

№ 1479**2026 yil «26» «sentabr»**

ATB «O'zsanoatqurilishbank» uchun «STYX» dasturiy majmuasini (takomillashtirilgan modullar va amaldagi mahsulotlar) yangilash, litsenziyalash va texnik qo'llab-quvvatlash bo'yicha texnik topshiriq

1. UMUMIY QOIDALAR

1.1 Hujjatning vazifasi

Ushbu Texnik topshiriq ATB «O'zsanoatqurilishbank» uchun «STYX KMS» dasturiy majmuasining takomillashtirilgan modullarini yetkazib berish, litsenziyalash va qo'llab-quvvatlashga qo'yiladigan talablarni belgilaydi. Hujjat loyiha bo'yicha ishlarni bajarish uchun asos bo'lib xizmat qiladi va Ijrochi hamda Buyurtmachi o'rtasidagi o'zaro hamkorlikni tartibga soladi.

1.2 Loyihaning maqsadi

Loyihaning maqsadi quyidagilardan iborat:

- ATB «O'zsanoatqurilishbank» uchun «STYX KMS» dasturiy majmuasini modernizatsiya qilish, optimallashtirish va dolzarb versiyaga yangilash.
- Mobil ERIn qo'llab-quvvatlash maqsadida joriy Styx Metin Mobile SDK modernizatsiya qilish.
- O'zR Markaziy banki Yagona reyestri bilan integratsiya va O'zbekiston Respublikasi Markaziy banki qarorlariga muvofiqlikni ta'minlash.
- Yangi dasturiy modullar hisobiga tizim funksionalligini kengaytirish.

1.3. Xarid predmetining tasnifi (qo'shimcha talab)

Ijrochi texnik-tijorat taklifini tayyorlash jarayonida xarid qilinayotgan dasturiy ta'minot va xizmatlarni quyidagi toifalar bo'yicha tasniflashi hamda Buyurtmachi bilan kelishishi lozim.

Litsenziya asosida yetkazib beriladigan bazaviy dasturiy platformalar (Upgrade):

- STYX KMS;
- STYX CA;
- STYX AS.

Mazkur komponentlar Buyurtmachining mavjud PKI infratuzilmasidagi dasturiy ta'minotni ishlab chiqaruvchi tomonidan qo'llab-quvvatlanayotgan eng so'nggi barqaror versiyaga (Upgrade) yangilashni nazarda tutadi.

Litsenziya asosida yetkazib beriladigan qo'shimcha dasturiy mahsulotlar:

- STYX Archive Module;
- Universal StyxClient Driver;
- Styx Metin Mobile SDK;
- STYX Cluster Module (Active/Passive).

Mazkur komponentlar tayyor dasturiy mahsulot sifatida yetkazib berilishi, o'rnatilishi, sozlanishi va Buyurtmachining mavjud PKI infratuzilmasiga integratsiya qilinishi lozim.

Noldan ishlab chiqiladigan (Custom Development) dasturiy modullar:

- ERI kalitlari ombori hisobi;
- Boshqaruv paneli (Dashboard)ning kengaytirilgan qismi;
- Hisobotlar modulining yangi shablonlari;
- Mijozlarni filiallar o'rtasida ko'chirish moduli;
- STYX Auto Update mexanizmi;
- «Tekmetes» MBX axborot tizimi bilan integratsiya.

Mazkur modullar Buyurtmachining texnik topshirig'i asosida ishlab chiqilishi, sinovdan o'tkazilishi va amaldagi STYX PKI infratuzilmasiga to'liq integratsiya qilinishi lozim.

Litsenziyalash talablari

Mazkur loyiha doirasida yuqorida ko'rsatilgan barcha dasturiy komponentlar **yagona litsenziya to'plami (1 ta License Package)** sifatida yetkazib beriladi. Litsenziya tarkibiga STYX KMS, STYX CA, STYX AS, STYX Archive Module, Universal StyxClient Driver, Styx Metin Mobile SDK hamda STYX Cluster Module (Active/Passive) kiradi.

Texnik-tijorat taklifida litsenziyaning tarkibi, foydalanish huquqlari, texnik qo'llab-quvvatlash muddati, yangilanish (Upgrade) huquqi va kafolat shartlari batafsil ko'rsatilishi hamda Buyurtmachi bilan kelishilishi lozim.

2. TIZIM ARXITEKTURASI

Tizim Linux platformasida amalga oshirilgan va 3 ta virtual mashinaga (VM) ajratilgan. Har bir VM aniq belgilangan vazifalar doirasini bajaradi, bu komponentlarni izolyatsiya qilishni, yuqori xavfsizlikni va mustaqil masshtablashni ta'minlaydi. Linux platformasida ishlovchi virtual mashinalar (VM) hamda ularni joylashtirish uchun zarur bo'lgan server infratuzilmasi bank tomonidan taqdim etiladi.

Key Management System — Kalitlarni boshqarish tizimi

- PKI standartlariga muvofiq kriptografik kalitlarni (yopiq va ochiq) generatsiya qilish.
- Kalitlarni rollar bo'yicha kirishni chegaralagan holda xavfsiz saqlash.
- Kalitlarni himoyalangan kanallar orqali tizim komponentlariga (CA, AS) taqsimlash va uzatish.
- Kalitlarni jadval bo'yicha yoki hodisaga ko'ra yangilash va rejali rotatsiya qilish.
- Uzilishlarga chidamlilik uchun STYX Cluster Module (Active/Passive) moduli bilan integratsiya.
- Kalitlar bilan barcha operatsiyalar jurnalini yuritish (audit-log).

VM 2: Styx CA

Certificate Authority — Sertifikatsiya markazi

- Foydalanuvchilar, serverlar va qurilmalar uchun X.509 raqamli sertifikatlarini berish.
- CA ildiz kaliti yordamida sertifikatlarni imzolash.
- Bekor qilingan sertifikatlar ro'yxatini (CRL — Certificate Revocation List) saqlash va yuritish.
- Sertifikatlar holatini real vaqt rejimida onlayn tekshirish uchun OCSP protokolini qo'llab-quvvatlash.
- Administrator so'roviga ko'ra yoki muddat tugashi bo'yicha sertifikatlarni bekor qilish (chaqirib olish).
- O'zR Markaziy banki Yagona reyestri bilan REST API protokoli orqali integratsiya.
- Berilgan va bekor qilingan sertifikatlarning to'liq tarixini yuritish.

VM 3: Styx AS

Authentication Service — Autentifikatsiya xizmati

- Sertifikatsiya markazi (CA) tomonidan berilgan raqamli imzolarni tekshirish.
- Foydalanuvchilar va serverlarni X.509 sertifikatlari asosida autentifikatsiya qilish.
- Imzolangan hujjatlar va tranzaksiyalarning haqiqiyliги hamda yaxlitligini tasdiqlash.
- Sertifikatning dolzarbligini OCSP va CRL orqali tekshirish.
- Tizimning istalgan komponenti tomonidan imzolangan ma'lumotlarga ishonchni ta'minlash.
- Dolzarb ochiq kalitlarni olish uchun KMS bilan o'zaro aloqa.
- Audit maqsadlarida barcha autentifikatsiya operatsiyalarini jurnalga yozish.

Ushbu yo'nalish bo'yicha ishlar quyidagilarni o'z ichiga oladi:

№	Ishlar mazmuni
01	STYX dasturiy majmuasini (KMS, CA, AS) bankning amaldagi virtual mashinalarida so'nggi dolzarb versiyaga yangilash.
02	Yangilangan komponentlarning ATB «O'zsanoatqurilishbank» joriy infratuzilmasi bilan moslashuvchanligini tekshirish.
03	Yangilashdan so'ng tizimning barcha modullari ishini to'g'riligini sinovdan o'tkazish.
04	Sinov jarayonida aniqlangan kamchilik va xatolarni bartaraf etish.
05	Boshqa BANK larning STYX dasturiy ta'minotiga xalaqit qilmasligini qat'ian choralari ko'rish. (texnik talab sifatida: yangilash jarayonida xizmatlarning uzluksiz ishlashi ta'minlanishi, tizimning mavjud funktsionalligi buzilmasligi hamda boshqa STYX instansiyalariga salbiy ta'sir ko'rsatmasligi lozim.)
06	SQB Business mijozlari faqat SQB Styx (ERI) dasturini qiyinchiliklarsiz ishlatishini ta'minlash. (texnik talab sifatida: yangilanishdan so'ng SQB Business mijozlari SQB Styx (ERI) dasturidan uzluksiz va xatosiz foydalanishini tekshiruvchi funktsional va yuklama testlari o'tkazilishi lozim.)

Eslatma: Barcha ishlar ATB «O'zsanoatqurilishbank» ning amaldagi infratuzilmasida bankning asosiy biznes-jarayonlarini to'xtatmasdan bajariladi.

Joriy va maqsadli versiyalar: Ijrochi ATB «O'zsanoatqurilishbank»da hozirda ishlab turgan STYX KMS, Styx CA va Styx AS komponentlarining aniq joriy versiya raqamlarini, shuningdek ular yangilanadigan maqsadli versiya raqamlarini ushbu bo'limda aniq ko'rsatishi lozim (masalan: STYX KMS v.X.X → v.Y.Y).

2.2 Server infratuzilmasiga qo'yiladigan talablar

ATB «O'zsanoatqurilishbank» ning server infratuzilmasi o'rnatilgan va ishlamoqda. Ushbu loyiha doirasida yangi uskunalar o'rnatish talab etilmaydi.

3. DASTURIY MODULLAR VA KOMPONENTLAR

Loyiha doirasida Styx KMS majmuasining bazaviy funktsionalligini kengaytiruvchi quyidagi dasturiy modullar yetkazib beriladi va o'rnatiladi:

Modul / Komponent	Turi	Vazifasi
Styx Archive Module	Arxivlash	Bekor qilingan, muddati tugagan va yaroqsiz sertifikatlarni uzoq muddat saqlash va arxivlashni ta'minlash.
Universal StyxClient Driver	Mijoz drayveri	Windows 7, 8, 8.1, 10, 11 va macOS ni qo'llab-quvvatlash — token va sertifikatlar bilan ishlash.
Styx Metin Mobile SDK	Mobil SDK	ERI va kriptografik operatsiyalarni mobil ilovalarga integratsiya qilish.
STYX Cluster Module (Active/Passive)	Klasterlash	Tizimning uzilishlarga chidamliligi va yuqori mavjudligini ta'minlash.
ERI kalitlari hisobi (ombor hisobi)	Kalitlarni boshqarish	Yangi sotib olingan ERI kalitlarini qabul qilish va hisobga olish; bank va filiallar kesimida umumiy miqdorni ko'rsatish; so'rov yuborish va sertifikatlarni faqat ro'yxatga olingan kalitlarga

Modul / Komponent	Turi	Vazifasi
		yozish.
STYX Auto Update yaratilsin	Avtomatik yangilanish moduli (Auto Update)	STYX Token Manager dasturining yangi versiyalarini avtomatik tarqatish (Auto Update) mexanizmini ishga tushirish maqsadida SQB Business serverida alohida papka (directory) ajratilishi talab etiladi. Mazkur papkaga STYX Token Manager'ning yangi versiyalari joylashtiriladi va mijoz dasturi ushbu manzilni tekshirib, yangi versiya mavjud bo'lsa avtomatik ravishda yuklab olib o'rnatadi. Texnik talablar SQB Business serverida STYX Auto Update uchun alohida katalog yaratilsin. Papka HTTP/HTTPS orqali o'qish (Read) huquqi bilan ochilsin. Yangi versiyalarni joylashtirish uchun faqat administratorlarga yozish (Write) huquqi berilsin. Serverda kamida 200 mb bo'sh joy ajratilsin (zaruratga qarab oshirilishi mumkin). Auto Update servisining uzluksiz ishlashi uchun katalog doimiy foydalanish imkoniyatiga ega bo'lsin. Fayllar xavfsizlik siyosatiga muvofiq antivirus tomonidan bloklanmasligi ta'minlansin. URL manzil STYX Token Manager tomonidan foydalanish uchun taqdim etilsin.

3.1 Styx Archive Module — Arxivlash moduli

Modul tizim ma'lumotlarini uzoq muddat saqlash va arxivlashni ta'minlaydi:

- Sertifikatlar, kalitlar va operatsiyalar jurnallarini jadval bo'yicha avtomatik arxivlash.
- Ruxsatsiz kirishdan himoya qilish uchun arxiv ma'lumotlarini shifrlash.
- Zarurat tug'ilganda ma'lumotlarni arxivdan tiklash.
- Muddat va ma'lumot turi bo'yicha sozlanadigan saqlash siyosati (retention policy).

3.2 Universal StyxClient Driver — Universal mijoz drayveri

Drayver foydalanuvchi tomonida token va sertifikatlar bilan ishlashni ta'minlaydi:

- Operatsion tizimlarni qo'llab-quvvatlash: Windows 7, 8, 8.1, 10, 11 (32/64-bit) va macOS.
- ERI kalitlarini saqlash uchun USB-tokenlar va smart-kartalar bilan ishlash.
- Yopiq kalit (PKCS#12) va sertifikatni tokenga yozish.
- Web-interfeys orqali ishlash uchun Chrome, Firefox, Edge brauzerlari bilan moslashuvchanlik.
- Token ulanganda uni avtomatik aniqlash va ishga tushirish.

3.3 Styx Metin Mobile SDK — Mobil SDK

SDK kriptografik funksiyalarni mobil ilovalarga integratsiya qilish uchun mo'ljallangan:

- Android (5.0+) va iOS (12+) platformalarini qo'llab-quvvatlash.
- ERI kalitlarini mobil qurilmada generatsiya qilish va saqlash.
- Hujjatlar va ma'lumotlarni bevosita mobil qurilmadan imzolash.
- Imzolari verifikatsiya qilish uchun Styx AS serveri bilan o'zaro aloqa.
- Bankning uchinchi tomon mobil ilovalariga integratsiya uchun REST API taqdim etish.

3.4 STYX Cluster Module Active/Passive — Klasterlash moduli

Modul tizimning uzilishlarga chidamliligi va yuqori mavjudligini ta'minlaydi:

- Active/Passive sxemasi: asosiy tugun (Active) so'rovlarni qayta ishlaydi, zaxira tugun (Passive) o'tishga tayyor turadi.
- Asosiy tugun ishdan chiqqanda zaxira tugunga avtomatik o'tish (failover) — 30 soniyadan ko'p bo'lmagan vaqtda.
- Tugunlar o'rtasidagi holatni real vaqt rejimida sinxronlash.
- Tugunlar holatini monitoring qilish va o'tish vaqtida administratorni xabardor qilish.
- Xizmatni to'xtatmasdan rejali o'tish imkoniyati (graceful switchover).

3.5 SQB Business orqali sertifikatsiya — METIN moduli

Yangi komponent raqamli sertifikatni bevosita SQB Business mobil ilovasi orqali berishni ta'minlaydi:

- SERTIFIKAT berilayotganda mijoz 5 xonali parol kiritadi (12345–55555 oralig'idagi qiymatlar istisno qilinadi).
- Mijoz shaxsini tasdiqlash uchun OTP-kod kiritadi, so'ngra mustaqil ravishda parol o'rnatadi va sertifikatni oladi.
- Operatsiya ro'yxatga olingan ERI kalitidan foydalangan holda «METIN» majmuasi doirasida bajariladi.

3.6 ERI kalitlari hisobi — ombor hisobi

Modul bank tomonidan sotib olingan ERI kalitlarining to'liq hisobini, ulardan foydalanishni nazorat qilishni va foydalanuvchilar kirishini chegaralashni ta'minlaydi:

- Yangi sotib olingan ERI kalitlarini qabul qilish va ro'yxatga olish: donalab yoki yig'ma fayl orqali yuklash.
- Kalitlarning umumiy miqdorini bank bo'yicha umuman va filiallar kesimida ko'rsatish.
- Har bir kalit holatini ko'rsatish: «foydalanilgan / foydalanilmagan».
- Kalitlarni bank filiallari bo'yicha taqsimlash va qayta taqsimlash.
- Foydalanuvchilar so'rov yuborishi va sertifikatlarni faqat ro'yxatga olingan ERI kalitlariga yozishi mumkin.
- Tizim ro'yxatga olinmagan kalitlarga so'rov yuborishni bloklaydi va foydalanuvchiga ogohlantirish beradi.
- Ilgari sotib olingan (eski) ERI kalitlarini hisob va nazorat tizimiga kiritish: avval foydalanilgan kalitlarni «foydalanilgan» holati bilan avtomatik tarzda kirim qilish va ularni hisobga olingan sifatida ma'lumotlar bazasida qayd etish imkoniyati.

3.7 Yangi modullarga qo'yiladigan umumiy texnik talablar

Quyidagi umumiy texnik talablar yangi ishlab chiqiladigan barcha modullarga (ERI ombor hisobi, Dashboard, Hisobotlar, Client migratsiyasi, Token blokdan chiqarish, Telefon raqami sinxronizatsiyasi) tegishlidir:

- Veb-interfeys: responsive dizayn, SQB Business UI/UX konsepsiyasiga muvofiqlik.
- Ma'lumotlar bazasi tuzilishi: yangi jadvallar sxemasi va mavjud KMS ma'lumotlar bazasi bilan bog'liqligi (foreign key) hujjatlashtirilishi lozim.
- API: har bir modul uchun REST API endpointlari, so'rov/javob formatlari (JSON Schema) va autentifikatsiya mexanizmi hujjatlashtirilishi lozim.
- Huquqlar (roles/permissions): rol darajasidagi kirish huquqlari (administrator, limited administrator, user, operator) aniq belgilanishi lozim.
- Jurnallar (logging): har bir modulda bajarilgan operatsiyalar audit jurnaliga yozilishi va eksport qilish imkoniyati bo'lishi lozim.

4. FUNKSIONAL TALABLAR

4.1 Styx KMS — Kalitlarni boshqarish tizimi

ATB «O‘zsanoatqurilishbank» uchun yangilangan KMS tizimi quyidagi funksional imkoniyatlarni ta’minlashi lozim:

ERI kalitlarining ombor hisobi:

- Yangi sotib olingan ERI kalitlari hisobini bank bo‘yicha umumiy miqdorni ko‘rsatgan holda yuritish.
- Bosh ofis xodimlari tomonidan kalitlarni kirim qilish imkoniyati — donalab yoki yig‘ma fayl orqali yuklash.
- Kalitlarni bank filiallari bo‘yicha taqsimlash va qayta taqsimlash.
- KMS tizimida ro‘yxatga olingan ERI kalitlari bilan operatsiyalarni nazorat qilish.
- Har bir kalit holatini ko‘rsatish: foydalanilgan / foydalanilmagan.

Hisobotlar moduli:

- Asosiy va arxiv ma’lumotlar bazasidan namuna olgan holda hisobotlarni shakllantirish.
- Hisobotni shakllantirish uchun davr (sanalar) va filial nomini qo‘lda tanlash.
- Hisobotlar quyidagi ko‘rsatkichlarni o‘z ichiga olishi lozim:
 - ☞ berilgan sertifikatlar soni;
 - ☞ amal qilish muddati 1 oydan kam qolgan sertifikatlar soni;
 - ☞ amal qilish muddati tugagan sertifikatlar soni;
 - ☞ bekor qilingan sertifikatlar soni;
 - ☞ amaldagi sertifikatlar soni;
 - ☞ berilgan sertifikatlarning umumiy soni;
 - ☞ mobil banking uchun berilgan sertifikatlar soni;
 - ☞ boshqa toifalar bo‘yicha sertifikatlar.

Boshqaruv paneli (Dashboard):

- Bosh ofis xodimlari uchun — filiallar bo‘yicha ma’lumotlarni tanlash va ko‘rish imkoniyatiga ega kengaytirilgan statistika.
- Filial xodimlari (USER) uchun — faqat o‘z filiali bo‘yicha statistikani ko‘rish: berilgan, muddati tugagan, bekor qilingan, amaldagi sertifikatlar, mobil bank va IABS uchun sertifikatlar.

KMS tizimida mijoz telefon raqamini o‘zgartirish

- Filial xodimlari mijozning mobil telefon raqamini o‘zgartirganda, KMS tizimi va ABS (CROBS) bank tizimi o‘rtasida integratsiyani (alohida metod) amalga oshirish lozim. Bu integratsiya boshqa ma’lumotlarga o‘zgartirish kiritmasdan faqat mijoz telefon raqamini sinxron yangilashni ta’minlashi kerak.

KMS tizimida amalga oshirishi lozim bo‘lgan ishlar

- KMS dasturiy majmuasida sertifikatlarni bekor qilish mexanizmini barcha nazarda tutilgan bekor qilish sabablarini to‘g‘ri qayta ishlagan holda to‘liq amalga oshirish va ishlashini ta’minlash: «Sertifikat amal qilish muddati tugagan», «Token yo‘qolgan», «Token ishlamayapti», «Token bloklangan», «Direktor almashishi», «Kompaniya hisobni yopmoqda».
- KMS tizimida ERI kalitlari holati (bloklangan/boklanmagan) hisobini tegishli DBO xizmatlari bo‘yicha amalga oshirish, shuningdek STYX Client versiyalarini nazorat qilish mexanizmini kritik versiyalar uchun majburiy yangilash imkoniyati bilan amalga oshirish.
- Mijozlarni bank filiallari o‘rtasida ko‘chirish modulini amalga oshirish. Modul mijozni bank ichida bir filialdan boshqasiga o‘tkazish imkoniyatini ta’minlashi lozim. Ko‘chirish jarayoni mijoz ko‘chirilayotgan filial xodimi tomonidan boshlanishi va bajarilishi kerak.
- Mijozlarni bank filiallari o‘rtasida ko‘chirish modulini amalga oshirish — mijozni bank ichida bir filialdan boshqasiga o‘tkazadi. Ko‘chirish jarayoni jo‘natuvchi filial xodimi tomonidan boshlanishi va faqat qabul qiluvchi filial xodimi tasdiqlaganidan so‘ng yakunlanishi lozim, shundan keyingina ko‘chirish muvaffaqiyatli bajarilgan hisoblanadi.

- Eslatma: yuqoridagi ikkita band bir xil funksionallikni (mijozlarni filiallar o'rtasida ko'chirish) tavsiflaydi va bitta bandga birlashtirilishi tavsiya etiladi — qabul qiluvchi filial xodimi tasdiqlashini talab qiluvchi tartib asosiy variant sifatida qoldirilsin.
- Qo'shimcha ravishda, bitta mijozni ikki KMS foydalanuvchisi tomonidan rollarni chegaralagan holda bir vaqtda xizmat ko'rsatish imkoniyatini ta'minlash: asosiy foydalanuvchi va qo'shimcha foydalanuvchi.
- Sertifikatni uzaytirish jarayonida foydalanilayotgan token (ERI kalit tashuvchisi) yo'qolgan tokenlar reyestrda mavjudligini tekshirishni amalga oshirish lozim. Agar tekshiruv natijasida token yo'qolgan deb qayd etilgan bo'lsa, tizim uni keyingi foydalanishni taqiqlashi va foydalanuvchiga sertifikat berish (uzaytirish) uchun yangi token ro'yxatdan o'tkazishni taklif qilishi kerak.
- Sertifikat berish bo'yicha arizasi bekor qilingan mijoz ma'lumotlarini o'zgartirishda yuzaga keladigan xatoni tuzatish.
- «Hisobotlar» bo'limiga Markaziy bankka shakllantirish va keyinchalik yuborish uchun yangi hisobot shablonini qo'shish.
- Sertifikatni uzaytirishga yuborilgan ariza faylining ko'rinmaslik muammosini tuzatish.
- KMS tizimida ePass2003 tokeni ro'yxatdan o'tkazilayotganda uning administrativ PIN-kodini (Admin PIN) avtomatik almashtirish mexanizmini amalga oshirish, so'ngra ushbu PIN-kodni KMS ma'lumotlar bazasida himoyalangan ko'rinishda saqlash.
- Noto'g'ri foydalanuvchi PIN-kodini ketma-ket uch marta kiritish natijasida bloklangan tokenni blokdan chiqarish imkoniyatini nazarda tutish.
- Blokdan chiqarish jarayoni vakolatli bank xodimi tomonidan mijoz identifikatsiyasidan so'ng saqlangan administrativ token PIN-kodidan foydalangan holda KMS tizimi orqali bajarilishi lozim. Admin PINni almashtirish va tokenni blokdan chiqarish bo'yicha barcha operatsiyalar tizim audit jurnalida qayd etilishi kerak.
- Dasturiy ta'minot tokenni noto'g'ri PIN-kodni ketma-ket uch marta kiritishdan so'ng bloklangan holatda mijozning o'zi tomonidan blokdan chiqarish mexanizmini amalga oshirishi lozim. Blokdan chiqarish sertifikat egasining shaxsini tasdiqlovchi bir martalik parol (OTP) ko'rinishidagi qo'shimcha autentifikatsiya omilidan foydalangan holda bajarilishi kerak.
- Dasturiy ta'minot mijozga sertifikatni SQB Business mobil ilovasi orqali olish jarayonida sertifikat PIN-kodini o'rnatish imkoniyatini ta'minlashi lozim. PIN-kodni o'rnatishdan oldin mijoz bir martalik parol (OTP) kiritish orqali tasdiqlash jarayonidan o'tishi kerak. PIN-kod 5 ta raqamdan iborat bo'lishi lozim. Oddiy va oldindan aytib bo'ladigan kombinatsiyalardan (masalan: 12345, 23456, 34567, 55555 va shunga o'xshash ketma-ketliklar yoki bir xil raqamlardan) foydalanish taqiqlanishi kerak. Sertifikatni berish va olish faqat OTP-kod muvaffaqiyatli tasdiqlangach va mijoz xavfsizlik talablariga mos PIN-kodni o'rnatgach bajarilishi lozim.

STYX Token Manager Universal dasturiy ta'minotiga qo'yiladigan talablar

- STYX Token Manager Universal dasturiy mahsuloti Bankda foydalaniladigan barcha raqamli imzo (ERI) qurilmalari bilan ishlash uchun yagona platforma sifatida ishlab chiqilishi lozim.
- Dasturiy ta'minot dizayni Bank bilan majburiy kelishilishi lozim. Foydalanuvchi interfeysi SQB Business tizimida qo'llaniladigan dizayn konsepsiyasi va foydalanuvchi tajribasi (UI/UX) tamoyillariga mos kelishi kerak.
- Dasturiy ta'minot eng sodda, qulay va intuitiv tushunarli foydalanuvchi interfeysini ta'minlashi, asosiy operatsiyalarni minimal harakatlar bilan bajarishni nazarda tutishi lozim.
- STYX Token Manager Universal quyidagi operatsion tizimlarda to'liq va barqaror ishlashni ta'minlashi lozim:
 - ☞ Microsoft Windows;
 - ☞ macOS;
- Dasturiy ta'minot ko'rsatilgan operatsion tizimlarning dolzarb yangilanishlari bilan mos bo'lishi va foydalanuvchi tomonidan qo'shimcha sozlashsiz ishlashni ta'minlashi lozim.
- Dasturiy majmuaning barcha zarur komponentlari yagona o'rnatish paketi tarkibida yetkazib berilishi lozim.
- Universal o'rnatuvchi (Universal Installer) quyidagi komponentlarning mavjudligini avtomatik aniqlashi va zarurat bo'lganda o'rnatishi lozim:
 - ☞ STYX Token Manager;

☞ STYXCNG;

☞ Universal StyxCClient;

☞ ePass drayveri;

☞ dasturiy ta'minotning to'g'ri ishlashini ta'minlovchi barcha zarur kriptografik kutubxonalar, modullar va komponentlar.

- Dasturiy ta'minot ishlab chiquvchining amaldagi raqamli imzosi (Code Signing Certificate) bilan imzolanishi lozim, bu Microsoft Defender hamda boshqa korporativ va uchinchi tomon antivirus himoya vositalari tomonidan to'g'ri tanib olinishini va bloklanmasligini ta'minlaydi.
- Yechim Bankning korporativ axborot xavfsizligi talablariga mos kelishi va axborotni himoya qilishning zamonaviy kriptografik mexanizmlaridan foydalanishi lozim.
- Elektron imzo operatsiyasini bajarish jarayonida tizim imzolash operatsiyasi bevosita sertifikat egasi tomonidan amalga oshirilayotganini tasdiqlovchi qo'shimcha autentifikatsiya imkoniyatini ta'minlashi lozim.
- Tizim ulangan qurilmaning quyidagi parametrlarini avtomatik aniqlashi va foydalanuvchiga ko'rsatishi lozim:
 - ☞ token turi;
 - ☞ token modeli;
 - ☞ seriya raqami;
 - ☞ o'rnatilgan dasturiy ta'minot versiyasi (Firmware).
- Dasturiy ta'minot token, sertifikatlar, drayverlar va operatsion tizim holatini avtomatik tekshiruvchi, shuningdek ishlashga ta'sir qiluvchi muammolarni aniqlovchi o'rnatilgan diagnostika modulini o'z ichiga olishi lozim.
- Xatolar yoki noto'g'ri ishlash yuzaga kelganda dasturiy ta'minot foydalanuvchiga tushunarli xato xabarlarini, ularni bartaraf etish bo'yicha tavsiyalar va tegishli ogohlantirishlarni ko'rsatishi lozim.
- Bajarilgan barcha operatsiyalar audit jurnalida qayd etilishi va texnik qo'llab-quvvatlash, tahlil va hodisalarni tekshirish maqsadida keyinchalik eksport qilish imkoniyati bilan ta'minlanishi lozim.
- Yechim arxitekturasini masshtablanadigan va kengaytiriladigan bo'lishi, dasturiy ta'minotni jiddiy qayta ishlamasdan yangi token modellari, qo'shimcha autentifikatsiya usullari va Bank axborot tizimlari bilan keyingi integratsiya imkoniyatini ta'minlashi lozim.
- Tizim qo'llab-quvvatlanadigan token versiyalarini markazlashgan nazorat va boshqarishni ta'minlashi lozim. Zarurat tug'ilganda elektron imzo operatsiyalarini bajarishda ayrim token versiyalaridan foydalanishni cheklash yoki o'chirish imkoniyati nazarda tutilishi kerak.

«Tekmetes» MBX tizimini bankning ro'yxatga olish markazi bilan integratsiyalash

- «Tekmetes» tashkilotining masofaviy bank xizmati (MBX) tizimini bankning amaldagi ro'yxatga olish markazi bilan integratsiyalashni amalga oshirish. Integratsiyani amalga oshirish doirasida ro'yxatga olish markazi dasturiy majmuasining qo'shimcha funksionalini ishlab chiqishni, shuningdek integratsiyalanadigan komponentlar o'rtasida to'g'ri o'zaro aloqani ta'minlash uchun zarur sozlashlar va tizimni moslashtirishni bajarishni ta'minlash.
- Integratsiya endpointlari (URL manzillari) aniq ko'rsatilishi lozim.
- Autentifikatsiya mexanizmi (API key, OAuth2, mTLS va h.k.) belgilanishi lozim.
- So'rov va javoblar JSON formatida, aniq sxema (JSON Schema) asosida amalga oshirilishi lozim.
- Barcha ulanishlar TLS 1.2 yoki undan yuqori versiya orqali shifrlanishi lozim.
- Timeout va retry (qayta urinish) siyosati belgilanishi lozim (masalan: timeout — 30 soniya, 3 marta qayta urinish).
- Integratsiya muvaffaqiyatsiz yakunlangan holatlar uchun rollback mexanizmi ko'zda tutilishi lozim.

Jurnalga yozish va xabarnomalar:

- KMS tizimida filial xodimlarining barcha harakatlarini to'liq jurnalga yozish (logging).
- Foydalanuvchi (USER) uchun sertifikat amal qilish muddati tugashidan 30, 15 va 7 kun oldin ogohlantiruvchi oynani avtomatik ko'rsatish.

4.2 Universal StyxCClient Driver — Universal mijoz drayveri

Yangilangan mijoz drayveri quyidagilarni ta'minlashi lozim:

- ePass2003 va BST qurilmalarini qo'llab-quvvatlash.
- Operatsion tizimlar bilan moslashuvchanlik: Windows 7, Windows 8, Windows 10, Windows 11 (32/64-bit), Windows Server 19, Windows Server 22, Windows Server 25.
- Funktsionallikning operatsion tizim yangilanishlaridan mustaqilligi.
- Barcha zarur komponentlarni (STYXCNG, StyxClient, ePass drayveri) yagona o'rnatish fayli (minINSTALL) orqali ish stansiyasiga avtomatik o'rnatish.
- O'rnatish paketining operatsion tizimdan maksimal mustaqilligi.

4.3 Styx AS — Autentifikatsiya xizmati

Yangilangan autentifikatsiya xizmati quyidagilarni ta'minlashi lozim:

- Amal qilish muddati tugagan kalitlar bo'yicha barcha operatsiyalarni (autentifikatsiya, imzolash va boshqalar) bajarishni taqiqlash.
- AS Server WEB UI veb-interfeysi orqali muddati tugagan sertifikatlar amalini sanani ko'rsatgan holda majburiy to'xtatish imkoniyati.
- Muddati tugagan sertifikatlarni avtomatik darhol bloklash va belgilangan jadvalga muvofiq o'z vaqtida uzaytirish uchun filiallarga so'rovlar yuborish.

4.4 STYX Cluster Module — Zaxira sertifikatli markazi (Active/Passive)

Klasterlash moduli quyidagilarni ta'minlashi lozim:

- Active/Passive klaster arxitekturasi asosida sertifikatli xizmatlarining uzluksiz ishlashi.
- Asosiy tugun (Active) barcha operatsiyalarni bajaradi: sertifikatlarni berish, tekshirish, autentifikatsiya.
- Zaxira tugun (Passive) sinxron kutish rejimida bo'ladi va darhol o'tishga tayyor turadi.
- Asosiy tugun ishdan chiqqanda zaxira tugunga avtomatik o'tish (failover) — administrator aralashuvisiz.
- Tugunlar o'rtasida ma'lumotlarni real vaqt rejimida yoki belgilangan interval bilan sinxronlash.
- Xizmatlarning yuqori mavjudligi (High Availability), uzilishlarga chidamliligi va barqarorligi.

4.5 STYX Archive — Sertifikatlarni arxivlash moduli

Arxivlash moduli quyidagilarni ta'minlashi lozim:

- Muddati tugagan va/yoki o'chirilgan sertifikatlarni arxiv omboriga ko'chirgan holda avtomatik arxivlash.
- Bekor qilingan, muddati tugagan va yaroqsiz sertifikatlarni uzoq muddat saqlash va arxivlashni ta'minlash.
- Sertifikatlar va arxiv fayllarini chop etish hamda yozish operatsiyalarini hisobga olish va nazorat qilish.

4.6 O'zR Markaziy banki Yagona reyestri bilan integratsiya

Tizim O'zR Markaziy banki Yagona sertifikatlar reyestri bilan integratsiyani ta'minlashi lozim:

- Ma'lumotlarni real vaqt rejimida REST API protokoli orqali uzatish.
- Hujjatni imzolash paytida ERIning haqiqiylikini va sertifikatning amaldaligini tekshirish.
- ERI imzolangan serverlari ATB «O'zsanoatqurilishbank» ga tegishlilikini tasdiqlash.
- Reyestr bilan ulanish xatolarini qayta ishlash va administratorni xabardor qilish.

5. XAVFSIZLIK TALABLARI

- Komponentlararo barcha ulanishlar (KMS ↔ CA ↔ AS) TLS 1.2 yoki undan yuqori protokol bo'yicha shifrlanadi.
- Yopiq kalitlar faqat shifrlangan ko'rinishda (AES-256) saqlanadi.
- Administrativ interfeyslarga kirish — faqat himoyalangan HTTPS kanali orqali.
- Rollar bo'yicha kirishni chegaralash (RBAC): tizim administratori, mintaqaviy administrator, auditor.
- Barcha foydalanuvchi harakatlari va tizim hodisalarining o'zgarmas audit jurnalini yuritish.

- 5 marta muvaffaqiyatsiz kirish urinishidan so'ng hisob yozuvini avtomatik bloklash.
- Dasturiy ta'minot OWASP Top 10 talablariga muvofiq ishlab chiqilgan bo'lishi lozim.
- Ishlab chiqish jarayonida xavfsiz kodlashtirish (Secure Coding) standartlariga rioya qilinishi lozim.
- Ishga tushirishdan oldin va davriy ravishda penetratsion test (Penetration Test) o'tkazilishi lozim.
- Tizim mustaqil audit tekshiruvidan o'tkazilishi mumkinligi ta'minlanishi lozim.
- Bank SIEM tizimi bilan integratsiya (log yuborish) imkoniyati ko'zda tutilishi lozim.
- Yechim korporativ antivirus vositalari bilan to'liq moslashuvchan bo'lishi va ular tomonidan bloklanmasligi lozim.

6. AMALGA OSHIRISH BOSQICHLARI

№	Bosqich	Ishlar mazmuni	Muddat
1	Infratuzilmani tayyorlash	Amaldagi STYX tizimi infratuzilmasini tahlil qilish.	1 kun
2	STYX komponentlarini yangilash	STYX (KMS, CA, AS) komponentlarini ATB «O'zsanoatqurilishbank» amaldagi serverlarida so'nggi versiyaga yangilash va qayta o'rnatish; komponentlarni o'rnatish, bazaviy konfiguratsiya.	3 kun
3	Qo'shimcha modullarni o'rnatish	Archive, StyxClient Driver, Mobile SDK, Cluster Active/Passive	2 kun
4	MB Yagona reyestri bilan integratsiya	REST API integratsiyasini sozlash, ma'lumot almashinuvini sinash	1 kun
5	Sinov va qabul qilish	Funksional va yuklama sinovi, kamchiliklarni bartaraf etish	1 hafta
6	Administratorlarni o'qitish	5 kishigacha o'qitish, hujjatlarni topshirish	2 kun
Barcha modullarni integratsiya muddati 1 haftadan oshmasligi lozim va to'liq bitkazilgan hold bo'lishi kerak (под ключ)			

7. ISHLARNI QABUL QILISH TARTIBI

- Qabul qilish ikkala tomon imzolagan Qabul-topshirish dalolatnomasi asosida amalga oshiriladi.
- Buyurtmachi ishlarning yakunlanishi to'g'risida xabardor qilingan paytdan boshlab 10 ish kuni ichida tekshiruv o'tkazishga haqli.
- Tekshiruv natijalari bo'yicha kamchiliklar ro'yxati bilan bayonnoma tuziladi (mavjud bo'lsa).
- Ijrochi kamchiliklarni kelishilgan muddatlarda bartaraf etadi, shundan so'ng ishlar qabul qilingan hisoblanadi.
- O'lchanadigan (measurable) qabul mezonlari: texnik topshiriqda nazarda tutilgan har bir yangi modul va tashqi axborot tizimi bilan integratsiya bo'yicha funksional sinovlar muvaffaqiyatli yakunlangan bo'lishi lozim. Har bir ishlab chiqilgan modul va integratsiya uchun kamida 5-10 ta test elektron sertifikatini muvaffaqiyatli yaratilishi, yozilishi, tekshirilishi va amaliy ishlashi tasdiqlanishi kerak. Jumladan, Styx Metin Mobile SDK bo'yicha Android va iOS platformalarida elektron raqamli imzo yaratish va tekshirish funksiyalari muvaffaqiyatli sinovdan o'tkazilgan bo'lishi, «Tekmetes» MBX, MB Yagona reyestri hamda texnik topshiriqda ko'rsatilgan boshqa tashqi axborot tizimlari bilan integratsiyalar bo'yicha test ssenariylari muvaffaqiyatli bajarilgan bo'lishi lozim. Barcha REST API xizmatlari bo'yicha funksional test hisobotlari, integratsiya natijalari va qabul qilish sinovlari bayonnomalari Buyurtmachiga taqdim etilishi shart.
- Kafolatli qo'llab-quvvatlash — Dalolatnoma imzolangan sanadan boshlab 12 oy.
- Kafolat muddati davomida quyidagilar ta'minlanishi lozim: aniqlangan xatolarni bepul tuzatish (bug fix); kritik xavfsizlik zaifliklari bo'yicha xavfsizlik yamoqlarini (security patch) o'z vaqtida taqdim etish; mahsulotning yangi versiyalariga bepul yoki kelishilgan shartlarda o'tish (version update); tezkor murojaat uchun ishonch telefoni/hotline liniyasi; muammoni bartaraf etishda kechikish yuzaga kelganda ichki eskalatsiya tartibi (escalation matrix) belgilanishi.

8. TEXNIK QO‘LLAB-QUVVATLASH SHARTLARI (SLA)

8.1 Texnik qo‘llab-quvvatlash tarkibi

Texnik qo‘llab-quvvatlash deganda quyidagilar tushuniladi:

- Dasturiy ta‘minotni o‘rnatish, sozlash va foydalanish bo‘yicha maslahatlar.
- Tizimdan foydalanish jarayonida aniqlangan xato va nosozliklarni bartaraf etish.
- Yangilanishlar va patchlarni taqdim etish (Ijrochi tomonidan chiqarilgan taqdirda).

8.2 Xizmat ko‘rsatish darajalari (Service Level Agreement)

Yuqorida ko‘rsatilgan nosozliklarni bartaraf etish muddatlari tavsiya etilgan qiymatlar hisoblanadi. Amaliyotda, ayniqsa **Severity 1** toifasidagi murakkab nosozliklar bo‘yicha muammoni to‘liq bartaraf etish muddati xatoning murakkabligi, ishlab chiqaruvchi ishtiroki, tashqi tizimlarga bog‘liqlik hamda ekspluatatsiya muhitining xususiyatlariga qarab farq qilishi mumkin. Shu munosabat bilan **Severity 1** uchun quyidagi SLA ko‘rsatkichlarini qo‘llash tavsiya etiladi: **Response Time — 1 soat, Workaround — 4 soatgacha, Fix — 24–72 soat**. Aniq bartaraf etish muddati nosozlikning murakkabligi va bajarilishi lozim bo‘lgan ishlar hajmidan kelib chiqib, Buyurtmachi va Ijrochi tomonidan alohida kelishiladi hamda SLA shartlarida belgilanadi.

Murojaat turi	Ustuvorlik	Reaksiya vaqti	Bartaraf etish vaqti
Kritik xato (Severity 1) — tizim ishini to‘liq bloklovchi nosozlik	KRITIK	1 soatdan ko‘p emas	2 soatdan ko‘p emas
Jiddiy xato (Severity 2) — to‘liq to‘xtatmasdan asosiy funksiyalarni cheklash	YUQORI	2 soatdan ko‘p emas	1 ish kunidan ko‘p emas
Ahamiyatsiz xato (Severity 3) — asosiy funksiyalarga ta‘sir qilmaydigan nosozlik	O‘RTA	1 ish kuni	5 ish kunidan ko‘p emas
Maslahat so‘rovi	PAST	2 ish kuni	2 ish kuni

8.3 Qo‘llab-quvvatlash xizmatining ish tartibi

Texnik qo‘llab-quvvatlash xizmati quyidagi tartibda ishlaydi:

- Kunlar: dushanba – juma, bayram va dam olish kunlaridan tashqari.
- Soatlar: Toshkent vaqti bilan 09:00 dan 18:00 gacha (UTC+5).

8.4 Aloqa kanallari

Qo‘llab-quvvatlash xizmatiga murojaatlar quyidagi kanallar orqali qabul qilinadi:

- Ishonch telefoni — Ijrochi rekvizitlarida ko‘rsatilgan.
- Elektron pochta — Ijrochi rekvizitlarida ko‘rsatilgan.

9. ISHLASH KO‘RSATKICHLARI VA YUKLAMA TALABLARI (PERFORMANCE)

- Tizim Buyurtmachining ishlab chiqarish muhitidagi amaldagi va istiqboldagi yuklamalarni qo‘llab-quvvatlashi, bir vaqtning o‘zida ishlayotgan foydalanuvchilarga barqaror va uzluksiz xizmat ko‘rsatishi hamda foydalanuvchilar soni ortgan taqdirda ham tizimning ishlash unumdorligi pasaymasligi lozim.
- Sertifikatlarni chiqarish jarayoni — foydalanuvchi tomonidan yuborilgan sertifikat yaratish so‘rovi administrator tomonidan tasdiqlangandan so‘ng elektron sertifikat muvaffaqiyatli yaratilishi, ro‘yxatdan o‘tkazilishi va "Active" holatiga o‘tkazilishi lozim. Sertifikatni chiqarish jarayoni xatosiz bajarilishi hamda foydalanuvchiga yakuniy natija haqida tegishli xabarnoma taqdim etilishi kerak.
- REST API xizmatlari Buyurtmachining amaldagi va istiqboldagi yuklamalarini barqaror qayta ishlash imkoniyatini ta‘minlashi, bir vaqtning o‘zida kelib tushadigan so‘rovlarni xatosiz va uzluksiz qayta ishlashi hamda yuklama ortgan taqdirda ham tizimning ishlash unumdorligi pasaymasligi lozim.

- OSCP xizmati sertifikat holatini tekshirish bo'yicha kelib tushadigan so'rovlarni uzluksiz, barqaror va xatosiz qayta ishlashi hamda Buyurtmachining ishlab chiqarish muhitidagi yuklamalar ostida o'z vaqtida javob qaytarishini ta'minlashi lozim. Xizmatning ishlash unumdorligi Buyurtmachining amaldagi va istiqboldagi ekspluatatsiya talablariga mos bo'lishi kerak.
- Yuklama sinovlari (load testing) natijalari qabul-topshirish bosqichida taqdim etilishi lozim.

10. APPARAT TA'MINOTI TALABLARI (HARDWARE)

STYX PKI dasturiy majmuasini joriy etish uchun bank tomonidan mavjud server infratuzilmasidan zarur resurslar ajratiladi.

STYX PKI dasturiy majmuasini joriy etish uchun mavjud server infratuzilmasi dasturiy komponentlarning barqaror va uzluksiz ishlashini ta'minlashi lozim. Har bir server alohida virtual mashinada (VM) joylashtirilishi lozim.

Minimal apparat resurslari quyidagicha bo'lishi lozim:

Komponent	CPU	RAM	Disk (SSD)
- STYX KMS Server	4-6 vCPU	4-8 GB	100-200 GB
- STYX CA Server	4-6 vCPU	4-8 GB	100-200 GB
- STYX AS Server	4-6 vCPU	4-8 GB	100-200 GB
- STYX Archive Module Server	4-6 vCPU	4-8 GB	100-200 GB

Yuqori mavjudlik (High Availability) va xizmatlarning uzluksiz ishlashini ta'minlash maqsadida STYX Cluster Module (Active/Passive) joriy etilishi lozim. Klaster yechimi uchun 3 ta qo'shimcha virtual mashina (VM) ajratilishi lozim:

- STYX KMS Passive Server — 4-6 vCPU, 4-8 GB RAM, 100-200 GB SSD;
- STYX CA Passive Server — 4-6 vCPU, 4-8 GB RAM, 100-200 GB SSD;
- STYX AS Passive Server — 4-6 vCPU, 4-8 GB RAM, 100-200 GB SSD.

Klaster **Active/Passive** rejimida ishlashi, ma'lumotlar replikasiyasini, avtomatik **Failover** mexanizmini hamda asosiy serverda nosozlik yuzaga kelganda xizmatlarning zaxira serverga avtomatik o'tishini ta'minlashi lozim. Serverlar o'rtasida sinxronizatsiya doimiy ravishda amalga oshirilishi, xizmatlarning uzilishi minimal darajada bo'lishi va ma'lumotlarning yo'qolishiga yo'l qo'yilmasligi kerak.

Yakuniy apparat resurslari Bankning amaldagi infratuzilmasi, foydalanuvchilar soni va ekspluatatsiya muhitidagi real yuklama ko'rsatkichlari asosida aniqlashtiriladi.

11. ZAXIRALASH VA HALOKATDAN KEYIN TIKLASH SIYOSATI (BACKUP / DR)

- To'liq zaxira nusxalash (Full Backup) va oraliq zaxira nusxalash (Incremental Backup) jadvali belgilanishi lozim.
- Ma'lumotlarni tiklash (Recovery) tartib-taomili hujjatlashtirilishi lozim.
- Ruxsat etilgan maksimal ma'lumot yo'qotish vaqti (RPO — Recovery Point Objective) va tiklash vaqti (RTO — Recovery Time Objective) ko'rsatkichlari belgilanishi lozim.
- Halokatdan keyin tiklash (Disaster Recovery) doirasida ikkinchi (zaxira) data-markaz mavjudligi yoki uni tashkil etish zarurati aniqlanishi va tegishli talablar belgilanishi lozim.

12. MIGRATSIYA REJASI

- Mavjud ma'lumotlarning (sertifikatlar, kalitlar, foydalanuvchi ma'lumotlari) yangi versiyaga qanday ko'chirilishi (migratsiya jarayoni) bosqichma-bosqich tavsiflanishi lozim.
- Muvaffaqiyatsiz migratsiya holatida oldingi holatga qaytish (rollback) tartibi belgilanishi lozim.
- Migratsiya davomidagi xizmat to'xtash vaqti (downtime) oldindan baholanishi va Buyurtmachi bilan kelishilishi lozim.
- Ishlab chiqarish muhitiga o'tishdan oldin test muhitida sinov migratsiyasi (test migration) o'tkazilishi lozim.
- Imkon qadar cheklangan miqdordagi filiallarda pilot ishga tushirish amalga oshirilishi va natijalari baholanganidan so'ng butun tizimga tarqatilishi tavsiya etiladi.

13. IJROCHIGA QO'YILADIGAN TALABLAR

Ijrochi quyidagi talablarga javob berishi lozim:

1. STYX dasturiy ta'minotini yetkazib berish, joriy etish, modernizatsiya qilish va texnik qo'llab-quvvatlash ishlarini amalga oshirish huquqini tasdiqlovchi, ishlab chiqaruvchi yoki huquq egasi tomonidan berilgan amaldagi avtorizatsiya xatiga (Authorization Letter) ega bo'lishi.
2. Loyihani amalga oshirish uchun mas'ul loyiha menejeri, shuningdek PKI (Public Key Infrastructure) infratuzilmasi, kriptografik himoya vositalari, axborot xavfsizligi va tizim integratsiyasi sohalarida zarur bilim va tajribaga ega malakali mutaxassislarni biriktirishi lozim. Ishtirokchi mazkur mutaxassislar haqidagi ma'lumotlarni (rezyume, sertifikatlar va boshqa tasdiqlovchi hujjatlar) taklif tarkibida taqdim etishi shart.
3. Tizim bo'yicha kafolat muddati davomida hamda Buyurtmachining ehtiyojiga ko'ra kafolat muddati tugaganidan keyin O'zbekiston Respublikasi hududida texnik qo'llab-quvvatlash xizmatlarini ko'rsatish imkoniyatiga ega bo'lishi lozim.
4. Bank-moliya sohasida PKI infratuzilmasi, elektron raqamli imzo (ERI) yoki axborot xavfsizligi tizimlarini joriy etish va qo'llab-quvvatlash bo'yicha kamida bitta muvaffaqiyatli amalga oshirilgan loyiha tajribasiga ega bo'lishi. Ushbu tajriba shartnoma, bajarilgan ishlar dalolatnomasi bilan tasdiqlanishi lozim.
5. Buyurtmachi mutaxassislari tizimni ekspluatatsiya qilish, ma'murlashtirish va texnik qo'llab-quvvatlash bo'yicha zarur bilimlarni berishni (Knowledge Transfer), shuningdek foydalanish qo'llanmalari, ma'muriy yo'riqnomalar va boshqa texnik hujjatlarni taqdim etishni ta'minlashi.
6. Tizimni joriy etish va sozlash ishlarini bajarish jarayonida Buyurtmachining axborot xavfsizligi siyosati, ichki normativ hujjatlari hamda O'zbekiston Respublikasining amaldagi normativ-huquqiy hujjatlari talablariga to'liq rioya qilishi.
7. Amal qilish muddati kamida 5 (besh) yil bo'lgan kriptografiya bo'yicha muvofiqlik sertifikatiga ega bo'lishi shart.
8. Axborotning kriptografik himoya vositalarni ishlab chiqish, ishlab chiqarish va realizatsiya qilish faoliyati uchun litsenziyaga ega bo'lishi lozim.
9. Loyihani amalga oshirish jarayonida Buyurtmachining mavjud ma'lumotlar bazasi saqlanishi va yo'qotilmasligi ta'minlanishi shart.

14. TO'LOV SHARTLARI

- Shartnoma qiymatining 30 foizi oldindan to'lov tariqasida amalga oshiriladi.
- Qolgan 70 foizi o'rnatish va sozlash ishlari to'liq yakunlangandan, yakuniy qabul qilish-topshirish dalolatnomasi ikki tomon tomonidan imzolanganidan hamda hisob-faktura taqdim etilgan sanadan boshlab 10 (o'n) kalendar kuni ichida to'lanadi.



kelishuvchilar: T.Rapiyev, A.Orifjonov, N.Umarov, A.Kenjaye

<https://hujjat.sqb.uz/?pin=pG39kB23&id=b5fe4a58-2946-41a9-b4be-6217182c4e92>