Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының сыртқы істер Министрлігі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының сыртқы істер Министрлігі" мемлекеттік мекемесі
Конкурстың №:	№ 17951917-1
Конкурстың атауы:	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі
Лоттың нөмірі:	№ 87991412-ОК2
Лоттың атауы	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620920.000.000027
Қызметтің атауы:	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	5432681.02
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	5432681.02
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	техникалық ерекшелігіне сәйкес
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	6

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Бағдарламалық жасақтаманың техникалық және функционалдық сипаттамалары: Жүйе құрамына кіретін бағдарламалық қамтамасыз етуге қойылатын жалпы талаптар: - Жүйе Интернет желісі арқылы кемінде 800 пайдаланушының бір мезгілде жұмыс істеу мүмкіндігін қамтамасыз етуі тиіс. - Жүйе пайдаланушылар санын арттыру мүмкіндігін қамтамасыз ету үшін жүйе архитектурасын қайта қараусыз виртуалды ресурстарды көбейту арқылы ауқымдауды (масштабтауды) қолдауы тиіс. - Жүйе аутентификация сервері мен пайдаланушыларды басқару жүйесі «бұлтта» орналасқан аралас (гибридті) шешім түрінде жүзеге асырылуы тиіс. - Бағдарламалық жасақтаманың бұлтты бөлігі Қазақстан Республикасының аумағында орналасуы тиіс. - Тапсырыс берушінің инфрақұрылымында орналастырылатын жүйе компоненттері істен шығуға төзімділікті қамтамасыз ету үшін кластерленуі тиіс. - Кластерленетін компоненттер «Active/Standby» істен шығуға төзімді конфигурациясын қамтамасыз етуі тиіс. - Тапсырыс берушінің инфрақұрылымында орналастырылатын жүйе компоненттері виртуалдандыру ортасына орнату мүмкіндігіне ие болуы тиіс. Қойылатын талаптар: Бағдарламалық жасақтаманың барлық сипаттамалары осы техникалық ерекшелікте көрсетілген минималды пайдалану сипаттамаларына сәйкес келуі немесе олардан жоғары болуы тиіс. Әлеуетті жеткізушіге қойылатын талаптар: Әлеуетті жеткізуші ұсынылатын Multifactor бағдармалық жасақтаманың лицензиясын ұзарту бойынша қызметті көрсету құқығын растайтын өндірушілерден не олардың дилерлерінен немесе дистрибьюторларынан хаттың көшірмесін (авторизациялық хатты) ұсынуға міндетті. Пайдалану сипаттамалары: Лицензияның қолданылу мерзімі: лицензияны белсендіру күнінен бастап кемінде 6 ай. Қызмет көрсету мерзімі: Шарт күшіне енген күннен бастап 30 (күнтізбелік) күн ішінде. Қызмет көрсету орны: Астана қ., Д. Қонаев көшесі, 31 Функционалға қойылатын талаптар: - Жүйе аутентификацияның екінші факторы ретінде OTP, Push-хабарламалар, SMS-хабарламалар, қоңырау шалу, Telegram мессенджеріндегі хабарлама түрлерін пайдалануға мүмкіндік беруі тиіс. - Жүйе екі факторлы аутентификацияны келесі жағдайларда жүзеге асыру мүмкіндігін қамтамасыз етуі тиіс: - Тапсырыс берушінің ақпараттық ресурстарына Интернет желісі арқылы VPN қосылу арқылы қол жеткізген кезде (келесі өндірушілердің VPN шешімдерін қолдауы тиіс: Cisco, CheckPoint, FortiGate, Huawei, Palo Alto, Mikrotik, OpenVPN, Traffic Inspector Next Generation, S-Terra, сондай-ақ Radius және/немесе LDAP аутентификация протоколдарын қолдайтын басқа да өндірушілер), сондай-ақ PAM-жүйелерімен (Wallix) бірге жұмыс істеу мүмкіндігі болуы тиіс; - IEEE 802.11 стандарттарына негізделген Тапсырыс берушінің сымсыз желі контроллерлерімен интеграция кезінде; - Корпоративтік электрондық поштаға қол жеткізген кезде (Microsoft Outlook Web Access және ActiveSync қолдайтын мобильді құрылғылар арқылы); - Виртуалды жұмыс үстелдеріне (APM / VDI – RDP, Citrix және т.б.) қол жеткізген кезде. - Бұлттық қосымшаларға (SAML, OpenID Connect / OAuth) қол жеткізу кезінде; - Тапсырыс берушінің

	web-қосымшаларына, сайттарына және бұлттық сервистеріне қол жеткізу кезінде келесі стандартты протоколдарды пайдалану арқылы: RADIUS; REST; WCF; WS-Federation (ADFS); HTTP (SMS-шлюздармен интеграция мүмкіндігі үшін); - Пайдаланушылардың домен әкімшісі құқықтары бар MS Windows операциялық жүйелерімен басқарылатын жұмыс орындары мен серверлерге, сондай-ақ Root тіркелгісі құқықтары бар Unix операциялық жүйелерімен басқарылатын жұмыс орындары мен серверлерге, сондай-ақ инфрақұрылымның виртуализация құралдарына (Vmware vCloud Director, Huawei.Cloud және т.б.) қол жеткізу кезінде; - Жүйе келесі тіркелгі провайдерлерімен интеграция мүмкіндігіне ие болуы тиіс: Microsoft Active Directory, OpenLDAP, FreeIPA, Samba, SAML 1.0/2.0 IdP, Astra Linux Directory, OAuth 2.0 және OpenID Connect. - Жүйе қауіпсіздік оқиғаларын беру үшін SIEM санатындағы шешімдермен интеграция мүмкіндігін қамтамасыз етуі тиіс. - Жүйенің (On-Prem агент) Windows және Linux ортада орнату мүмкіндігі болуы тиіс. - Жүйе (On-Prem агент) RADIUS агенті, RADIUS-сервері ретінде, сондай-ақ Network Policy Server (NPS) проксиі ретінде жұмыс істей алуы тиіс. - Жүйе шартты RADIUS атрибуттарын беру мүмкіндігіне ие болуы тиіс. - Жүйе кіру кезінде Captcha тексерісін жүргізу мүмкіндігіне ие болуы тиіс. - Жүйеде пайдаланушының өз бетінше тіркелу функциясы қарастырылуы тиіс, бұл тіркеу жергілікті есептеу желісі арқылы да, Интернет желісі арқылы да қолжетімді болуы тиіс. Жүйенің ішіндегі ақпаратқа, сондай-ақ Жүйемен біріктірілген корпоративтік ресурстарға қолжетімділік тек әкімші тіркеуді растағаннан кейін жүзеге асырылуы тиіс. - Жүйеде авариялық жағдайларда пайдаланушылардың үзіліссіз жұмысын қамтамасыз ету үшін айналып өту (bypass) механизмдері көзделуі тиіс. - Жүйе алдын ала орнатылған рөлдермен икемді рөлдік қауіпсіздік моделін қолдауы тиіс. - Жүйе тіркелгі паролін іріктеу шабуылдарынан (bruteforce) қорғайтын функцияға ие болуы тиіс. - Жүйе Radius-интеграция кезінде бірінші факторға дейін 2FA сұрау функциясын қамтамасыз етуі тиіс. Басқару және әкімшілендіру құралдарына қойылатын талаптар: - Жүйеде Жүйе әкімшісіне арналған web-портал болуы тиіс. - Жүйеде ашық және құжатталған Rest Full API болуы тиіс. - Жүйеде өз-өзіне қызмет көрсету порталы арқылы пайдаланушы тіркелгісінің паролін қалпына келтіру мүмкіндігі болуы тиіс. - Жүйе әкімшісінің web-порталында келесі функционал қолжетімді болуы тиіс: - бірыңғай консоль арқылы орталықтандырылған басқару; - пайдаланушыларды (пайдаланушылар топтарын) басқару арқылы әкімшілік өкілеттіктерін бөлу, сонымен қатар бағдарламалық қосымшалар интерфейсі (API) арқылы (оның ішінде, бірақ шектелмей): пайдаланушыны құру / тіркеу; пайдаланушыны жою; пайдаланушыны бұғаттау; кез келген пайдаланушы үшін аутентификацияның екінші факторын бұғаттау. - Web-порталда жалпы оқиғалар журналын жүргізу жүйесі болуы тиіс (қосылу геолокациясын көру мүмкіндігімен қоса). - Әкімшілердің web-порталға қол жеткізуі тек екі факторлы аутентификация құралдарын қолдану арқылы

	жүзеге асырылуы тиіс. Оқиғалар журналын жүргізуге қойылатын талаптар: - Жүйеде пайдаланушылар әрекеттеріне аудит жүргізу ұйымдастырылуы тиіс, оның ішінде: -- пайдаланушының аутентификациясының сәтті/сәтсіз әрекеттері туралы оқиғалар журналы; -- жүйеде пайдаланушының тіркелу журналы (аутентификацияның екінші факторын алу бөлігі бойынша). - Жүйе аутентификация журналына жазылатын оқиғаларды сүзгіден өткізу мүмкіндігін қамтамасыз етуі тиіс. - Жүйе оқиғалар журналын Тапсырыс берушінің SIEM жүйелерімен интеграциялау мүмкіндігі үшін экспорттауға мүмкіндік беруі тиіс. Бір реттік құпиясөздерге (OTP) қойылатын талаптар: - Жүйеде Android, iOS және Harmony OS операциялық жүйелерімен басқарылатын мобильді құрылғыларға кіру сұраныстары үшін push-хабарламаларды жіберетін өзіндік мобильді қосымшасы болуы тиіс. - Жүйеде пайдаланушылардың бір реттік құпиясөздер (OTP) арқылы күшейтілген аутентификациясы ұйымдастырылуы тиіс: - Бағдарламалық токендер: оқиғаға байланысты HOTP – RFC 4226 стандартына сәйкес; уақытқа байланысты TOTP – RFC 6238 стандартына сәйкес. - Аппараттық OTP: HOTP – RFC 4226, және TOTP – RFC 6238 стандартына сәйкес. - OTP генерациялаудың қолдау көрсетілетін алгоритмдері: -- HOTP: -- RFC 4226 + HMAC-SHA-1 (6 сан) - - TOTP: -- RFC 6238 + HMAC-SHA-1 (6 сан) -- RFC 6238 + HMAC-SHA-256 (6 сан) -- RFC 6238 + HMAC-SHA-512 (6 сан) -- Push-хабарламалар -- Messaging-токендер (SMS) - OTP токендерін қолдана отырып аутентификация режимдерінің әртүрлілігі: -- тек OTP; -- домендік құпиясөз + OTP; Жүйенің жұмыс істеу режимдеріне қойылатын талаптар: - Жүйе келесі режимдерде жұмыс істеуі тиіс: - Қалыпты режим – Жүйе мен оған қатысты жүйелердің істен шығусыз жұмыс істеп, деректер алмасуын толық көлемде қамтамасыз ететін режим. Жүйенің қалыпты жұмыс режимі 24*7*365 формуласы бойынша (тәулік бойы, аптасына 7 күн, жылына 365 күн – демалыссыз және мерекесіз) есептелуі тиіс. - Авариялық режим – Жүйенің қандай да бір компоненті істен шыққан жағдайда оның басқа компоненттері толық көлемде жұмыс істеуін жалғастырып, істен шықпаған жүйелермен ақпарат алмасуды қамтамасыз ететін режим. - Сервистік режим – Жүйеде алдын ала жоспарланған кесте бойынша қызмет көрсету, қайта конфигурациялау немесе компоненттерді жаңарту жүргізілетін режим. Бұл режимде Жүйе жаңартылатын компонентке қатысы жоқ барлық компоненттердің толық көлемде жұмысын және ақпарат алмасуын қамтамасыз етуі тиіс. Жүйенің сенімділігі мен үздіксіз жұмысына қойылатын талаптар: Жүйе үздіксіз жұмыс істеуді қамтамасыз етуі тиіс: тәулігіне 24 сағат, аптасына 7 күн, жылына 365 күн – демалыссыз және мереке күндерсіз. Жүйенің үздіксіз жұмысы Тапсырыс беруші қолданатын есептеу жүйелерінің аппараттық және бағдарламалық құралдарының, деректерді сақтау жүйелерінің, резервтік көшіру жүйелерінің және басқа да ақпараттық бағдарламалық жүйелер мен қосымшалардың үздіксіздігін қамтамасыз ету шараларын ескере отырып қамтамасыз етілуі тиіс (аппараттық құралдарды резервтеу, үздіксіз қоректендіру көздерін пайдалану,

	дискілер мен модульдерді резервтеу және т.б.). Жүйенің істен шығуға төзімділігі келесі жолдармен қамтамасыз етілуі тиіс: - жүйенің аппараттық-бағдарламалық құралдарының сенімді жұмысы арқылы; - жүйенің толық істен шығуына әкелетін сыни элементтерін резервтеу арқылы; - негізгі компоненттер істен шыққан жағдайда резервтік негізгі элементтерге автоматты түрде ауысу механизмдерін пайдалану арқылы; - бір немесе бірнеше құрамдас компоненттер істен шыққан жағдайда Жүйенің жұмысқа қабілеттілігін сақтау мүмкіндігі арқылы; - жүйе компоненттерінің өндірушілерінің ұсыныстарына және Тапсырыс берушінің резервтеу саясатына сәйкес резервтік көшіру механизмдерін қамтамасыз етуге бағытталған кешенді шаралар арқылы. Бағдарламалық қамтамасыз етуді кепілді қолдауға қойылатын талаптар: Кепілдік қызмет көрсету Қазақстан Республикасының бүкіл аумағында бағдарламалық жасақтама өндірушісінің және (немесе) оның серіктестерінің сертификатталған мамандары арқылы орыс тілінде жүзеге асырылуы тиіс. Кепілдік қызмет көрсетуге өтінімдер келесі арналар арқылы қабылдануы тиіс: о электрондық пошта арқылы; о Telegram мессенджеріндегі арнайы чат арқылы; о Интернет желісіндегі сайт арқылы. - Кепілдік қолдаудың шектері Кепілдік келесі жағдайларды қамтиды: о Жүйе құрамына кіретін бағдарламалық жасақтаманың функционалдығына әсер ететін қателер; о Жүйе құрамына кіретін бағдарламалық жасақтаманың тұрақты жаңартуларына қатысты қателер мен сұрақтар; о Жүйе құрамына кіретін бағдарламалық жасақтаманың қате іске қосылуы (қате срабатывание); о Жүйе құрамына кіретін бағдарламалық жасақтамадағы жоғалған немесе бүлінген деректерді қалпына келтіру; о Келесі әрекеттер реттілігіне қатысты сұрақтар: Жүйе құрамына кіретін бағдарламалық жасақтаманы жүктеу тәртібі мен дереккөзі; Жүйе құрамына кіретін бағдарламалық жасақтаманы орнатуға қатысты негізгі сұрақтар; Жүйе құрамына кіретін бағдарламалық жасақтамамен жұмыс істеу кезінде бәсекелес бағдарламаларды жою; о Жүйе құрамына кіретін бағдарламалық жасақтаманы пайдалану лицензиясының әрекет етуіне қатысты сұрақтар. Кепілдік мерзімі (аймен) 6 Тапсырыс берушінің желілік инфрақұрылымының элементтерін есепке алмағанда, Жүйенің қол жетімділігіне қойылатын талаптар 1-кестеде келтірілген. 1-кесте. Жүйенің қол жетімділігіне қойылатын талаптар: Жұмыс режимі/параметрі Мәні Жүйенің штаттық режимде қол жетімділік коэффициенті 99,8% кем емес Жүйенің жылына қол жетімсіздігінің ең көп жиынтық уақыты 4 сағаттан артық емес (3 айда 1 реттен жиі емес) Жүйені ақаулықтан кейін қалпына келтіру үшін ең ұзақ уақыт (RTO – Recovery Time Objective) 24 сағаттан артық емес Істен шығу орын алғанға дейінгі деректердің жоғалуына жол берілетін ең ұзақ уақыт аралығы (RPO – Recovery Point Objective) 12 сағаттан артық емес.

Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Министерство иностранных дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Министерство иностранных дел Республики Казахстан"
№ конкурса:	№ 17951917-1
Наименование конкурса:	Услуги по технической поддержке лицензионного программного обеспечения
Номер лота:	№ 87991412-ОК2
Наименование лота:	Услуги по технической поддержке лицензионного программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620920.000.000027
Наименование услуги:	Услуги по технической поддержке лицензионного программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	5432681.02
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	5432681.02
Срок оказания услуги:	согласно условиям техспецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	6

Описание требуемых характеристик, параметров и иных исходных данных	Технические и функциональные характеристики ПО: Общие требования к ПО, входящего в состав Системы: - Система должна обеспечить возможность одновременной работы не менее 800 пользователей при доступе из сети Интернет. - Система должна поддерживать масштабирование посредством увеличения виртуальных ресурсов без пересмотра архитектуры системы (для возможности увеличении количества пользователей). - Система должна быть реализована в виде гибридного решения с сервером аутентификации и системой управления пользователями в «облаке». - Облачная часть ПО должна располагаться на территории Республики Казахстан; - Компоненты системы, которые размещаются в инфраструктуре заказчика, должны быть кластеризированы, для обеспечения отказоустойчивости. - Кластеризуемые компоненты должны обеспечивать отказоустойчивую конфигурацию «Active/Standby». - Компоненты системы, которые размещаются в инфраструктуре Заказчика, должны иметь возможность установки в среде виртуализации. Предъявляемые требования: Все характеристики программного обеспечения должны соответствовать или превосходить минимальные эксплуатационные характеристики, указанные в данной технической спецификации. Требования к потенциальному поставщику: Потенциальный поставщик в составе конкурсной заявки должен предоставить копию письма (авторизационное письмо) от производителей либо их дилеров или дистрибьюторов, подтверждающее право на оказание услуги по продлению лицензий на программное обеспечение Multifactor. Эксплуатационные характеристики: Срок действия лицензии: не менее 6 месяцев со дня активации лицензии. Срок оказания услуги: в течении 30 (календарных) дней со дня вступления в силу Договора. Место оказания услуги: г. Астана, ул. Д. Кунаева 31. Требования к функционалу: - Система должна иметь возможность использования в качестве второго фактора аутентификации OTP, Push-уведомления, SMS уведомления, звонок, сообщение в мессенджер Telegram. - Система должна иметь возможность реализации двухфакторной аутентификации: при доступе к информационным ресурсам Заказчика из сети интернет с использованием VPN-соединения (должны поддерживаться VPN решения следующих производителей: Cisco, CheckPoint, FortiGate, Huawei, Palo Alto, Mikrotik, OpenVPN, Traffic Inspector Next Generation, S-Terra, а также других производителей, поддерживающих протоколы аутентификации Radius и/или LDAP) и PAM-системы (Wallix); - при интеграции с контроллерами беспроводных сетей Заказчика на основе стандартов IEEE 802.11; - при доступе к корпоративной электронной почте (Microsoft Outlook Web Access и мобильные устройства ActiveSync); - при доступе к виртуальным рабочим столам (APM / VDI - RDP, Citrix и др.) - при доступе к облачным приложениям (SAML, OpenID Connect / OAuth) - при доступе к web-приложениям, сайтам и облачным сервисам Заказчика с использованием стандартных протоколов: RADIUS; REST; WCF; WS-Federation (ADFS); HTTP (для возможности интеграции с SMS-шлюзами); - при доступе пользователей на рабочие места и

	сервера под управлением операционных систем MS Windows с правами доменного администратора и на рабочие места и сервера под управлением операционных систем Unix с правами учетной записи Root, средствам виртуализации инфрастуктуры (Vmware vCloud Director, Huawei.Cloud и др.) -Система должна иметь возможность интеграции с провайдерами учётных записей: Microsoft Active Directory, OpenLDAP, Freeipa, Samba, SAML 1.0/2.0 IdP, Astra Linux Directory , OAuth 2.0 и OpenID Connect - Система должна иметь возможность интеграции с решениями класса SIEM для передачи событий безопасности. - Система (On-Prem агент) должна иметь возможность установки в Windows и Linux среде. - Система (On-Prem агент) должна иметь возможность работы как RADIUS агент, RADIUS-сервер, прокси к Network Policy Server (NPS) - Система должна иметь возможность передачи условных RADIUS атрибутов - Система должна иметь возможность проверки Captcha при входе - В Системе должна быть возможность самостоятельной регистрации пользователем в режиме диалога, как при доступе из локальной вычислительной сети, так и при доступе из сети Интернет. Доступ к информации внутри Системы, а также к корпоративным ресурсам, с которыми интегрирована Система, производится только после подтверждения регистрации администратором Системы. - В системе должна быть предусмотрена возможность сквозных (bypass) механизмов для обеспечения бесперебойной работы пользователей при аварийных ситуациях. - Система должна поддерживать гибкую ролевую модель безопасности с предустановленными ролями. - Система должна иметь функционал, защищающий от перебора паролей учетной записи (bruteforce). - Система должна иметь функционал запроса 2FA перед первым фактором для Radius-интеграций. Требования к средствам управления и администрирования: - Система должна иметь web-портал для администратора Системы. - Система должна иметь открытый и документированный Rest Full API - Система должна иметь возможность сброса пароля от учетной записи пользователя на портале самообслуживания - В web-портале администратору системы должен быть доступен следующий функционал: - централизованное управления через единую консоль; - управления пользователями (группами пользователей) для разделения полномочий администрирования в том числе через программный интерфейс приложений API (включая, но не ограничиваясь): создание/регистрация пользователя; удаление пользователя; блокировка пользователя; блокировки второго фактора аутентификации для любого пользователя; - Web-портал должен иметь общую систему журналирования событий (включая возможность просмотра геолокации подключения). - Доступ администраторов к web-порталу возможен только с использованием средств двухфакторной аутентификации. Требования к журналированию событий: - В Системе должен быть организован аудит действий пользователей системы: -- журнал событий успешной/неуспешной попытки аутентификации пользователя; -- журнал регистрации пользователя в Системе (в части получения второго фактора

	аутентификации); - Система должна предусматривать возможность фильтрации событий, записываемых в журнал аутентификации. - Система должна иметь возможность выгрузки журналов событий для возможности интеграции с SIEM-системами Заказчика. Требование к одноразовым паролям: - Система должна иметь собственное мобильное приложение для отправки push-уведомлений запросов доступа на мобильных устройствах под управлением операционных систем Android/iOS/Harmony OS; - В системе должна быть организована усиленная аутентификация пользователей по одноразовым паролям (OTP): - Программные токены TOTP/HOTP по событию – HOTP согласно RFC 4226; и по времени – TOTP согласно RFC 6238. - Аппаратные OTP – HOTP согласно RFC 4226; и TOTP согласно RFC 6238. - Поддерживаемые алгоритмы генерации OTP: -- HOTP: -- RFC 4226 + HMAC-SHA-1 (6 цифр); -- TOTP: -- RFC 6238 + HMAC-SHA-1 (6 цифр); -- RFC 6238 + HMAC-SHA-256 (6 цифр); -- RFC 6238 + HMAC-SHA-512 (6 цифр); -- Push-уведомления; -- Messaging-токены (SMS). - Вариативность режимов аутентификации с применением OTP-токенов: -- только OTP; -- доменный пароль + OTP; Требования к режимам функционирования Системы: - Система должна функционировать в следующих режимах: Нормальный режим – режим, при котором Система и смежные системы работают без сбоев и реализуют обмен данными, работа Системы осуществляется в полном объеме. Нормальный режим функционирования Системы должен рассчитываться исходя из формулы 24*7*365 (24 часа в сутки 7 дней в неделю 365 дней в году без праздников и выходных дней); Аварийный режим – режим, при котором Система продолжает работу в случае выхода из строя одного из компонентов. В данном режиме Система должна предоставлять возможность работы всех остальных компонентов в полном объеме и предоставлять информационный обмен для систем, не затронутых сбоем вышедшего из строя компонента; Сервисный режим – режим, при котором в Системе по запланированному графику проводится обслуживание, реконфигурация или обновление компонентов. В данном режиме Система должна предоставлять возможность работы всех компонентов в полном объеме и предоставлять информационный обмен для систем, не затронутых работами на обновляемом компоненте. Требования к надежности и непрерывности работы Системы: Функционирование Системы должно обеспечиваться в режиме 24 часа в сутки, 7 дней в неделю 365 дней в году без праздников и выходных дней. Непрерывность работы Системы должна обеспечиваться с учетом применяемых Заказчиком мер по обеспечению непрерывности работы аппаратных и программных средств вычислительных систем, систем хранения данных, систем резервного копирования и других программных информационных систем и приложений (резервирование аппаратных средств, использование источников бесперебойного питания, резервирование дисков, модулей). Отказоустойчивость Система должна обеспечиваться за счет: надежности работы аппаратно-программных средств Системы; резервирования критически важных элементов Системы, отказ которых приведет к потере

	работоспособности всей Системы; использования механизмов автоматического переключения на резервные ключевые элементы Системы в случае сбоя основных компонентов; возможности Системы сохранять работоспособность после отказа одного или нескольких составных компонентов; комплекса мер по обеспечению механизмов резервного копирования, соответствующих принятой Заказчиком политике резервирования и рекомендациям производителя компонентов Системы. Требования к гарантийной поддержке программного обеспечения: Гарантийное обслуживание предоставляется на русском языке сертифицированными специалистами производителя ПО и (или) его партнерами на всей территории Республики Казахстан. Прием заявок на гарантийное обслуживание должен приниматься по: о электронной почте; о выделенном чате в мессенджере telegram; о через сайт в сети Интернет. Границы оказания гарантийной поддержки. Гарантия распространяется на: о ошибки, затрагивающие функциональность ПО, входящего в состав Системы; о ошибки и вопросы по регулярным обновлениям ПО, входящего в состав Системы; о ошибочные срабатывания ПО, входящего в состав Системы; о восстановление утраченных или поврежденных данных ПО, входящего в состав Системы; о вопросы о необходимом порядке действий, таким как: порядок и источник загрузки ПО, входящего в состав Системы; основные вопросы по установке ПО, входящего в состав Системы; удаление конкурирующих программ для ЭВМ при работе ПО, входящего в состав Системы; о вопросы, связанные с действием лицензии на использование ПО, входящего в состав Системы. Гарантийный срок (в месяцах) 6 Требования к доступности Системы, без учета элементов сетевой инфраструктуры Заказчика, приведены в Таблице 1. Таблица 1. Требования к доступности Системы: Режим работы / параметр Значение Коэффициент доступности Системы в штатном режиме Не менее 99,8% Максимальное суммарное время недоступности Системы в год Не более 4 часов (не чаще 1 раза в 3 месяца) Максимальное время для восстановления Системы после сбоя (RTO – Recovery Time Objective) Не более 24 часов Максимальный промежуток времени до наступления сбоя, данные за который могут быть утрачены (RPO – Recovery Point Objective) Не более 12 часов.

Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	