Тендерлік құжаттамаға
6-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы	"ҚазАвтоЖол" Ұлттық компаниясы" акционерлік қоғамы
Ұйымдастырушының атауы	"ҚазАвтоЖол" Ұлттық компаниясы" АҚ "Ақылы автомобиль жолдар дирекциясы" филиалы
Тендердің №	№ 17885924-1
Тендердің атауы	Бағдарламалық қамтамасыз ету тауарын электрондық сатылым
Лоттың №	№ 88200618-ОТ2
Лоттың атауы	Бағдарламалық қамтамасыз ету
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*	620129.000.000000
Тауардың атауы*	Бағдарламалық қамтамасыз ету
Өлшем бірлігі*	Дана
Саны (көлемі)*	1
Бірлік бағасы, қосылған құн салығын қоспағанда*	64655172.41
Қосылған құн салығын қоспағанда, сатып алуға бөлінген жалпы сома*	64655172.41
Жеткізу шарты (ИНКОТЕРМС 2010-ға сәйкес)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	с момента заключения договора в течение 30 календарных дней.
Аванстық төлем мөлшері*	0
Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	
Шығарылған жылы (Тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс)	2026
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауарлардың қажетті функционалдық, техникалық, сапалық, өнімділігі мен басқа да сипаттамаларының сипатталуы	ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК Биометриялық аутентификация жүйесі 1. Жалпы мәліметтер Биометриялық аутентификация жүйесі (бұдан әрі — Жүйе) физикалық және логикалық қол жеткізуді бақылау, есептік деректерді рұқсатсыз пайдалануды болдырмау және Тапсырыс берушінің ақпараттық жүйелерінде пайдаланушылардың іс-әрекеттерін дұрыс есепке алуды қамтамасыз ету мақсатында пайдаланушылардың жеке басын олардың бірегей физиологиялық сипаттамалары бойынша растауға арналған. 2. Функционалдық талаптар Жүйе Тапсырыс берушінің инфрақұрылымы шегінде биометриялық деректерді орналастыру және өңдеу мүмкіндігімен бағдарламалық қамтамасыз ету түрінде жеткізілуі тиіс. Жүйе пайдаланушыны қашықтан верификациялауды және кейінгі заңды маңызы бар іс-қимылдың толық циклін қамтамасыз етуі тиіс: тірілікті биометриялық тексеру (liveness), бет-әлпетті Тапсырыс берушінің базасымен салыстыру. Жүйе біртұтас платформа ретінде жеткізілуі керек, онда әр модуль үшін жеке интеграцияны дамытпай-ақ, бір реттелетін бизнес-процесте компоненттерді бөлек немесе дәйекті пайдалану мүмкіндігі болуы керек. Жүйе мынадай негізгі сценарийлерді қамтамасыз етуі тиіс: - пайдаланушының liveness-тексеруден өтуі, бет-әлпеттің ең жақсы кадрын, liveness-тексеруден өтудің балама видеосын, liveness-тексеруден өтудің түпнұсқа видеосын және нәтижені ала отырып; - клиенттің бет-әлпетін Тапсырыс берушінің дерекқорындағы эталондық бейнемен салыстыру; - қорытынды нәтижені Тапсырыс берушінің АЖ-не API, вебхук және/немесе кабинет арқылы беру. - Өнеркәсіптік контур шеңберіндегі барлық трафик пен дербес және биометриялық деректерді өңдеу Тапсырыс берушінің инфрақұрылымында және Қазақстан Республикасының аумағында жүзеге асырылуы тиіс. - Жүйеде нақты уақыт режиміндегі мониторинг және сервис тоқтаған немесе кез келген қателер туындаған кезде бапталған хабарламалар болуы тиіс. - Жүйеде орыс және ағылшын тілдерінде толық және өзекті құжаттама болуы тиіс. - Биометриялық верификациядан өту кезінде Жүйе сәтсіз әрекеттерді барынша азайту үшін пайдаланушыға нұсқаулар шығаруы тиіс. - Сәтсіз транзакцияларда/сессияларда және қайталама әрекеттерде логтарда қателердің себептері көрсетілуі тиіс. - Логтар жалпы транзакциялық сәйкестендіргішті қамтуы тиіс. Журналдау Жүйенің әрбір компонентінде жүргізілуі тиіс. - Жүйе ақпараттық және бірмәнді қате хабарламаларын қайтаруы тиіс. - Әрбір қате хабарламасы мыналарды қамтуы тиіс: a. туындау себебінің сипаттамасы; b. қате деңгейі (мысалы: validation / server / network); c. пайдаланушыға арналған ұсынымдар немесе одан әрі іс-қимылдар (қолданылатын болса). Шешім конфигурацияланатын және кеңейтілетін болуы тиіс. Тапсырыс беруші жеке сервистерді не бірыңғай сценарий шеңберіндегі кешенді процесті пайдалану мүмкіндігіне ие болуы тиіс. 2.1. Liveness биометриялық сәйкестендіру компоненті Жүйе пайдаланушының тірі қатысуын нақты уақыт режимінде тексеруді, бет-әлпеттің ең жақсы кадрын бөліп алуды, балама видео құруды, түпнұсқа видеоны сақтауды, шабуылдарды талдауды және нәтижені қайтаруды қамтамасыз етуі тиіс. Жүйе кадрдағы пайдаланушының бет-әлпетін анықтауы, позицияны, бұрылысты, жарықтандыруды, кадр сапасын, шамадан тыс жарықты, қараңғыланууды, бұлыңғырлануды, бірнеше бет-әлпеттің болуын және биометрия сапасына әсер ететін өзге факторларды бақылауы тиіс. Жүйеде түпкілікті клиент үшін іс-қимылдар/сигналдар санын реттеу функционалы болуы тиіс, мысалы: жақындау, алыстау, басты оңға/солға бұру. Жүйе пайдаланушыға түсінікті нұсқауларды шығаруы тиіс: бет-әлпетті сопақшаға орналастыру, жақындау/алыстау, басты бұру, жарықтандыруды жақсарту, қажет болғанда көзілдіріктің шешу, әрекетті қайталау. Жүйе liveness-тің белсенді және бәсең әдістерін қолдауы тиіс, бұл ретте нақты режим операция тәуекеліне, арнаға және Тапсырыс берушінің талаптарына қарай бапталуы тиіс. Жүйе мынадай әртүрлі шабуыл түрлерін анықтауы тиіс: - қағаздағы фотосурет, - экраннан түсірілген фото/видео, - бейнежазбалар, - маскалар, - 3D-маскалар, - аватарлар, - deepfake/face swap, - виртуалды камералар, - эмуляторлар, - видеоағынды ауыстыру, - күдікті іске қосу ортасы, - cloud phone/remote relay белгілері, - тиісті SDK/сигналдар болған кезде root/jailbreak немесе өзге тәуекел-индикаторлар. Жүйе кейінгі FaceMatch, есептік құжатты қалыптастыру және Тапсырыс берушінің АЖ-не беру үшін liveness процесінен бет-әлпеттің ең жақсы кадрын қайтаруы тиіс. - Livenesstен өту әрекеттерінің саны Тапсырыс беруші сервистің конфигурациясында баптауы тиіс. Жүйе интерфейс пен нұсқауларды кемінде орыс, қазақ және ағылшын тілдерінде локализациясын қолдауы тиіс. Жүйе таңдалған интеграция тәсіліне қарай мобильді браузерлерде, webview-де және desktop-браузерлерде дұрыс жұмыс істеуі тиіс. Штаттық жүктеме кезінде liveness нәтижесін серверлік өңдеудің орташа уақыты пайдаланушының іс-қимылдары мен сыртқы жүйелердің уақытын есепке алмағанда 5 секундтан аспауы тиіс. Жүйе барлық әрекеттерді, оның ішінде сәтті, сәтсіз әрекеттерді, қайталауларды, пайдаланушының бас тартуын және техникалық қателерді журналдауды қамтамасыз етуі тиіс. Жүйе liveness-тің бизнес-бас тартуларын, бейненің төмен сапасын, пайдаланушының бас тартуын, клиенттің техникалық қателерін, желілік қателерді және backend-сервистің қателерін нақты ажыратуы тиіс. Жүйе биометриялық верификациядан өту шеңберінде алынған және/немесе қалыптастырылған мынадай деректерді Тапсырыс берушінің серверлерінде беру және сақтау мүмкіндігін қамтамасыз етуі тиіс: - биометриядан өту видеосы; - пайдаланушы бет-әлпетінің ең жақсы кадры (best frame); - салыстыру үшін пайдаланылған эталондық фотосурет; - ұқсастық коэффициенті; - liveness-тексеру нәтижесі; - транзакция/сессия сәйкестендіргішті; - тексеруден өткен күні мен уақыты; - биометриялық верификация жүргізілген құрылғы туралы мәліметтер. Жүйе жұмысының сапасы жалпыға бірдей қабылданған салалық метрикалар пайдаланыла отырып бағаланады: - APCER - шабуылдарды/алаяқтық әсерлерді өткізіп жіберу көрсеткіші; - BPCER - адал пайдаланушыны қабылдамау көрсеткіші. Пайдаланушылық сценарийлер, кіріс деректерінің сапасы, түсіру жағдайлары, пайдаланылатын жабдық және бағдарламалық орта сақталған жағдайда Жүйе жұмысының нысаналы көрсеткіштері мыналарды құрауы тиіс: - APCER ≤ 0,5 %; - BPCER ≤ 8 %. 2.2. FaceMatch компоненті FaceMatch компоненті liveness-тен алынған пайдаланушы бейнесін бір немесе бірнеше көзден алынған эталондық бейнемен салыстыруды орындауы тиіс: Тапсырыс берушінің ішкі жүйесі, бұрын жүктелген бейне. Жүйе салыстыру пайызын, нәтижені, сондай-ақ туындаған жағдайда қателердің сипаттамасын қайтаруы тиіс. Жүйе бейнені Тапсырыс берушінің дерекқорындағы фотосуретпен салыстыруды қолдауы тиіс. Барлық салыстыру операциялары журналдануы тиіс. Биометриялық верификация сұрауларында операциялардың барлық түрлері үшін Жүйе ұқсастық шегін жеке кіріс параметрі ретінде қосу мүмкіндігін беруі тиіс. Бет-әлпетті тану жүйесі жалған қабылдау (FAR — 0,001%-дан аспайды) және жалған қабылдамау (FRR — 0,4%-дан аспайды) қателерін барынша азайту үшін танудың жоғары дәлдігін қамтамасыз етуі тиіс. Тану сезімталдығы мен анықтығының ең төмен шегі: 1 000 000 фотосуреттен тұратын іріктемеде TPR кемінде 99,6%, FPR 0,4%-дан аспайды. 2.3. Әкімшілендіру және мониторинг кабинеті Платформада сервистерді, пайдаланушыларды, рөлдерді, қолжетімділіктерді, API-кілттерді баптауға арналған әкімшінің web-кабинеті болуы тиіс. Кабинет қолжетімділік құқықтарын араживтеуді қолдауы тиіс: әкімші, тек қарауға арналған пайдаланушы, есептілік пайдаланушысы. Кабинет сәттілік саны, бас тарту себептері, қайталаулар және сервистердің жұмысы бойынша дашбордтар беруі тиіс. Кабинет есептерді келісілген форматтарда жүктеп алуды қолдауы тиіс: CSV/XLSX/JSON/PDF. Жүйе шартта өзгеше белгіленбесе, келісілген рөлдік модель шеңберінде әрбір есептік жазба үшін жеке ақы алмай, кабинетте Тапсырыс беруші қызметкерлерінің шектеусіз санын қолдауы тиіс. 3. Лицензиялауға қойылатын талаптар Жеткізуші лицензияның қолданылу мерзімі ішінде верификацияға транзакциялар саны шектеусіз бағдарламалық қамтамасыз етуді пайдалануға жылдық лицензия береді. 4. Үйлесімділікке, өнімділіктің масштабталуына қойылатын талаптар Платформа смартфондарда, планшеттерде, ДК-де және камерасы бар өзге құрылғыларда жұмыс істеуді қолдауы тиіс. Hosted Frontend камераға қол жеткізу талаптары сақталған жағдайда Chrome, Safari, Edge, Firefox өзекті нұсқаларын, iOS/Android мобильді браузерлерін және Тапсырыс беруші қосымшаларындағы webview-ді қолдауы тиіс. Платформа Тапсырыс берушінің архитектурасы мен қодын өзгертпей backend-сервистерді көлденең масштабтауды қолдауы тиіс. Платформа айына кемінде 1 000 000 транзакцияны өңдеуді, масштабтау мүмкіндігімен қолдауы тиіс. Жаппай пайдалану кезінде жүйе сыни backendоперациялардың деградациясынсыз минутына 1500-ден астам сұрау көлеміндегі бір мезгілдегі ең жоғары жүктемеге төзуі тиіс. Қалыпты жағдайларда liveness/FaceMatch серверлік өңдеу уақыты пайдаланушының іс-қимылдары мен сыртқы мемлекеттік жүйелердің уақытын есепке алмағанда әрбір компонент бойынша 10 секундқа дейін болуы тиіс. 5. Орналастыруға қойылатын талаптар Жүйе Тапсырыс берушінің инфрақұрылымында мынадай нұсқаларды пайдалана отырып орналастыруды қолдауы тиіс: Docker Compose — жүйені әзірлеу, тестілеу және шектеулі масштабтағы өзге орталарда орналастыру үшін. Орналастыру шешімнің қажетті компоненттерін контейнерлендірілген ортада іске қосуды қамтамасыз етуі тиіс. Kubernetes / OKD — өнеркәсіптік ортада орналастыру үшін. Орналастыру Helm-чарттарын немесе шешім қолдайтын өзге стандартты оркестрация тетігін пайдалана отырып, компоненттерді масштабтау және олардың конфигурациясын басқару мүмкіндігімен жүзеге асырылуы тиіс. 6. Қауіпсіздікке қойылатын талаптар Тапсырыс беруші периметрінің қауіпсіздігіне әсер етуі мүмкін кез келген өзгерістер тек Тапсырыс берушімен келісілгеннен кейін орындалуы тиіс. Жүйе мүмкін болған барлық жерде деректерді берудің қорғалған хаттамаларын пайдалануы тиіс. Қорғалған хаттамаларды пайдалану Confidential және Highly Confidential санаттарындағы деректерді, әсіресе клиенттердің дербес деректерін беру, сақтау және өңдеу кезінде міндетті болып табылады. Рұқсат етілген хаттамаларға мыналар кіреді, бірақ олармен шектелмейді: HTTPS, SSH, SNMPv3, TLS 1.2 және одан жоғары нұсқасы, IPSec, LDAPS. Жүйе есептік жазбалардың барлық параметрлерін өзгерту мүмкіндігін қамтамасыз етуі тиіс, оның ішінде: құпиясөздер, кодтық тіркестер, шифрлау кілттері, SNMP параметрлері, кез келген өзге өзгертілетін деректер. Өндіруші беретін барлық әдепкі есептік жазбаларды (guest, admin, root және т.б.), мұндайлар болған жағдайда, өзгерту немесе өшіру мүмкіндігі көзделуі тиіс. Жүйе пайдаланушылардың (әкімшілердің, операторлардың және т.б.) іс-қимылдарын толық журналдауды қамтамасыз етуі тиіс. Логтар мыналарды қамтуы тиіс: - оқиғалардың күні мен уақыты - қосылу көзінің IPмекенжайы - пайдаланушыны сәйкестендіру - іс-қимылдар (қарау, өзгерту, жою, командаларды орындау) - кіру әрекеттері (сәтті және сәтсіз) - журналдауды өшіру немесе тоқтату оқиғалары - қауіпсіздікке байланысты барлық оқиғалар Қосымша тетіктер, мысалы биометриялық тексеруді кэштеу немесе өзге тетіктер болған жағдайда, мұндай тетіктер Тапсырыс беруші үшін әдепкі бойынша өшірілуі және тек Тапсырыс берушімен келісу бойынша қосылуы тиіс. Жүйе барлық құпияларды, дербес және сыни деректерді тек HTTP POST-сұраудың денесінде беруді қамтамасыз етуі тиіс. Мұндай деректерді URL (query-параметрлер), тақырыптар немесе сұраудың өзге ашық бөліктері арқылы беруге жол берілмейді. 7. Кепілдік қызмет көрсетуге қойылатын талаптар Кепілдік мерзімі кемінде 12 айды құрауы тиіс. 8. Техникалық қолдауға қойылатын талаптар Жеткізуші Жүйені кемінде 12 ай мерзімге және кемінде 5x8 режимінде (жұмыс уақыты дүйсенбіден жұмаға дейінгі жұмыс күндері сағат 9:00-ден 18:00-ге дейін) техникалық қолдаумен қамтамасыз етуі тиіс. Мұндай стандартты қолдау Жүйені пайдалануға байланысты проблемаларды тегін шешуге және Жүйені тегін жаңартуға (БҚ және/немесе қозғалтқыштардың жаңа нұсқаларын не түзетулерді алуға) мүмкіндік беруі тиіс. Жүйені пайдалану кезінде туындайтын проблемаларды шешу үшін Жеткізуші Тапсырыс берушіден немесе оның өкілдерінен өтінімдер қабылдауға арналған электрондық сервис (веб-портал, арнайы email-мекенжай, мобильді қосымша және т.б.) ұсынуы тиіс, мұндай өтінімдер қолдау жүйесінде автоматты түрде тіркелуі тиіс. Мұндай сервис өтінімдердің құрылғанын растау, өтінімдер мәртебесінің өзгеруі және т.б. функционалына ие болуы тиіс. Мұндай сервиспен жұмыс істеу және жеткізушінің өкілдерімен коммуникация қазақ немесе ағылшын, немесе орыс тілінде қолжетімді болуы тиіс. Жеткізуші Интернет желісінде жүйенің техникалық құжаттамасына және әкімшілендіру жөніндегі құжаттамаға алдын ала тіркеусіз ашық қолжетімділікті қамтамасыз етуі тиіс. 9. Әлеуетті жеткізуші тендерге қатысу өтінімінің құрамында мыналарды ұсынады: – Жүйенің өндірушісінен не оның ресми өкілінен (дилерінен немесе дистрибьюторынан) әлеуетті жеткізушінің аталған өндірушінің өнімін Қазақстан Республикасының аумағында жеткізуге құқығын растайтын хаттың (сертификаттың, куәліктің) көшірмесін не әлеуетті жеткізушінің Жүйенің бағдарламалық қамтамасыз етуіне құқықтарын растайтын құжаттың көшірмесін; – Жүйенің ұсынылатын бағдарламалық қамтамасыз етуі нұсқасының ақпараттық қауіпсіздік талаптарына сәйкестігі бойынша қолданыстағы сынақ актісінің көшірмесін; – Жүйе құрамдас бөлігінің ұсынылатын нұсқасы бойынша Liveness тестілеуінен өткенін растайтын құжаттың көшірмесін; – Жүйе өндірушісіне аккредиттелген сертификаттау органы берген ISO/IEC 27001:2022 сәйкестік сертификатының қолданыстағы көшірмесін.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (монтаждау, іске қосу, дайындау, тексеру және тауарларды сынау)	Жеткізуші Жүйені енгізуді және Тапсырыс берушінің 2 қызметкерін Жүйені баптау мен онымен жұмыс істеу бойынша оқытуды қамтамасыз етуге тиіс. Жүйені енгізу шеңберінде мынадай іс-шаралар орындалуы тиіс: - Тапсырыс берушінің дайындалған инфрақұрылымын және осы техникалық ерекшеліктің талаптарын ескере отырып Жүйені орналастыру схемасын әзірлеу және келісу; - әзірленген және келісілген архитектураға сәйкес орнату; - саясаттар мен қағидаларды әзірлеу, баптау және бейімдеу.

Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

* мәліметтер сатып алу жоспарынан алынады (автоматты түрде көрсетіледі).

Ескерту:

1. Функционалдық, техникалық, сапалық, пайдаланушылық, өзге де сипаттамалар, ілеспе қызметтер бойынша әрбір талап және қосымша талаптар бөлек жолда көрсетіледі.

2. Өзге құжаттарда техникалық ерекшеліктің талаптарын белгілеуге жол берілмейді.

Приложение 6
к тендерной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Национальная компания "ҚазАвтоЖол"
Наименование организатора	Филиал "Дирекция платных автомобильных дорог" АО "Национальная компания "ҚазАвтоЖол"
№ тендера	№ 17885924-1
Наименование тендера	Электронные закупки товара программное обеспечение
Номер лота	№ 88200618-ОТ2
Наименование лота	Программное обеспечение
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*	620129.000.000000
Наименование товара*	Программное обеспечение
Единица измерения*	Штука
Количество (объем)*	1
Цена за единицу, без учета налога на добавленную стоимость*	64655172.41
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*	64655172.41
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*	с момента заключения договора в течение 30 календарных дней.
Размер авансового платежа*	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	
Год выпуска (Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора)	2026
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ Система биометрической аутентификации 1. Общие сведения Система биометрической аутентификации (далее — Система) предназначена для подтверждения личности пользователей по их уникальным физиологическим характеристикам с целью контроля физического и логического доступа, исключения несанкционированного использования учетных данных и обеспечения достоверного учета действий пользователей в информационных системах Заказчика. 2. Функциональные требования Система должна поставляться в виде программного обеспечения с возможностью развертывания и обработки биометрических данных в пределах инфраструктуры Заказчика. Система должна обеспечивать полный цикл дистанционной верификаций пользователя и последующего юридически значимого действия: биометрическая проверка на живость (liveness), сопоставление лица с базой Заказчика. Система должна поставляться как единая платформа, в которой должна присутствовать возможность использования компонентов отдельно либо последовательно в одном настраиваемом бизнес-процессе без необходимости разрабатывать отдельную интеграцию под каждый модуль. Система должна обеспечивать следующие ключевые сценарии: - прохождение пользователем liveness-проверки с получением лучшего кадра лица, альтернативного видео прохождения livenessпроверки, оригинальным видео прохождения liveness-проверки и результата; - Сопоставление лица клиента с эталонным изображением с базы данных Заказчика; - Передача итогового результата в ИС Заказчика через API, вебхук и/или кабинет. - Весь трафик и обработка персональных и биометрических данных в рамках промышленного контура должны осуществляться в инфраструктуре Заказчика и на территории Республики Казахстан. - Система должна иметь мониторинг в режиме реального времени с настроенными уведомлениями при остановке сервиса или возникновении любых ошибок. - Система должна иметь полноценную и актуальную документацию на русском и английском языке. - При прохождении биометрической верификации система должна выводить подсказки для пользователя для минимизации неуспешных попыток. - При неуспешных транзакциях/сессиях и при повторных попытках в логах должны отображаться причины ошибок. - Логи должны содержать общий транзакционный идентификатор. Логирование должно происходить на каждом компоненте Системы. - Система должна возвращать информативные и однозначные сообщения об ошибках. - Каждое сообщение об ошибке должно включать: a. описание причины возникновения; b. уровень ошибки (например: validation / server / network); c. рекомендации или дальнейшие действия для пользователя (если применимо). Решение должно быть конфигурируемым и расширяемым. Заказчик должен иметь возможность использовать отдельные сервисы либо комплексный процесс в рамках единого сценария. 2.1. Компонент биометрической идентификации Liveness Система должна обеспечивать проверку живого присутствия пользователя в режиме реального времени, выделение лучшего кадра лица, создание альтернативного видео, сохранения оригинального видео, анализ атак и возврат результата. Система должна обнаруживать лицо пользователя в кадре, контролировать позицию, поворот, освещенность, качество кадра, засветы, затемнения, размытие, наличие нескольких лиц и другие факторы, влияющие на качество биометрии. Система должна иметь функциональность по регуляции кол-ва действий/сигналов для конечного клиента, такие как: приближение, отдаление, поворот головы вправо/влево. Система должна выводить пользователю понятные подсказки: поместить лицо в овал, приблизиться/отдалиться, повернуть голову, улучшить освещение, снять очки при необходимости, повторить попытку. Система должна поддерживать активные и пассивные методы liveness, при этом конкретный режим должен настраиваться в зависимости от риска операции, канала и требований Заказчика. Система должна обнаруживать различные виды атак, такие как: - фото на бумаге, - фото/видео с экрана, - видеозаписи, - маски, - 3D-маски, - аватары, - deepfake/face swap, - виртуальные камеры, - эмуляторы, - подмену видеопотока, - подозрительную среду запуска, - cloud phone/remote relay признаки, - root/jailbreak или иные риск-индикаторы при наличии соответствующего SDK/сигналов. Система должна возвращать лучший кадр лица из процесса liveness для дальнейшего FaceMatch, формирования отчетного документа, передачи ИС Заказчика. - Количество попыток прохождения liveness должно настраиваться Заказчиком в конфигурации сервиса. Система должна поддерживать локализацию интерфейса и подсказок минимум на русском, казахском и английском языках Система должна корректно работать на мобильных браузерах, webview, desktop-браузерах в зависимости от выбранного способа интеграции. Среднее время серверной обработки результата liveness при штатной нагрузке не должно превышать 5 секунд без учета времени действий пользователя и внешних систем. Система должна обеспечивать логирование всех попыток, включая успешные, неуспешные, повторов, отмены пользователем и технические ошибки. Система должна четко разделять бизнес-отказы liveness, низкое качество изображения, отказ пользователя, технические ошибки клиента, сетевые ошибки и ошибки backend-сервиса. Система должна обеспечивать возможность передачи и сохранения следующих данных, полученных и/или сформированных в рамках прохождения биометрической верификации на серверах Заказчика: - видео прохождения биометрии; - лучший кадр лица пользователя (best frame); - эталонное фото, использованное для сличения; - коэффициент схожести; - результат liveness-проверки; - идентификатор транзакции/сессии; - дата и время прохождения проверки; - сведения об устройстве, с которого проходила биометрическая верификация. Качество работы Системы оценивается с использованием общепринятых отраслевых метрик: - APCER - показатель пропуска атак/мошеннических воздействий; - BPCER - показатель отклонения добросовестного пользователя. При условии соблюдения пользовательским сценариям, качеству входных данных, условиям съемки, используемому оборудованию и программному окружению, целевые показатели работы Системы должны составлять: - APCER ≤ 0,5 %; - BPCER ≤ 8 %. 2.2. Компонент FaceMatch Компонент FaceMatch должен выполнять сравнение изображения пользователя, полученного из liveness, с эталонным изображением из одного или нескольких источников: внутренней системы Заказчика, ранее загруженного изображения. Система должна возвращать процент сличения, результат, а также описание ошибок в случае возникновения. Система должна поддерживать сравнение изображения с фото из базы данных Заказчика. Все операции сравнения должны логироваться. В запросах биометрической верификации для всех видов операций система должна предоставить возможность добавлять порог схожести как отдельный входной параметр. Система распознавания лиц должна обеспечивать высокую точность распознавания, чтобы минимизировать ошибки ложного принятия (FAR — не более 0,001%) и ложного отклонения (FRR — не более 0,4%). Минимальный порог чувствительности и достоверности распознавания: TPR не менее 99,6%, FPR не более 0,4% на выборке от 1 000 000 фотографий. 2.3. Кабинет администрирования и мониторинга Платформа должна иметь web-кабинет администратора для настройки сервисов, пользователей, ролей, доступов, API-ключей. Кабинет должен поддерживать разграничение прав доступа: администратор, пользователь только для просмотра, пользователь отчетности. Кабинет должен предоставлять дашборды по количеству успешности, причинам отказов, ретраям и работе сервисов. Кабинет должен поддерживать выгрузку отчетов в согласованных форматах: CSV/XLSX/JSON/PDF. Система должна поддерживать неограниченное количество сотрудников Заказчика в кабинете в рамках согласованной ролевой модели без отдельной платы за каждую учетную запись, если иное не установлено договором. 3. Требования к лицензированию Поставщик предоставляет годовую лицензию на использование программного обеспечения неограниченным количеством транзакций на верификацию в течение срока действия лицензии. 4. Требования к совместимости, масштабируемости производительности Платформа должна поддерживать работу на смартфонах, планшетах, ПК и иных устройствах с камерой. Hosted Frontend должен поддерживать актуальные версии Chrome, Safari, Edge, Firefox, мобильные браузеры iOS/Android и webview в приложениях Заказчика при соблюдении требований к доступу к камере. Платформа должна поддерживать горизонтальное масштабирование backend-сервисов без изменения архитектуры и кода Заказчика. Платформа должна поддерживать обработку не менее 1 000 000 транзакций в месяц с возможностью масштабирования. При массовом использовании система должна выдерживать пиковую одновременную нагрузку без деградации критичных backend-операций более 1500 запросов в минуту. Время серверной обработки liveness/FaceMatch в нормальных условиях должно составлять до 10 секунд по каждому компоненту без учета времени действий пользователя и внешних государственных систем. 5. Требования к развертыванию Система должна поддерживать развертывание в инфраструктуре Заказчика с использованием следующих вариантов: Docker Compose — для развертывания системы в средах разработки, тестирования и иных средах с ограниченным масштабом. Развертывание должно обеспечивать запуск необходимых компонентов решения в контейнеризированной среде. Kubernetes / OKD — для развертывания в промышленной среде. Развертывание должно осуществляться с использованием Helmчартов или иного стандартного механизма оркестрации, поддерживаемого решением, с возможностью масштабирования компонентов и управления их конфигурацией. 6. Требования к безопасности Любые изменения, способные повлиять на безопасность периметра Заказчика, должны выполняться только после согласования с Заказчиком. Система должна использовать защищённые протоколы передачи данных везде, где это возможно. Использование защищённых протоколов является обязательным при передаче, хранении и обработке данных категории Confidential и Highly Confidential, особенно персональных данных клиентов. Допустимые протоколы включают, но не ограничиваются: HTTPS, SSH, SNMPv3, TLS версии 1.2 и выше, IPSec, LDAPS. Система должна обеспечивать возможность изменения всех параметров учетных записей, включая: пароли, кодовые фразы, ключи шифрования, параметры SNMP, любые иные изменяемые данные. Должна быть предусмотрена возможность изменения или отключения всех учётных записей по умолчанию (guest, admin, root и т.д.), предоставляемых производителем, если такие имеются. Система должна обеспечивать полное логирование действий пользователей (администраторов, операторов и др.). Логи должны включать: - дату и время событий - IPадрес источника подключения - идентификацию пользователя - действия (просмотр, изменение, удаление, выполнение команд) - попытки входа (успешные и неудачные) - события отключения или остановки журналирования - все события, связанные с безопасностью В случае наличия дополнительных механизмов, например, кэширование биометрической проверки, или других механизмов, данные механизмы должны быть отключены для заказчика по умолчанию и должны быть включены только по согласованию с Заказчиком Система должна обеспечивать передачу всех секретов, персональных и критических данных исключительно в теле HTTP POST-запроса. Передача таких данных через URL (query-параметры), заголовки или иные открытые части запроса не допускается. 7. Требования к гарантийному обслуживанию Гарантия должна составлять не менее 12 месяцев. 8. Требования к технической поддержке Поставщик должен обеспечить Систему технической поддержкой сроком не менее 12 месяцев и не менее чем в режиме 5x8 (рабочие часы с 9:00 до 18:00, в рабочие дни с понедельника по пятницу). Такая стандартная поддержка должна позволять бесплатное решение проблем, связанных с эксплуатацией Системы и бесплатное обновление Системы (получение новых версий ПО и/или движков или исправления). Для решения проблем при эксплуатации Системы Поставщик должен предоставлять электронный сервис (веб-портал, специальный email-адрес, мобильное приложение и т. д.) для создания заявок от Заказчика или его представителей с автоматической регистрацией таких заявок в системе поддержки. Такой сервис должен иметь функционал подтверждения создания заявок, изменений статуса заявок и т.п. Работа с таким сервисом и коммуникация с представителями Поставщика должна быть доступна на казахском или английском, или русском языке. Поставщик должен предоставлять открытый доступ (без какой-либо предварительной регистрации) к технической документации и документации по администрированию системы в сети Интернет. 9. Потенциальный поставщик в составе заявки на участие в тендере представляет: – копию письма (сертификата, свидетельства) от производителя Системы либо его официального представителя (дилера или дистрибьютора), подтверждающего право потенциального поставщика на поставку продукции данного производителя на территории Республики Казахстан, либо копию документа, подтверждающего права потенциального поставщика на программное обеспечение Системы; – копию действующего акта испытаний на соответствие требованиям информационной безопасности в отношении предлагаемой версии программного обеспечения Системы; – копию документа, подтверждающего прохождение компонентом Системы Liveness независимого тестирования в отношении предлагаемой версии; – копию действующего сертификата соответствия ISO/IEC 27001:2022 для производителя Системы, выданного аккредитованным органом по сертификации.
Сопутствующие услуги (указываются при наличии) (монтаж, наладка, обучение, проверки и испытания товаров)	Поставщик должен обеспечить внедрение Системы и обучение 2-х сотрудников Заказчика по настройке и работе с Системой. В рамках внедрения Системы, должны быть выполнены следующие мероприятия: - Разработка и согласование схемы развертывания Системы с учётом подготовленной инфраструктуры Заказчика и требований настоящей технической спецификации; - Инсталляция согласно разработанной и согласованной архитектуры; - Разработка, настройка и адаптация политик и правил.

Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о закупках (указываются при наличии) (потенциальный поставщик за не указание и непредставление указанных сведений не отклоняется)	

* сведения подтягиваются из плана закупок (отображаются автоматически).

Примечание:

1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.

2. Квалификационные требования, предъявляемые потенциальным поставщикам в иных документах не устанавливаются.