қоймасына енгізіледі және олардың қолданылуы басталған күннен кешіктірілмей жарияланады. ҚТКТ қолданылу мерзімі күнтізбелік 7 (жеті) күнді құрайды, ҚТКТ жариялау кері қайтарылған (тоқтатыла тұрған) тіркеу куәліктерінің пайда болуына қарай жүргізіледі.

18. Тіркеу куәліктерінің мәртебесі туралы мәліметтер КО қызметінің регламентіне сәйкес жарияланады.

5. Тіркеу куәліктерін дайындау және негізгі жұпты орнату

19. КО Тіркеу куәліктерін беруге арналған өтініште көрсетілген мәліметтерге сәйкес Тіркеу куәліктерін дайындайды. Тіркеу куәліктерінің форматы ITU-T X. 509v3 және RFC 5280 ұсынымдарына негізделген.

20. КО ЭСҚ кілттері сертификатталған АККҚ қолдану арқылы қалыптастырылады.

21. ЭСҚ кілттері ГОСТ 34.310-2004 алгоритміне сәйкес қалыптастырылады.

22. ЭСҚ жабық кілтінің генерациялау және сапасын тексеру параметрлері ҚР СТ 1073-2007 сәйкес сертификатталған АККҚ-мен автоматты түрде анықталады.

6. Тіркеу куәліктерін кеңейту

23. Тіркеу куәліктерінде төмендегі толықтырулар болуы мүмкін:

authorityKeyIdentifier	КО уәкілетті тұлғасы кілтінің сәйкестендіргіші
subjectKeyIdentifier	Тіркеу куәлігі иесінің кілтінің сәйкестендіргіші
ExtendedKeyUsage	Электрондық сандық қолтаңбасы бар электрондық құжат заңды мәнге ие болатын кілтті пайдалану саласы (салалары). Мүмкін мәндер: Server Authentication, Client Authentication, Secure e-mail, Time stamping, IPSec (Tunnel, User).
KeyUsage	Кілттің мақсаты. Мүмкін мәндер: Сандық қолтаңба, Бас тартпаушылық, Кілттерді шифрлау, Деректерді шифрлау.
Basic constraints (optional)	Субъект түрі
cRLDistributionPoint	Күші жойылған (кері қайтарып алынған) Тіркеу куәліктерінің тізімін тарату нүктесі
certificatePolicies	Тіркеу куәліктерінің саясаты
Authority Information Access (optional)	Тіркеу куәліктерінің мәртебесі туралы ақпарат алу тәсілі

6.1. Алгоритмдердің объектілік идентификаторлары

24. КО ЭСҚ құралы алгоритмдерінің келесі сәйкестендіргіштерін пайдаланады:

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. Түбірлік КО Тіркеу куәлігінің құрылымы (ГОСТ 34.310-2004 алгоритмі)

Атауы	**Мазмұны**
Нұсқасы	V3
Сериялық нөмірі	Тіркеу куәлігінің бірегей сериялық нөмірі
Қол қою алгоритмі	ГОСТ 34.310-2004 қол қою алгоритмі
Жеткізуші	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
Әрекет ету мерзімі	жарамды: YYMMDDHHMMSSZ UTC бастап жарамды: YYMMDDHHMMSSZ UTC дейін
Ашық кілт	Екілік түрдегі ашық кілттің мәні
Қолы	ЭСҚ

6.3. КО қатысушысының Тіркеу куәлігінің құрылымы (ГОСТ 34.310-2004 алгоритмі)

Атауы	**Мазмұны**
Нұсқасы	V3
Сериялық нөмірі	Тіркеу куәлігінің бірегей сериялық нөмірі
Қол қою алгоритмі	ГОСТ 34.310-2004 қол қою алгоритмі
Жеткізуші	CN = homecredit.kz Root Certificate Authority O = Subsidiary Bank Joint-Stock Company Home Credit Bank C=KZ
Субъект	Жеке тұлғалар: CN = Толық аты-жөні SERIALNUMBER = IIN123456789012 C=KZ Мұнда IIN123456789012 - жеке тұлғаның ЖСН
Әрекет ету мерзімі	жарамды: YYMMDDHHMMSSZ UTC бастап жарамды: YYMMDDHHMMSSZ UTC дейін
Ашық кілт	Екілік түрдегі ашық кілттің мәні
Қолы	Сандық қолтаңба.

7. ҚТКТ сипаттамасы

25. КО ҚТКТ-ны ITU-T X. 509v3 және RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile) ұсынымдарына негізделген форматта электрондық нысанда қалыптастырады.

7.1. ҚТКТ кеңейту

26. КО келесі толықтыруларды пайдалана алады:

CRL number	ҚТКТ реттік нөмірі
Authority Key Identifier	КО уәкілетті тұлғасы кілтінің сәйкестендіргіші
Reason Code	Тіркеу куәлігін кері қайтарып алу себебінің коды. Мүмкін мәндер (қоса алғанда, бірақ шектелместен): Пайдаланушы кілтін бұзу КО кілтінің жария етілуі; Тіркеу куәлігінің қолданылуын тоқтату.

7.2. ҚТКТ құрылымы (ГОСТ 34.310-2004 алгоритмі)

Атауы	Мазмұны
Нұсқасы	V2
Жеткізуші	CN = homecredit.kz Root Certificate Authority O = Subsidiary Bank Joint-Stock Company Home Credit Bank C=KZ
Шығарылған күні	жарамды: YYMMDDHHMMSSZ UTC бастап
Жаңарту күні	жарамды: YYMMDDHHMMSSZ UTC дейін
Кері қайтарып алынған тіркеу куәліктері	Келесі түрдегі дәйектілік: CertificateSerialNumber (Тіркеу куәлігінің сериялық нөмірі) Time (Кері қайтарып алуға өтінішті өңдеу күні мен уақыты)
Қол қою алгоритмі	ГОСТ 34.310-2004 қол қою алгоритмі
Қолы	Сандық қолтаңба.

8. Қорытынды ережелер

27. Саясат Банктің уәкілетті органы бекіткен және «Банк Хоум Кредит» АҚ ЕБ сайтында (https://homecredit.kz/) жарияланған күннен бастап күшіне енеді және Саясаттың жаңа редакциясы жарияланғанға дейін әрекет етеді.

28. Саясат Саясаттың жаңа редакциясымен ауыстырылған жағдайда тоқтатылады.

29. Саясаттың өзгерістерін бекіту туралы КО қатысушыларының ресми хабарламасы КО интернет-сайтында жариялау: (https://homecredit.kz/).

30. Саясатқа енгізілетін барлық өзгерістер күшіне енеді және оларды жариялағаннан кейін дереу КО-ның барлық қатысушылары орындауға міндетті болады.

31. Осы Саясат күшіне енген күннен бастап «Банк Хоум Кредит» АҚ ЕБ Куәландырушы орталығының Тіркеу куәліктерін қолдану саясатының («Банк Хоум Кредит» АҚ ЕБ Директорлар кеңесінің шешімімен бекітілген, 17.09.2020 ж. № 31/2020 хаттама) күші жойылды деп танылсын.

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 СОРС вносятся в Хранилище Регистрационных свидетельств и публикуются не позднее даты начала их действия. Срок действия СОРС составляет 7 (семь) календарных дней, публикация СОРС 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.).