

Форма 4.2 «Техническая спецификация для закупки товаров»

**Техническая спецификация
«Двухфакторная аутентификация»**

- 1 Предмет закупаемых товаров.** ПО для двухфакторной аутентификации
- 2 Обоснование закупаемых товаров.** Приобретение ПО необходимо для обеспечения безопасного доступа к корпоративным системам, защиты учетных записей пользователей и предотвращения несанкционированного доступа.
- 3 Объем закупаемых товаров**

№ п/п	Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики	Ед. изм.	Количество
1	2	3	4
1	1. Предоставление двухфакторной аутентификации без необходимости подключения к сети Интернет. 2. Возможность получения одноразового пароля с помощью мобильного приложения, push-уведомления, SMS-сообщения или токена. 3. Возможность указать собственные пути доставки одноразовых паролей. 4. Уникальный алгоритм генерации паролей для каждого пользователя. 5. Интеграция с Active Directory. 6. Возможность использования в инфраструктуре без домена. 7. Поддержка LDAP и MAC Open Directory. 8. Возможность добавления 2FA для безопасного доступа входа как локальной учетной записи, так и доменной учетной записи системы под управлением: Microsoft Windows, Linux или MAC OS X. 9. Наличие Identity Provider Connector для обеспечения 2FA облачных служб (поставщиком услуг) и поставщиком идентификационных данных, таких как: OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence. 10. Возможность использования резервного пароля (Master Recovery Key). 11. Поддержка аппаратных токенов, работающих по стандартам OATH, HOTP, TOTP, FIDO, FIDO2. 12. Защита VPN и VDI систем, таких как: Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC, Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, Netasq, VMware Horizon View и Citrix XenApp, Cyberoam. 13. Возможность использования двухфакторной аутентификации для защиты VPN подключений, Remote Desktop Protocol, авторизация в ОС, Web сервисов которые используют Microsoft ADFS 3 или 4, Microsoft Web Apps, Microsoft Exchange Server, Microsoft Share Point Server, Remote Desktop Web Access, Microsoft Dynamics CRM, VMware Horizon View, сервисы на основании RADIUS. 14. Защита через SSO и Microsoft Active Directory Federation Services для входа в Office 365 или Azure. 15. Использование двухфакторной аутентификации в безопасном режиме Windows и в режиме блокировки ПК. 16. Защита UAC доступа двухфакторной аутентификацией. 17. RADIUS PAM для ОС Linux/Mac, (Защита SSH, cli login, GUI login). (При условии членства в AD). 18. Возможность создавать белые списки IP адресов, доступ с которых не потребует двухфакторной аутентификации; наличие пакетов API и SDK позволяющих использовать двухфакторную аутентификацию с любым пользовательским приложением	шт	1300



	19. Поставка включает развертывание системы в отказоустойчивой конфигурации и интеграцию с существующими работающими системами для обеспечения двухфакторной аутентификации всех пользователей. 20. Информирование пользователя о попытке авторизации с возможностью подтвердить или отклонить проверку подлинности. 21. Наличие системы отчетности, которая может использоваться как для панели мониторинга, так и для формирования отчетов. 22. Наличие журнала аудита, в котором регистрируются и отслеживаются все изменения в конфигурации, запуске и остановке службы двухфакторной аутентификации. 23. Возможность интеграции с SIEM и другими системами мониторинга, анализа и реагирования. 24. Возможность администратора предоставлять альтернативный одноразовый пароль OTP в случае, если у пользователя нет доступа к токену или мобильному приложению. 25. Поставщик гарантирует непрерывную работоспособность системы в течение 1 года, обеспечивает полное сопровождение системы для бесперебойной работы, включая необходимые настройки и конфигурации. 26. Возможность импортировать пользователей в специальные области с помощью CSV или LDF. 27. Возможность ограничить количество использования одноразовых паролей для компьютеров, не имеющих подключения к серверу 2FA. 28. Поставляемая система должна быть последней стабильной версией, при появлении обновлений поставщик производит все виды обновлений 29. Наличие защиты от подбора одноразового пароля путём блокировки пользователя. 30. Наличие системы уведомлений о выбранных типах действий.		
	Требования к Поставщику товара нет		
	Обязанности Поставщика товара нет		

4 Место поставки товара

Поставщик предоставит товар в распоряжение получателя по адресу: Республика Казахстан, г. Алматы, пр. Абая 109В, БЦ «Глобус».

5 Сроки поставки товара

С даты подписания договора до 31.12.2026.

Директор ДТиИТ

 У Сяоцай

Заместитель директора ДТиИТ

 Мукушев Д.Б.



4.2-нысан «Тауарларды сатып алуға арналған техникалық сипаттізім»

Техникалық сипаттізім «Екі факторлы аутентификация»

- 1 Сатып алынатын тауарлардың мәні Екі факторлы аутентификацияға арналған бағдарламалық қамтамасыз ету
- 2 Сатып алынатын тауарлардың негіздемесі Бағдарламалық жасақтама корпоративтік жүйелерге қауіпсіз қол жеткізуді қамтамасыз ету, пайдаланушы есептік жазбаларын қорғау және рұқсатсыз қол жеткізудің алдын алу үшін қажет.
- 3 Сатып алынатын тауарлардың көлемі

№№ р/с	Сипаттамасы және қажетті функционалдық, техникалық, сапалық және пайдалану сипаттамалары	Өлш. бірл.	Саны
1	2	3	4
1	1. Интернетке қосылусыз екі факторлы аутентификацияны қамтамасыз етеді. 2. Бір реттік құпия сөзді мобильді қосымша, push-хабарлама, SMS немесе токен арқылы алу мүмкіндігі. 3. Бір реттік құпия сөздерді жеткізудің жеке жолдарын көрсету мүмкіндігі. 4. Әрбір пайдаланушыға арналған бірегей құпия сөз генерациялау алгоритмі. 5. Active Directory жүйесімен интеграция. 6. Доменсіз инфрақұрылымда пайдалану мүмкіндігі. 7. LDAP және Mac Open Directory қолдауы. 8. Microsoft Windows, Linux немесе macOS жүйелеріндегі жергілікті және домендік есептік жазбаларға қауіпсіз кіру үшін 2FA қосу мүмкіндігі. 9. Бұлттық қызметтер (қызмет провайдерлері) мен сәйкестендіру провайдерлері үшін 2FA қолдауына арналған Identity Provider Connector: OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence. 10. Қалпына келтіру құпия сөзімен (Master Recovery Key) жұмыс істеу мүмкіндігі. 11. OATH, HOTP, TOTP, FIDO, FIDO2 стандарттары бойынша аппараттық токендерді қолдау. 12. VPN және VDI жүйелерін қорғау: Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC, Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, Netasq, VMware Horizon View, Citrix XenApp, Cyberoam. 13. VPN қосылымдарын, Remote Desktop Protocol, операциялық жүйеге кіруді және Microsoft ADFS 3 немесе 4, Microsoft Web Apps, Microsoft Exchange Server, Microsoft SharePoint Server, Remote Desktop Web Access, Microsoft Dynamics CRM, VMware Horizon View, RADIUS негізіндегі қызметтерді қорғау үшін 2FA қолдану. 14. Office 365 немесе Azure жүйелеріне кіруді SSO және Microsoft Active Directory Federation Services арқылы қорғау. 15. Windows қауіпсіз режимінде және компьютерді құлыптау режимінде екі факторлы аутентификацияны пайдалану. 16. UAC рұқсаттарын екі факторлы аутентификация арқылы қорғау. 17. Linux/Mac OS жүйелеріне арналған RADIUS PAM (SSH, CLI login, GUI login қорғауы) (AD мүшелігі қажет). 18. Екі факторлы аутентификацияны қажет етпейтін IP-мекенжайлардың актізімін жасау мүмкіндігі; кез келген пайдаланушылық қосымшамен 2FA қолдану үшін API және SDK пакеттерінің болуы. 19. Жеткізу жүйені ақаулыққа төзімді конфигурацияда орналастыруды және	дана	1300

	барлық пайдаланушылардың екі факторлы аутентификациясын қамтамасыз ету үшін қолданыстағы жұмыс жүйелерімен біріктіруді қамтиды. 20. Пайдаланушыны авторизация әрекеті туралы хабардар ету және оны растау немесе қабылдау мүмкіндігі. 21. Мониторинг панелі мен есептерді қалыптастыруға арналған есеп беру жүйесі. 22. Конфигурациядағы өзгерістер, қызметтің іске қосылуы мен тоқтатылуы және екі факторлы аутентификацияға қатысты барлық оқиғаларды тіркейтін аудит журналы. 23. SIEM және басқа мониторинг, талдау және әрекет ету жүйелерімен интеграциялау мүмкіндігі. 24. Егер пайдаланушы токенге немесе мобильді қосымшаға қол жеткізе алмаса, әкімшіге балама OTP ұсыну мүмкіндігі. 25. Өнім беруші жүйенің 1 жыл бойы үздіксіз жұмыс істеуіне кепілдік береді, қажетті параметрлер мен конфигурацияларды қоса алғанда, үздіксіз жұмыс істеу үшін жүйенің толық қолдауын қамтамасыз етеді. 26. CSV немесе LDF арқылы пайдаланушыларды арнайы аймақтарға импорттау мүмкіндігі. 27. 2FA серверіне қосылмаған компьютерлерге арналған бір реттік құпия сөздерді қолдану санын шектеу мүмкіндігі. 28. Жеткізілетін жүйе соңғы тұрақты нұсқа болуы керек, жаңартулар пайда болған кезде Жеткізуші жаңартулардың барлық түрлерін шығарады 29. Бір реттік құпия сөзді таңдау арқылы шабуылдан қорғау (пайдаланушыны блоктау арқылы). 30. Белгілі бір әрекеттер бойынша хабарландыру жүйесінің болуы.		
	Тауарды Жеткізушіге қойылатын талаптар		
	Жоқ		
	Тауарды Жеткізушінің міндеттері		
	Жоқ		

4 Тауарларды жеткізу орны:

Тауарды жеткізу орны мен шарттары: Әлеуетті жеткізуші Тауарды Сатып алушының иелігіне төмендегі мекенжай бойынша ұсынуға тиіс: Қазақстан Республикасы, Алматы қаласы, Абай даңғылы, 109В, «Глобус» БО.

5 Тауарларды жеткізу мерзімі:

Басталуы - шарт жасалған күннен бастап, аяқталуы - 31.12.2026 ж.

ТЖАТ департаментінің директоры

 У Сяоцай

ТЖАТ департаменті директорының
орынбасары

 Мукушев Д.Б.

Form 4.2 Technical specification for purchase of goods

Technical specification «Two-Factor Authentication»

- 1 Item of purchased goods.** Software for two-factor authentication.
- 2 Justification of purchased goods.** The software is required to ensure secure access to corporate systems, protect user accounts, and prevent unauthorized access.
- 3 Volume of purchased goods**

No.	Description and required functional, technical, quality and performance characteristics	Unit	Quantity
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
1	1. Provides two-factor authentication without requiring an Internet connection. 2. Ability to receive a one-time password via a mobile app, push notification, SMS message, or token. 3. Option to specify custom delivery paths for one-time passwords. 4. Unique password generation algorithm for each user. 5. Integration with Active Directory. 6. Can be used in an infrastructure without a domain. 7. Supports LDAP and Mac Open Directory. 8. Ability to add 2FA for secure login to both local and domain accounts on systems running Microsoft Windows, Linux, or macOS. 9. Identity Provider Connector for enabling 2FA for cloud services (service providers) and identity providers such as OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence. 10. Ability to use a backup password (Master Recovery Key). 11. Supports hardware tokens that comply with OATH, HOTP, TOTP, FIDO, and FIDO2 standards. 12. Protection for VPN and VDI systems, including Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC, Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, Netasq, VMware Horizon View, and Citrix XenApp, Cyberoam. 13. Supports two-factor authentication for securing VPN connections, Remote Desktop Protocol, OS login, and web services using Microsoft ADFS 3 or 4, Microsoft Web Apps, Microsoft Exchange Server, Microsoft SharePoint Server, Remote Desktop Web Access, Microsoft Dynamics CRM, VMware Horizon View, and RADIUS-based services. 14. Protection via SSO and Microsoft Active Directory Federation Services for logging into Office 365 or Azure. 15. Enables two-factor authentication in Windows Safe Mode and PC lock mode. 16. UAC access protection using two-factor authentication. 17. RADIUS PAM for Linux/Mac OS (protection for SSH, CLI login, GUI login) (requires AD membership). 18. Ability to create IP whitelists that bypass two-factor authentication; includes API and SDK packages for integrating 2FA with custom applications. 19. The delivery includes the deployment of the system in a fault-tolerant configuration and integration with existing operating systems to ensure two-factor authentication of all users. 20. Notifies users of authentication attempts with an option to approve or deny authentication. 21. Reporting system for dashboard monitoring and report generation. 22. Audit log that records and tracks all changes in configuration, service start/stop events, and two-factor authentication operations. 23. Integration with SIEM and other monitoring, analysis, and response systems.	pcs	1300

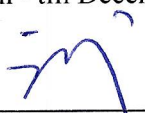
	24. Administrators can provide an alternative OTP if the user has no access to a token or mobile app. 25. The supplier guarantees the continuous operation of the system for 1 year, provides full system maintenance for uninterrupted operation, including the necessary settings and configurations. 26. Ability to import users into specific areas via CSV or LDF. 27. Option to restrict the number of OTP uses on computers that are not connected to the 2FA server. 28. The supplied system must be the latest stable version, and when updates become available, the supplier performs all types of updates. 29. Protection against OTP brute-force attacks through user account lockout. 30. Notification system for selected types of actions.		
	Requirements for the Product Supplier		
	No		
	Responsibilities of the Product Supplier		
	No		

4 Place of delivery of goods:

Place and terms of delivery of goods: potential supplier shall deliver the goods to the Buyer at the address: Republic of Kazakhstan, Almaty, Abai ave., 109V, BC "Globus".

5 Period of delivery of goods:

Beginning - from the date of conclusion of the contract, completion - till December 31, 2026.

Director of IT and Telecommunication Department _____  **Wu Xiaocai**

Deputy Director of IT and Telecommunication Department _____  **D.B. Mukushev**