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

«Kaspi Bank» АҚ Куәландырушы
орталығының құжаттарын бекіту туралы»
«28» __11__ 2023 жылғы № ____ бұйрыққа
№ 3 қосымша

«Kaspi Bank» АҚ Куәландырушы орталығының тіркеу куәліктерін қолдану саясаты

«Kaspi Bank» АҚ Куәландырушы орталығының тіркеу куәліктерін қолдану саясаты (бұдан әрі – Саясат) КО Қатысушыларының Тіркеу куәліктерін қолдануының жалпы ережелерін баяндайды. Саясат RFC 3647 ұсынымдарына сәйкес дайындалды.
Саясат «Kaspi Bank» АҚ Куәландырушы орталығы қызметінің регламентінің (бұдан әрі – Регламент) ажырамас бөлігі болып табылады және КО шығаратын Тіркеу куәліктерінің түрлерін, оларды тексеру рәсімдерін және олардың қолданысын айқындайды.

1. Тіркеу куәліктерін пайдалану

1.1. Тіркеу куәліктері электрондық құжаттарды жасаған кезде, сондай-ақ Тіркеу куәліктерінің иелерін бірдейлендіру үшін осы Тіркеу куәліктерінде көрсетілген мәліметтерге сәйкес ЭЦҚ үшін пайдаланылады.

1.2. Тіркеу куәлігі иесінің ЭЦҚ-сын қолдану саласы Регламентте айқындалған.

1.3. Тіркеу куәлігі ЭЦҚ-ның Ашық кілтінің мәнін ЭЦҚ-ның тиісті Жабық кілтін пайдаланатын пайдаланушыны сәйкестендіретін ақпаратпен байланыстырады. Тіркеу куәлігін Тіркеу куәлігінің иесі немесе ЭЦҚ-ны тексеру үшін Тіркеу куәлігінен ЭЦҚ-ның Ашық кілтін іске қосатын Сенім білдіретін тарап қолданады. Тіркеу куәлігіне сенім білдіру деңгейі келесі факторлармен:

1) Регламентпен;
2) Саясатпен;
3) Қазақстан Республикасының заңнамасымен айқындалады.

2. Тіркеу куәлігінің мазмұны

2.1. КО 3-нұсқаның ITU-T X.509 және RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile) ұсынымдарына сәйкес келетін Тіркеу куәліктерін береді. Берілген Тіркеу куәліктерінің «Субъект» және «Баспагер» жолдарында ITU-T X.501 (Distinguished Names (бұдан әрі – DN)) ұсынымдарына сәйкес берілген мәліметтер қамтылған.

2.2. Тіркеу куәліктерінде көрсетілген жеке тұлғаның немесе заңды тұлғаның сенімхат бойынша өкілінің жеке деректері жеке басын куәландыратын құжаттарда көрсетілген мәліметтермен дәл сәйкес келуге тиіс.

2.3. Тіркеу куәліктерінің барлық типтері үшін C (Country) атрибутында елдің екі әріпті коды (ISO 3166-1 alpha-2) қамтылған.

2.4. Заңды тұлғалардың Тіркеу куәліктері үшін O (Organization) атрибуты заңды тұлғаның атауын қамтиды. Жеке тұлғалардың Тіркеу куәліктері үшін O атрибуты заңды тұлға – Тіркеу куәлігі арналған ақпараттық жүйенің иесінің атауын қамтуы мүмкін.

2.5. Жеке және заңды тұлғалардың Тіркеу куәліктері үшін CN (Common Name) атрибуты жеке тұлға – Тіркеу куәлігінің иесінің тегін, есімін және әкесінің атын (бар болса) (қатаң көрсетілген тәртіппен) қамтиды. Есімдері бірдей әртүрлі жеке тұлғалардың арасында күрделілікті болдырмау үшін, Тіркеу куәлігінің CN атрибутында жеке тұлғаның сәйкестендіруші есімінен бөлек басқа қосымша мәтін қамтылуы мүмкін. Қосымша мәтін оны жеке тұлғаның есімімен ауыстырып алмайтындай етіп жасалуға тиіс. Мәтінді бөлуші ретінде бос орын қалдырып, жеке тұлғаның есімінен кейін жіберу және шеңбер жақшаға алу ұсынылады. КО CN атрибутының ішіндегісін тексермейді, сондықтан сенім білдіретін тараптарға мәтіннің мазмұнына арқа сүйеуге тыйым салынады. Сервердің Тіркеу куәліктері үшін CN атрибутында сервердің толық домендік атауы қамтылған. Қызметтердің Тіркеу куәліктері үшін CN атрибутында қызметтің атауы қамтылған.

2.6. Serial Number атрибуты ұйымдар мен жеке тұлғаларды сәйкестендіру үшін пайдаланылуы мүмкін. Онда CWA 16036 ұсынымдарына сәйкес сәйкестендіруші қамтылған (Cyber-Identity - Unique Identification Systems For Organizations and Parts Thereof).

2.7. UID (Unique ID) атрибуты кейбір жағдайда бірдей болатын есімдерді (жеке тұлғаның тегін, есімін және әкесінің атын) ажырату үшін пайдаланылуы мүмкін. Онда үкімет немесе азаматтық билік жеке тұлғаға тағайындаған сәйкестендіруші қамтылған.

2.8. Қосымша OU (Organization Unit), L (Locality) және E (e-mail) атрибуттары пайдаланылуы мүмкін.

2.9. DN ерекшелендіретін есімі әр Өтініш беруші үшін бірегей болуға тиіс. Егер Өтініш берушінің берген DN есімі бірегей болмаса, онда КО Өтініш берушіден есімнің бірегейлігін қамтамасыз ету үшін CN атрибутын өзгертіп, сұратуды қайтадан ұсынуды талап етеді. Осы құжатқа сай екі есім, егер олар тек тіркеліммен, астын сызу символдарының немесе сөздердің арасындағы бос орынның санымен ғана ерекшеленсе, сәйкес деп саналады. Сонымен тіркелім, астын сызатын немесе бос орынның символдары есімдерді ажырату үшін пайдаланылмауға тиіс. Тіркеу куәлігі бірегей жеке/заңды тұлғаға немесе ресурсқа, немесе қызметке жатқызылуға тиіс. Тіркеу куәлігінің иесі ғана Тіркеу куәлігін пайдалануық керек. КО DN ерекшелендіретін есімін басқа Өтініш беруші қайта пайдаланбайтынына кепілдік береді. Егер жеке немесе заңды тұлға қазір бар Тіркеу куәлігіндегідей DN есімімен Тіркеу куәлігін сұратса (бұл Тіркеу куәлігінің күйіне қарамастан) және Тіркеу куәлігін өзгертуге арналған сұрату болмаса, онда КО уәкілетті жұмыскері жеке/заңды тұлға – бастапқы Тіркеу куәлігін алған кезде сәйкестендірілген субъект екенін тексеру үшін дербес куәландырушы ақпаратқа сүйене алады. Егер сәйкестігі анықталмаса, DN есімі қайта пайдаланылмайды. Бірнеше Тіркеу куәліктерінде көрсетілетін, әртүрлі Тіркеуші куәліктерінің иелеріне тиесілі мәліметтер толық сәйкес келген жағдайларда, оларға арнайы атрибут (мысалы, сериялық нөмірі) енгізіледі, атрибут олардың иелерін сәйкестендіруге мүмкіндік береді.

2.10. Берілген Тіркеу куәліктері және ККТКТ Тіркеу куәліктерін сақтайтын орынға енгізіледі және олардың қолданысы басталған күннен кешіктірілмей жарияланады. ККТКТ-тың қолданылу мерзімі күнтізбелік 7 (жеті) күнді құрайды, ККТКТ кері қайтарылған (тоқтата тұрылған) Тіркеу куәліктерінің пайда болуына қарай жарияланады.

2.11. Тіркеу куәліктерінің мәртебесі туралы мәліметтер Регламентке сәйкес жарияланады.

3. Тіркеу куәліктерін дайындау және кілттік жұбын орнату

3.1. КО Тіркеу куәліктерін Өтініште көрсетілген мәліметтерге сәйкес дайындайды. Тіркеу куәліктерінің пішімі ITU-T X.509v3 және RFC 5280 ұсынымдарына негізделген.

3.2. КО ЭЦҚ кілттері сертификатталған АКҚҚ қолданылып жасақталады.

3.3. ЭЦҚ кілттері 34.310-2004 МЕМСТ алгоритміне сәйкес жасақталады.

3.4. ЭЦҚ Жабық кілтінің генерациясы мен сапасын тексеру параметрлері сертификатталған АКҚҚ-мен 1073-2007 ҚР СТ-ға сәйкес автоматты түрде айқындалады.

3.5. ЭЦҚ жабық кілттері бұлтты ЭЦҚ-да Тіркеу куәліктерінің қолданылу мерзімі ішінде сақталады.

4. Тіркеу куәліктерін кеңейту

Тіркеу куәліктерінде келесі толықтырулар қамтылуы мүмкін:

authorityKeyIdentifier	КО уәкілетті тұлғасының кілтінің сәйкестендірушісі
subjectKeyIdentifier	Тіркеу куәлігінің иесінің кілтінің сәйкестендірушісі
ExtendedKeyUsage	Электрондық цифрлық қолтаңбамен электрондық құжаттың заңды маңызы болатын кілтті пайдалану саласы (салалары). Ықтимал мәндері: Server Authentication, Client Authentication, Secure e-mail, Time stamping, IPSec (Tunnel, User), ▪ 1.2.398.3.14.9 - Кілттер қоймасы ◦ 1.2.398.3.14.9.1 – Файлдық сақтау орны ◦ 1.2.398.3.14.9.2 - Бұлтты сақтау орны ▪ 1.2.398.3.14.10 – Пайдаланушылар ▪ 1.2.398.3.14.10.1 – Жеке тұлға ◦ 1.2.398.3.14.10.2 - Заңды тұлға • 1.2.398.3.14.10.2.1 - Заңды тұлғаның бірінші басшысы • 1.2.398.3.14.10.2.2 - Қол қою құқығы берілген тұлға
KeyUsage	Кілттің мақсаты. Ықтимал мәндері: Тіркеу куәліктеріне қол қою, ККТКТ-ге дербес қол қою (CRL), ККТКТ-ге қол қою (CRL), цифрлық қолтаңба, бас тартпау, кілттерді шифрлау, деректерді шифрлау, кілттерді келісу

Basic constraints (optional)	Субъектінің типі
cRLDistributionPoint	Жойылған (кері қайтарылған) Тіркеу куәліктерінің тізімін тарату орны
certificatePolicies	1.2.398.3.14.2 - Тіркеу куәліктерінің саясаты:
Authority Information Access (optional)	Тіркеу куәліктерінің күйі туралы ақпаратты алу тәсілі

4.1. Алгоритмдердің Объектілік сәйкестендірушілері

34.10-2004 МЕМСТ	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) sign(2)
34.311-95 МЕМСТ	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) hash(1)
34.310-2004 МЕМСТ	1.2.398.3.10.1.1.1.2 қолтаңбасы 34.310-2004 МЕМСТ
34.311-95 МЕМСТ	iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) hash(1)
28147-89 МЕМСТ	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. Негізгі КО-ның Тіркеу куәліктерінің құрылымы (34.310-2004 МЕМСТ алгоритмі)

Атауы	Мазмұны
Нұсқа	V3
Сериялық нөмірі	Тіркеу куәлігінің бірегей сериялық нөмірі
Қолтаңбаның алгоритмі	34.310-2004 МЕМСТ қолтаңба алгоритмі
Жеткізуші	CN = Kaspi.kz Root Certificate Authority O = «Kaspi Bank» АҚ C = KZ
Субъект	CN = Kaspi.kz Root Certificate Authority O = «Kaspi Bank» АҚ C = KZ
Қолданылу мерзімі	YYMMDDHHMMSSZ UTC бастап жарамды YYMMDDHHMMSSZ UTC дейін жарамды
Ашық кілт	Ашық кілттің бинарлық түрдегі мәні

4.3. КО Қатысушысының Тіркеу куәлігінің құрылымы (34.310-2004 МЕМСТ алгоритмі)

Атауы	Мазмұны
Нұсқа	V3
Сериялық нөмірі	Тіркеу куәлігінің бірегей сериялық нөмірі
Қолтаңбаның алгоритмі	34.310-2004 МЕМСТ қолтаңба алгоритмі
Жеткізуші	CN = Kaspi.kz Root Certificate Authority O = «Kaspi Bank» АҚ C = KZ
Субъект	Жеке тұлғалар: CN = толық Т.А.Ә. SERIALNUMBER = IIN123456789012 C = KZ мұнда IIN123456789012 – жеке тұлғаның ЖСН. Заңды тұлғалар: CN = жұмыскердің толық Т.А.Ә. SERIALNUMBER = IIN123456789012 O = Ұйымның атауы OU = BIN123456789012 C = KZ мұнда IIN123456789012 – жеке тұлғаның ЖСН, BIN123456789012 – заңды тұлғаның БСН
Қолданылу мерзімі	YYMMDDHHMMSSZ UTC бастап жарамды YYMMDDHHMMSSZ UTC дейін жарамды
Ашық кілт	Ашық кілттің бинарлық түрдегі мәні

5. ККТКТ сипаттамасы

КО ККТКТ-ны ITU-T X.509v3 және RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile) ұсынымдарына негізделген пішімде электрондық нысанда жасақтайды.

5.1. ККТКТ-ты кеңейту

КО келесі толықтыруларды пайдалана алады:

CRL number	ККТКТ реттік нөмірі
Authority Key Identifier	КО уәкілетті тұлғасының кілтінің сәйкестендірушісі
Reason Code	Тіркеу куәлігін кері қайтару себебінің коды. Ықтимал мәндері (оған қоса, бірақ шектелмей): 1 - Кілттерді компрометациялау 3 - Пайдаланушының аты немесе сертификаттағы басқа ақпарат өзгертілді 4 - Сертификат басқасымен ауыстырылды 5 - Сертификат берілген мақсаттар үшін енді қажет емес.

5.2. ККТКТ-ның құрылымы (34.310-2004 МЕМСТ алгоритмі)

Атауы	Мазмұны
Нұсқа	V2
Баспагер	CN = Kaspi.kz Root Certificate Authority O = «Kaspi Bank» АҚ C = KZ
Бастап жарамды	YYMMDDHHMMSSZ UTC бастап жарамды
Келесі жаңарту	YYMMDDHHMMSSZ UTC дейін жарамды
Қолтаңбаның алгоритмі	34.310-2004 МЕМСТ қолтаңба алгоритмі
CRL нөмірі	CRL нөмірі
Куәліктер орталығы кілтінің сәйкестендірушісі	Кілт сәйкестендірушісі Сертификатты жеткізуші: Каталог мекенжайы: CN = Kaspi.kz Root Certificate Authority O = «Kaspi Bank» АҚ C = KZ Сертификаттың сериялық нөмірі
Таңба ізі	Сертификат хэші
Кері қайтарып алынған Тіркеу куәліктері	Келесі түрдің реттілігі: Сериялық нөмірі Кері қайтарып алынған күн Кері қайтару себебінің коды (CRL)

6. КО туралы ақпарат

6.1. Саясат оны www.kaspibank.kz сайтында жариялаған сәттен бастап күшіне енеді және Саясаттың жаңа редакциясын жариялағанға дейін қолданылады.

6.2. КО-ның www.kaspibank.kz/?ft=245&type=497 мекенжайындағы интернет-сайтында жариялау КО Қатысушыларына Саясаттың өзгерістерін бекіту туралы ресми хабарлау болады.

6.3. Саясатқа енгізілетін барлық өзгерістер баспада жарияланғаннан кейін дереу күшіне енеді және КО барлық Қатысушыларының орындауы үшін міндетті болады.

***