

Об утверждении Правил интеграции цифровых объектов "цифрового правительства"

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 1 июля 2026 года № 368/НҚ.
Зарегистрирован в Министерстве юстиции Республики Казахстан 2 июля 2026 года № 39199

Примечание ИЗПИ!

Вводится в действие с 12.07.2026.

В соответствии с пунктом 3 статьи 83 Цифрового кодекса Республики Казахстан ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила интеграции цифровых объектов "цифрового правительства".

2. Признать утратившими силу некоторые приказы по перечню согласно приложению к настоящему приказу.

3. Комитету государственных услуг Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством порядке Республики Казахстан обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития Республики Казахстан после его официального опубликования.

4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

5. Настоящий приказ вводится в действие с 12 июля 2026 года и подлежит официальному опубликованию.

*Заместитель Премьер-Министра –
Министр искусственного интеллекта
и цифрового развития Республики Казахстан*

Ж. Мадиев

"СОГЛАСОВАН"

Комитет национальной
безопасности Республики Казахстан

Утверждены приказом
Заместитель Премьер-Министра –
Министр искусственного интеллекта

Правила интеграции цифровых объектов "цифрового правительства"

Глава 1. Общие положения

1. Настоящие Правила интеграции цифровых объектов "цифрового правительства" (далее – Правила) разработаны в соответствии с пунктом 3 статьи 83 Цифрового кодекса Республики Казахстан (далее – Кодекс) и определяют порядок интеграции цифровых объектов "цифрового правительства".

2. В настоящих Правилах используются следующие основные понятия:

1) архитектурно-координационный центр – юридическое лицо, определяемое Правительством Республики Казахстан, обеспечивающее целостность, совместимость и эффективность цифровой архитектуры государственных органов, государственных юридических лиц, субъектов квазигосударственного сектора, юридических лиц, пятьдесят и более процентов голосующих акций (долей участия) которых прямо или косвенно принадлежат субъектам квазигосударственного сектора, а также иных организаций, участвующих в процессах государственного управления;

2) сервис по предоставлению открытых данных – способ передачи данных в одностороннем порядке между цифровыми объектами;

3) токен верификации – электронный ключ в виде набора определенного количества цифр и букв, предназначенный для подтверждения получения согласия инициатором и (или) оператором от субъекта персональных данных;

4) безопасность веб-сервисов (WebServiceSecurity) (далее – WSSecurity) – стандарт применения функций безопасности при обмене сообщениями между веб-сервисами SOAP. При применении стиля архитектуры программного обеспечения для распределенных систем (REST) безопасность сервиса обеспечивается через меры безопасности HTTPs, и применением аутентификации пользователей;

5) государственный сервис контроля доступа к персональным данным – услуга, обеспечивающая информационное взаимодействие собственников и (или) операторов, третьих лиц с субъектом персональных данных и уполномоченным органом при доступе к персональным данным, содержащимся в цифровых объектах государственных органов и (или) государственных юридических лиц, включая получение от субъекта персональных данных согласия на сбор, обработку персональных данных или их передачу третьим лицам;

6) публичный Peer IP-адрес – уникальный IP-адрес устройства, терминирующего VPN-туннель и используемого в сети Интернет, на стороне инициатора интеграционного сервиса;

7) межсетевой протокол Internet Protocol (далее – IP) – маршрутизируемый протокол межсетевого уровня стека TCP/IP, предназначенный для передачи датаграмм между узлами компьютерной сети, обеспечивая их логическую адресацию;

8) интеграционные сервисы – функциональные цифровые объекты, обеспечивающие взаимодействие, обмен данными и выполнение согласованных операций между цифровыми объектами посредством стандартных интерфейсов, протоколов и механизмов доступа, определенных уполномоченным органом;

9) инициатор интеграционного сервиса – собственник или владелец цифрового объекта, инициирующий запрос на предоставление интеграционного сервиса;

10) собственник или владелец интеграционного сервиса – собственник или владелец цифрового объекта, предоставляющий интеграционный сервис;

11) расширяемый язык разметки (eXtensible Markup Language) (далее – XML) – расширяемый язык разметки, используемый для хранения и передачи данных в структурированном и машиночитаемом формате;

12) транспортная подпись – электронная цифровая подпись, используемая для обеспечения целостности и авторства передаваемых сообщений при информационном взаимодействии цифровых систем с применением спецификации WSSecurity;

13) удостоверяющий центр – юридическое лицо, созданное в соответствии с законодательством Республики Казахстан, которое подтверждает достоверность сертификатов открытых ключей электронной цифровой подписи, принадлежность и действительность открытых ключей электронной цифровой подписи;

14) API с открытым правом доступа (далее – OpenAPI) – формализованная спецификация, предоставляющая интерфейс между презентационной частью цифровой системы, ее пользовательским интерфейсом, библиотеками низкого уровня и application programming interface;

15) прикладной программный сервис – прикладное программное обеспечение, предназначенное и (или) используемое для выполнения прикладных пользовательских задач, цифровизации бизнес-процессов, обеспечения информационного взаимодействия и иных сервисных функций;

16) прикладной программный интерфейс (Application programming interface, далее – API) – набор правил и протоколов для взаимодействия программных компонентов цифровых систем друг с другом;

17) протокол прикладного уровня Hyper Text Transfer Protocol (далее – HTTP) — протокол, обеспечивающий взаимодействие между клиентом и сервером посредством передачи гипертекстовых документов в формате HTML;

18) единая транспортная среда государственных органов (далее – ЕТС ГО) – сеть телекоммуникаций, входящая в инфраструктуру "цифрового правительства" и предназначенная для обеспечения взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету), ведомственных и корпоративных

сетей телекоммуникаций государственных органов, их подведомственных организаций и органов местного самоуправления, а также иных субъектов цифровой среды, определенных уполномоченным органом, с соблюдением требуемого уровня кибербезопасности;

19) простой протокол доступа к объектам (SimpleObjectAccessProtocol, далее – SOAP) – протокол, основанный на XML для передачи сообщений при интеграции цифровых систем;

20) паспорт сервиса – веб-страница конкретного сервиса, содержащая сведения о контактах ответственных лиц собственника или владельца, сопровождающей организации (при ее наличии) и разработчика сервиса, назначении, функциональных возможностях, технических характеристиках, режимах взаимодействия, условиях информационного обмена, подключения и иных параметрах интеграционного сервиса или прикладного программного сервиса, обеспечивающий информирование инициаторов интеграционного взаимодействия и участников интеграционной архитектуры об условиях, и стандартах к использованию данного сервиса;

21) реестр сервисов – перечень зарегистрированных интеграционных и прикладных программных сервисов на цифровой платформе "Smart Bridge";

22) интеграционный сервис уведомительного характера – способ информационного взаимодействия цифровых объектов, с направлением уведомления собственнику или владельцу интеграционного сервиса о начале мероприятий по интеграции цифровых объектов;

23) уполномоченный орган в сфере цифровизации (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере цифровизации;

24) цифровая система – функционально связанный комплекс цифровых ресурсов, использующий объекты цифровой инфраструктуры с целью обеспечения создания, сбора, обработки, хранения и распространения цифровых данных, а также автоматизирующий взаимодействие субъектов цифровой среды и (или) обеспечивающий оказание услуг в цифровой среде;

25) цифровой объект – обособленный элемент цифровой среды, созданный, используемый или передаваемый посредством цифровых технологий, обладающий уникальными цифровыми характеристиками и позволяющий субъектам цифровой среды осуществлять правомочия владения, пользования либо распоряжения в объеме, установленном законодательством Республики Казахстан;

26) интеграция цифровых объектов – мероприятия по организации и обеспечению взаимодействия между цифровыми объектами посредством интеграционных сервисов с использованием стандартных протоколов передачи данных;

27) журнал цифровых событий – файлы, содержащие информацию о работе системы, используемую для мониторинга ее работы и выявления причин, в случае возникновения сбоя;

28) модуль идентификации и аутентификации Identity Provider веб-портала "цифрового правительства" – специализированный модуль, обеспечивающий централизованную аутентификацию пользователей, а также подключение внешних систем через механизмы единого входа;

29) оператор "цифрового правительства" (далее – оператор) – юридическое лицо, определяемое Правительством Республики Казахстан, обеспечивающее функционирование цифровых объектов "цифрового правительства";

30) внешний шлюз "цифрового правительства" (далее – ВШЦП) – подсистема шлюза "цифрового правительства", предназначенная для обеспечения взаимодействия цифровых объектов, находящихся в ЕТС ГО, с цифровыми объектами, находящимися вне ЕТС ГО;

31) платежный шлюз "цифрового правительства" – цифровой объект, автоматизирующий процессы передачи информации о проведении платежей в рамках оказания возмездных услуг;

32) цифровые объекты "цифрового правительства" – цифровые объекты государственных органов и иных лиц, предназначенные для осуществления деятельности государственных органов, выполнения государственных функций и оказания государственных услуг;

33) шлюз "цифрового правительства" (далее – ШЦП) – цифровой объект, предназначенный для интеграции цифровых объектов "цифрового правительства" с иными цифровыми объектами;

34) электронная цифровая подпись (далее – ЭЦП) – цифровая запись (набор цифровых данных), созданная с использованием закрытого ключа электронной цифровой подписи и средств электронной цифровой подписи, подтверждающая достоверность электронного документа, его принадлежность и неизменность содержания;

35) электронное сообщение (далее – сообщение) – электронный документ в формате XML, JSON, предназначенный для обмена информацией между цифровыми объектами;

36) формат Java Script Object Notation (далее – JSON) – текстовый формат обмена данными, основанный на JavaScript;

37) механизм взаимной аутентификации mTLS – механизм защиты сетевого взаимодействия, при котором подлинность обеих сторон соединения подтверждается посредством взаимной проверки цифровых сертификатов с использованием протокола TLS 1.2 и выше;

38) стиль архитектуры программного обеспечения Representational State Transfer (далее – REST) – согласованный набор ограничений, учитываемых при проектировании

распределенных цифровых систем или взаимодействия сервисов, использующий стандарты HTTP, URL, JSON и XML;

39) SSL-сертификат (Secure Sockets Layer) – регистрационное свидетельство, предназначенное для использования интернет-ресурсом или цифровой системой для обеспечения процедуры аутентификации;

40) цифровая платформа "Smart Bridge" (далее – Smart Bridge) – цифровой объект, предназначенный для публикации на нем интеграционных сервисов государственных и негосударственных цифровых объектов, прикладных программных сервисов с целью предоставления доступа к ним и (или) организации их взаимодействия;

41) протокол Transmission Control Protocol (далее – TCP) – протокол транспортного уровня стека TCP/IP, обеспечивающий надежную передачу сетевых пакетов в компьютерной сети между отправителем и получателем через предварительно установленное между ними соединение и контроль потока передаваемых сетевых пакетов;

42) указатель ресурса Uniform Resource Locator (далее – URL) – унифицированный указатель ресурса в сети Интернет;

43) протокол User Datagram Protocol (далее – UDP) – протокол транспортного уровня стека TCP/IP, обеспечивающий передачу автономных датаграмм в компьютерной сети между отправителем и получателем без гарантий их доставки;

44) логическая сеть Virtual Private Network (далее – VPN) – сеть, использующая технологию виртуализацию для расширения IP-адреса в публичной телекоммуникационной сети с помощью шифрования и туннелирования;

45) X.509 сертификат – цифровой сертификат, используемый для аутентификации, шифрования и обеспечения целостности данных при взаимодействии цифровых объектов;

46) XSD-схема (XML Schema Definition) – язык описания структуры XML-документа, определяющий правила, которым должен соответствовать XML-файл.

3. Интеграция цифровых объектов осуществляется посредством ШЦП и (или) ВШЦП, за исключением:

1) сервисов, предоставляемых удостоверяющими центрами, кроме интеграционного взаимодействия цифровых объектов внутри контура ЕТС ГО;

2) цифровых объектов, содержащих сведения, составляющие государственные секреты Республики Казахстан и служебную информацию с пометкой "Для служебного пользования";

3) цифровых объектов, размещенных на платформе "цифрового правительства" и предназначенных для формирования единого пространства данных для целей предоставления аналитической информации по деятельности государственных органов Республики Казахстан;

4) цифровых объектов, размещенных на платформе "цифрового правительства" и предназначенных для осуществления налогового и таможенного администрирования в соответствии с налоговым и таможенным законодательством Республики Казахстан;

5) цифровых объектов, получающих от государственных органов, воинских формирований, воинских частей и воинских организаций информации, необходимой для выполнения задач, возложенных на органы национальной безопасности;

6) сервисов по предоставлению открытых данных посредством OpenAPI, API, с использованием форматов XML, JSON и протоколов HTTP и HTTPS, посредством архитектурного стиля REST, включая интернет-порталы открытых данных, открытых бюджетов и открытых нормативных правовых актов;

7) информационного взаимодействия между веб-порталом "цифрового правительства" и мобильным приложением "цифрового правительства" в рамках оказания государственных и иных услуг в электронной форме;

8) модуля идентификации и аутентификации Identity Provider веб-портала "цифрового правительства".

4. Интеграция негосударственных цифровых объектов с цифровыми объектами "цифрового правительства" осуществляется на возмездной основе с заключением договора на оказание услуг с оператором, за исключением случаев, когда интеграция цифровых объектов "цифрового правительства" установлена законодательством Республики Казахстан.

При отсутствии заключенного договора, оператор приостанавливает подключение инициатора интеграционного сервиса к интеграционному сервису до заключения договора на оказание возмездных услуг с оператором.

5. При интеграции негосударственных цифровых объектов с государственными цифровыми объектами собственники и (или) владельцы цифровых систем заключают договор совместных работ по кибербезопасности.

6. Интеграция цифровых объектов осуществляется посредством Smart Bridge с учетом форматов данных веб-сервисов SOAP, указанных в приложении 1 к настоящим Правилам.

7. Заявки и документы на интеграцию цифровых объектов удостоверяются ЭЦП уполномоченных лиц участников интеграционного взаимодействия.

8. Интеграция цифровых объектов осуществляется при условии наличия интеграционного сервиса или прикладного программного сервиса в реестре сервисов.

9. Оператор осуществляет разработку и (или) публикацию интеграционного и (или) прикладного программного сервиса, а также актуализирует или исключает их из реестра сервисов по запросу собственника или владельца интеграционного сервиса или уполномоченного органа, составленного в произвольной форме, с уведомлением уполномоченного органа и архитектурно-координационного центра.

10. При неиспользовании государственного интеграционного сервиса инициатором интеграционного сервиса, оператор в течение десяти рабочих дней отключает его от сервиса, содержащего персональные данные и конфиденциальную информацию, по запросу уполномоченного органа и (или) собственника или владельца интеграционного сервиса, и (или) архитектурно-координационного центра с уведомлением уполномоченного органа.

11. При оказании возмездных услуг в цифровой форме цифровой объект автоматически направляет информацию о проведенном платеже в платежный шлюз "цифрового правительства" для его фиксации.

12. К заявке на подключение к интеграционному сервису или на публикацию интеграционного сервиса прикладываются протоколы испытаний с положительным результатом испытаний на соответствие требованиям кибербезопасности, выданных не более чем за три года до подключения, при отнесении цифровой системы инициатора интеграционного сервиса к цифровым объектам, указанным в пункте 2 статьи 49 Закона "О кибербезопасности".

Глава 2. Порядок интеграции цифровых объектов "цифрового правительства"

Параграф 1. Порядок публикации интеграционного сервиса на Smart Bridge по инициативе инициатора интеграционного сервиса

13. Для публикации интеграционного сервиса в реестре сервисов инициатор интеграционного сервиса направляет посредством Smart Bridge запрос об определении собственника или владельца цифрового объекта, в котором содержатся необходимые сведения, архитектурно-координационному центру.

14. При получении уведомления о поступлении запроса архитектурно-координационный центр рассматривает его в течение двух рабочих дней и предоставляет инициатору интеграционного сервиса:

- 1) подтверждение и информацию о собственнике или владельце цифрового объекта, а также рекомендации по разработке интеграционного сервиса в рамках архитектуры "цифрового правительства";
- 2) мотивированный отказ.

15. Инициатор интеграционного сервиса, при подтверждении архитектурно-координационного центра, авторизуется на Smart Bridge и направляет заявку на создание интеграционного сервиса в произвольной форме собственнику или владельцу цифрового объекта.

16. Собственник или владелец цифрового объекта рассматривает заявку на создание интеграционного сервиса в течение двух рабочих дней после ее поступления. По результатам рассмотрения собственник или владелец цифрового объекта:

- 1) согласовывает заявку на создание интеграционного сервиса;

- 2) возвращает ее на доработку инициатору интеграционного сервиса;
- 3) отказывает в создании интеграционного сервиса с указанием причин.

17. При согласовании заявки на создание интеграционного сервиса, собственник или владелец цифрового объекта заполняет заявку на публикацию интеграционного сервиса на цифровой платформе "Smart Bridge" согласно приложению 2 к настоящим Правилам (далее – заявка на публикацию интеграционного сервиса), с уведомлением инициатора интеграционного сервиса и уполномоченного органа.

18. При возврате заявки на создание интеграционного сервиса собственником или владельцем цифрового объекта на доработку, инициатор интеграционного сервиса в течение двух рабочих дней дорабатывает данную заявку и повторно направляет на рассмотрение собственнику или владельцу цифрового объекта.

19. При отказе собственником или владельцем цифрового объекта в создании интеграционного сервиса, мероприятия по его публикации прекращаются.

20. При поступлении заявки на публикацию интеграционного сервиса оператором осуществляется ее проверка на полноту и правильность заполнения в течение трех рабочих дней. При отрицательном результате проверки, оператор направляет заявку на публикацию интеграционного сервиса на доработку с указанием причин.

21. Собственник или владелец цифрового объекта в течение двух рабочих дней дорабатывает заявку на публикацию интеграционного сервиса и направляет согласованную собственником или владельцем цифрового объекта заявку на публикацию интеграционного сервиса оператору.

22. При положительном результате проверки заявки на публикацию интеграционного сервиса, оператор в течение десяти рабочих дней предоставляет инициатору интеграционного сервиса доступ к тестовой среде ШЦП, ВШЦП и подключает его для проведения тестирования интеграции.

23. Разработчики интеграционного сервиса со стороны собственника или владельца цифрового объекта, инициатора интеграционного сервиса вносят изменения в цифровые объекты для проведения тестирования по их интеграции.

24. Разработчики интеграционного сервиса со стороны собственника или владельца цифрового объекта, инициатор интеграционного сервиса и оператор проводят тестирование интеграционного сервиса в срок не более трех месяцев до получения положительного результата.

25. Со стороны ШЦП, ВШЦП подтверждением реализации интеграционного сервиса является передача сообщений (для асинхронного сервиса – получение отправителем уникального идентификатора сообщения, для синхронного – получение ответного сообщения) между участниками взаимодействия, фиксируемых в журнале событий ШЦП.

26. Со стороны участников интеграционного взаимодействия подтверждением реализации интеграционного сервиса является выполнение условий взаимодействия и обработка данных участниками взаимодействия.

27. При положительном результате тестирования интеграционного сервиса собственник или владелец интеграционного сервиса формирует акт тестирования и ввода в эксплуатацию интеграционного сервиса согласно приложению 3 к настоящим Правилам (далее – акт тестирования и ввода в эксплуатацию), удостоверяет его своей ЭЦП и направляет ее на согласование инициатору интеграционного сервиса.

При отрицательном результате тестирования интеграции продолжается до получения положительного результата.

28. Инициатор интеграционного сервиса при получении заявки на публикацию интеграционного сервиса и акта тестирования и ввода в эксплуатацию в течение трех рабочих дней согласовывает акт тестирования и ввода в эксплуатацию, удостоверив его своей ЭЦП, и направляет его на согласование оператору.

29. Оператор рассматривает акт тестирования и ввода в эксплуатацию в течение трех рабочих дней с момента получения заявки на публикацию интеграционного сервиса и акта тестирования.

30. При отрицательном результате проверки оператор возвращает акт тестирования и ввода в эксплуатацию на доработку собственнику или владельцу интеграционного сервиса. Собственник или владелец интеграционного сервиса в срок не более трех рабочих дней осуществляет доработку акта тестирования и повторно направляет его на рассмотрение инициатору интеграционного сервиса.

31. При положительном результате проверки акта тестирования оператор согласовывает акт тестирования и ввода в эксплуатацию, в течение десяти рабочих дней публикует паспорт сервиса на Smart Bridge и предоставляет инициатору интеграционного сервиса доступ к интеграционному сервису на промышленной среде ИШЦП, ВШЦП. Уполномоченный орган и архитектурно-координационный центр уведомляются о публикации интеграционного сервиса посредством личного кабинета Smart Bridge.

Параграф 2. Порядок публикации интеграционного сервиса на Smart Bridge по инициативе собственника или владельца цифрового объекта

32. Для публикации интеграционного сервиса в реестре сервисов собственник или владелец интеграционного сервиса запускает процесс по публикации интеграционного сервиса на Smart Bridge.

33. Собственник или владелец интеграционного сервиса заполняет требования к взаимодействию с интеграционным сервисом согласно приложению 4 к настоящим Правилам (далее – требования к взаимодействию с интеграционным сервисом) и заявку на публикацию интеграционного сервиса, принимает условия интеграции, с

приложением XSD-схемы, а также XML примеров запроса и ответа с тестовыми данными.

34. Оператор, получив уведомление о поступлении заявки на публикацию интеграционного сервиса, осуществляет проверку заявки на публикацию интеграционного сервиса и заявки на организацию сетевого доступа на полноту и правильность заполнения в течение трех рабочих дней.

При отрицательном результате проверки оператор направляет их на доработку с указанием причин.

35. При положительном результате проверки заявки на публикацию интеграционного сервиса оператор в течение десяти рабочих дней осуществляет публикацию в реестре сервисов и предоставляет собственнику или владельцу интеграционного сервиса доступ к тестовой и промышленной среде ШЦП, ВШЦП.

36. Уполномоченный орган и архитектурно-координационный центр уведомляются о публикации интеграционного сервиса посредством Smart Bridge.

37. При указании собственником или владельцем интеграционного сервиса, подключающегося к сервису собственника или владельца цифрового объекта, публикация интеграционного сервиса проводится в порядке, установленном пунктами 17-31 настоящих Правил.

Параграф 3. Порядок подключения к интеграционному сервису или к прикладному программному сервису

38. При наличии необходимого интеграционного сервиса в реестре сервисов на Smart Bridge инициатор интеграционного сервиса заполняет заявку на подключение к интеграционному сервису согласно приложению 5 к настоящим Правилам (далее – заявка на подключение к интеграционному сервису) и принимает условия интеграции.

39. Подключение к интеграционному сервису осуществляется с учетом требований к взаимодействию с интеграционным сервисом.

40. При использовании интеграционных сервисов собственниками или владельцами негосударственных цифровых систем для оказания государственных услуг, собственники или владельцы интеграционных сервисов заключают соглашение об использовании интеграционных сервисов собственниками или владельцами негосударственных цифровых систем для оказания государственных услуг согласно приложению 6 к настоящим Правилам с уполномоченным органом в сфере оказания государственных услуг на Smart Bridge.

41. При инициировании государственным органом заявки на подключение к интеграционному сервису государственного органа, заявка направляется на рассмотрение оператору. Собственнику или владельцу интеграционного сервиса направляется уведомление об инициировании заявки на подключение к интеграционному сервису на электронную почту и личный кабинет Smart Bridge.

42. При инициировании собственником или владельцем негосударственной цифровой системы заявки на подключение к интеграционному сервису, собственнику или владельцу интеграционного сервиса посредством Smart Bridge направляется уведомление о необходимости рассмотрения заявки на подключение к интеграционному сервису.

43. При подключении негосударственных цифровых систем к интеграционному сервису, в заявке на публикацию которого собственником или владельцем указано об отсутствии в нем персональных данных и наличии не менее 100 подключений к нему, данный интеграционный сервис считается сервисом уведомительного характера.

При инициировании заявки собственником или владельцем негосударственной цифровой системы на подключение к сервису уведомительного характера заявка направляется на рассмотрение оператору и собственнику или владельцу интеграционного сервиса посредством Smart Bridge.

44. Собственник или владелец интеграционного сервиса, получив уведомление о необходимости рассмотрения заявки на подключение к интеграционному сервису, в течение двух рабочих дней направляет ответ о согласии либо мотивированный отказ с указанием причин.

Отказ, не содержащий правовых или технических оснований, а также отказ, сводящийся к требованию совершения действий, не предусмотренных Правилами, признается немотивированным и не допускается.

45. При непредставлении ответа собственником или владельцем интеграционного сервиса в установленный срок, заявка на подключение к интеграционному сервису уведомительного характера считается согласованной.

46. После согласования заявки на подключение к интеграционному сервису оператор уведомляется о необходимости рассмотрения и согласования заявки посредством Smart Bridge.

47. После получения уведомления оператор в течение трех рабочих дней осуществляет проверку на полноту и правильность заполнения заявки на подключение к интеграционному сервису и при отсутствии замечаний согласовывает ее.

При отрицательном результате проверки заявки на подключение к интеграционному сервису, оператор направляет ее на доработку с указанием технических причин.

48. Инициатор интеграционного сервиса в течение трех рабочих дней осуществляет доработку заявки на подключение к интеграционному сервису и повторно направляет ее:

- 1) на рассмотрение оператору и на ознакомление собственнику или владельцу интеграционного сервиса в случае интеграции государственных цифровых систем;
- 2) на рассмотрение собственнику или владельцу интеграционного сервиса в случае интеграции негосударственных цифровых систем с государственными.

49. При согласовании заявки на подключение к интеграционному сервису оператор в течение десяти рабочих дней предоставляет собственнику или владельцу интеграционного сервиса, инициатору интеграционного сервиса доступ к тестовой среде ШЦП, ВШЦП для проведения тестирования интеграционного сервиса до получения положительного результата в срок не более трех месяцев.

50. Со стороны ШЦП, ВШЦП подтверждением реализации интеграционного сервиса является передача сообщений (для асинхронного сервиса – получение отправителем уникального идентификатора сообщения, для синхронного – получение ответного сообщения) между участниками взаимодействия, фиксируемая в журнале событий ШЦП, ВШЦП.

51. Со стороны собственника или владельца интеграционного сервиса и инициатора интеграционного сервиса подтверждением реализации интеграционного сервиса является выполнение условий взаимодействия и обработка данных.

52. При положительном результате тестирования интеграционного сервиса инициатор интеграционного сервиса формирует акт тестирования и ввода в эксплуатацию, удостоверяет его своей ЭЦП и направляет его на согласование собственнику или владельцу интеграционного сервиса.

При отрицательном результате тестирования интеграционного сервиса продолжается до получения положительного результата.

53. Собственник или владелец интеграционного сервиса при получении заявки на подключение к интеграционному сервису и акта тестирования и ввода в эксплуатацию в течение трех рабочих дней согласовывает его, удостоверив его своей ЭЦП и направляет на согласование оператору.

54. Оператор рассматривает акт тестирования и ввода в эксплуатацию в течение трех рабочих дней с момента его получения.

55. При отрицательном результате проверки оператор возвращает акт тестирования и ввода в эксплуатацию на доработку инициатору интеграционного сервиса. Инициатор интеграционного сервиса в срок не более трех рабочих дней осуществляет его доработку и повторно направляет на рассмотрение собственнику или владельцу интеграционного сервиса.

56. При положительном результате проверки акта тестирования и ввода в эксплуатацию оператор согласовывает его и в течение десяти рабочих дней предоставляет инициатору интеграционного сервиса доступ к интеграционному сервису в среде промышленной эксплуатации ШЦП, ВШЦП. Уполномоченный орган и архитектурно-координационный центр уведомляются о подключении инициатора интеграционного сервиса к интеграционному сервису посредством Smart Bridge.

57. При наличии в интеграционном сервисе персональных данных интеграция производится с использованием государственного сервиса контроля доступа к персональным данным в соответствии с Правилами интеграции с государственным

сервисом контроля доступа к персональным данным, утвержденными приказом исполняющим обязанности Министра цифрового развития инноваций и аэрокосмической промышленности Республики Казахстан от 8 июля 2022 года № 236/НК (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 28786).

58. При подключении к интеграционным сервисам, осуществляющим обработку и предоставление персональных данных, со стороны ШЦП выполняется проверка токена верификации. При отсутствии токена верификации либо неуспешной его проверки, инициатору интеграционного сервиса не предоставляется доступ к нему с направлением уведомления с указанием причины отказа.

59. При наличии необходимого прикладного программного сервиса в реестре сервисов на Smart Bridge инициатор подключения к прикладному программному сервису заполняет заявку на его подключение и принимает условия подключения.

60. Заявка направляется на рассмотрение собственнику или владельцу прикладного программного сервиса посредством Smart Bridge.

61. Собственник или владелец прикладного программного сервиса при получении заявки на подключение к прикладному программному сервису в течение трех рабочих дней согласовывает его и направляет на согласование оператору или направляет мотивированный отказ с указанием причин.

Отказ, не содержащий правовых или технических оснований, а также отказ, сводящийся к требованию совершения действий, не предусмотренных Правилами, признается немотивированным и не допускается.

62. При согласовании заявки на подключение к прикладному программному сервису оператор в течение десяти рабочих дней предоставляет инициатору подключения к прикладному программному сервису доступ к тестовой среде для проведения тестирования прикладного программного сервиса до получения положительного результата в срок не более двух месяцев.

63. При положительном результате тестирования оператор в течение десяти рабочих дней предоставляет инициатору подключения к прикладному программному сервису доступа к нему в среде промышленной эксплуатации.

Параграф 4. Порядок актуализации интеграционного сервиса

64. Собственник или владелец интеграционного сервиса инициирует актуализацию интеграционного сервиса в случае изменения условий функционирования интеграционного сервиса или по запросу инициатора интеграционного сервиса.

65. Актуализация интеграционного сервиса осуществляется собственником или владельцем интеграционного сервиса после его авторизации на Smart Bridge путем

подачи оператору заявки на актуализацию интеграционного сервиса по форме согласно приложению 7 к настоящим Правилам (далее – заявка на актуализацию интеграционного сервиса).

66. Оператор, получив уведомление о поступлении заявки на актуализацию интеграционного сервиса, осуществляет ее проверку на полноту и правильность заполнения в течение трех рабочих дней.

При отрицательном результате проверки заявки на актуализацию интеграционного сервиса, оператор направляет ее на доработку с указанием причин.

При положительном результате проверки заявки на актуализацию интеграционного сервиса оператор в течение десяти рабочих дней осуществляет актуализацию интеграционного сервиса.

Параграф 5. Порядок актуализации подключения к интеграционному сервису

67. При изменении условий функционирования подключения к интеграционному сервису инициатор интеграционного сервиса актуализирует подключение к нему.

68. Актуализация подключения к интеграционному сервису осуществляется инициатором интеграционного сервиса путем подачи оператору заявки на актуализацию подключения к интеграционному сервису по форме согласно приложению 8 к настоящим Правилам (далее – заявка на актуализацию подключения к интеграционному сервису) посредством Smart Bridge.

69. Оператор, получив уведомление о поступлении заявки на актуализацию подключения к интеграционному сервису, осуществляет ее проверку на полноту и правильность заполнения в течение трех рабочих дней.

При отрицательном результате проверки, оператор направляет заявку на актуализацию интеграционного сервиса на доработку с указанием причин.

При положительном результате проверки оператор в течение десяти рабочих дней осуществляет актуализацию подключения к интеграционному сервису.

Глава 3. Обеспечение эксплуатации и защиты интеграционного сервиса и прикладного программного сервиса

70. Интеграционные сервисы и прикладные программные сервисы размещаются на цифровой инфраструктуре, находящейся на территории Республики Казахстан.

71. ШЦП и ВШЦП обеспечивают передачу интеграционных сервисов и прикладных программных сервисов в круглосуточном режиме на постоянной основе за исключением технологических перерывов.

Время принятия сообщения ШЦП, ВШЦП не должно превышать одной минуты с момента его получения по универсальному синхронному каналу и асинхронному каналу.

72. Технологические перерывы в работах цифровых объектов инициатора интеграционного сервиса и собственника или владельца интеграционного сервиса или прикладного программного сервиса заранее оговариваются и согласовываются между ними и оператором за три рабочих дня до начала их проведения. Технологические перерывы должны приходиться на ночное время с 21:00 до 6:00 часов, а также в выходные и праздничные дни.

73. С целью проведения тестирования участниками взаимодействия обеспечивается работоспособность тестовой среды цифровых объектов.

74. При возникновении технической ошибки оператор и (или) собственник или владелец интеграционного сервиса и (или) инициатор интеграционного сервиса осуществляет перезагрузку цифрового объекта и уведомляют о времени проведения технических работ администраторов других цифровых объектов, в виде телефонограммы или по электронной почте.

75. При непринятии мер по исправлению возникших технических ошибок собственником или владельцем интеграционного сервиса или прикладного программного сервиса и (или) инициатором интеграционного сервиса оператор в течение трех рабочих дней отключает или приостанавливает соответствующий интеграционный сервис или прикладной программный сервис с уведомлением о временной недоступности сервиса.

76. При неисправности или проведении операторами связи плановых профилактических работ на каналах связи, обеспечивающих передачу интеграционного сервиса или прикладного программного сервиса, срок проведения технических работ определяется регламентом оператора связи.

77. При реализации интеграционного сервиса обеспечивается защита передаваемой информации путем:

1) использования механизмов контроля целостности и достоверности информации, в том числе подтверждением авторства, подписанных ЭЦП XML сообщений;

2) авторизации инициатора интеграционного сервиса и собственника или владельца интеграционного сервиса или прикладного программного сервиса на ШЦП, ВШЦП по логину и паролю, выдаваемыми оператором, по транспортной подписи или механизму взаимной аутентификации mTLS. Для интеграционных сервисов, реализованных в стиле архитектуры распределенных систем (REST) авторизация осуществляется по логину и паролю совместно с механизмом взаимной аутентификации mTLS;

3) журналированием событий, связанных с передачей интеграционного сервиса на ШЦП, ВШЦП.

78. Подтверждением авторства сообщений является положительный результат проверки соответствия транспортной подписи регистрационным свидетельством ЭЦП собственника или владельца интеграционного сервиса или прикладного программного сервиса и (или) инициатора интеграционного сервиса, направившего сообщение.

82. Транспортная подпись проверяется на ШЦП при вызове интеграционного сервиса по сценарию использования транспортной подписи согласно приложению 9 к настоящим Правилам и включают проверку принадлежности ЭЦП отправителю сообщения и проверку действительности ЭЦП.

86. При временном отключении интеграционного сервиса или прикладного программного сервиса, вызванного модификацией и (или) модификацией цифрового объекта, предоставляющего доступ к интеграционному сервису, собственник или владелец интеграционного сервиса или прикладного программного сервиса уведомляет уполномоченный орган и всех инициаторов интеграционного сервиса или прикладного программного сервиса посредством Smart Bridge за три рабочих дня до начала его отключения.

При прекращении работы интеграционного сервиса или прикладного программного сервиса, его собственник или владелец уведомляет уполномоченный орган и всех инициаторов интеграционного сервиса посредством Smart Bridge за один месяц до прекращения работы.

87. Собственник или владелец интеграционного сервиса и инициатор интеграционного сервиса определяют ответственных лиц, обеспечивающих кибербезопасность и постоянную готовность программных и технических средств и при изменении их состава, производят взаимное информирование об имеющихся изменениях, и сообщают новые сведения об ответственных лицах в течение семи рабочих дней.

92. При поступлении отзыва на Smart Bridge инициаторов интеграционного сервиса о неактуальности сведений, размещенных в паспорте сервиса, система фиксирует соответствующий статус. Собственник или владелец интеграционного сервиса обязан актуализировать сведения в срок не более одного месяца со дня поступления отзыва.

Приложение 1
к Правилам интеграции
цифровых объектов "цифрового
правительства"

Форматы данных веб-сервисов SOAP

1. Описание сообщений асинхронного канала:

1.1. интерфейс интеграционного сервиса на стороне шлюза "цифрового правительства" (далее – ШЦП) и внешнего шлюза "цифрового правительства" (далее – ВШЦП).

Используется метод отправки сообщений на асинхронный канал ШЦП, ВШЦП SendMessage.

Запрос на предоставление сервиса (SendMessageRequest) содержит следующие поля : Формат данных SendMessageRequest

--	--	--	--

Поле	Тип	Обязательность заполнения	Описание
request	AsyncSendMessageRequest	Да	Запрос
messageInfo	AsyncMessageInfo	Да	Метаданные сообщения
messageId	xsd: string	Да	Идентификатор сообщения в системе владельца интеграционного сервиса (формируется системой)
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения в системе владельца интеграционного сервиса (при существовании сообщения в рамках цепочки сообщений системы (отправителя) формируется системой владельца)
serviceId	xsd: string	Да	Идентификатор сервиса
messageType	xsd: string	Да	Тип сообщения: REQUEST – первое сообщения взаимодействия
routeId	xsd: string	Нет	Идентификатор маршрута сообщения (при необходимости в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя)
messageDate	xsd: dateTime	Да	Дата создания сообщения
sessionId	guid	Да	Идентификатор сессии ШЦП. Заполняется на ШЦП, не заполняется отправителем
sender	SenderInfo	Да	Объект "информация об отправителе" (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Да	Пароль отправителя
properties	property	Нет	Массив свойств, в которых указаны дополнительные свойства запроса по согласованию с ШЦП, системой

			получателя и отправителя.
Key	xsd: int		Ключ свойства
value	xsd: int	Нет	Значение свойства
messageData	messagedata	Да	Объект передачи данных
data	xsd: Anytype	Нет	Объект "данные сообщения"

Ответ ШЦП, ВШЦП на сообщение SendMessageResponse представляет собой массив элементов со следующими полями: Формат данных SendMessageResponse

Поле	Тип	Обязательность заполнения	Описание
response	AsyncSendMessageRequest	Да	Ответ
messageId	xsd: string	Да	Идентификатор сообщения
correlationId	xsd: string	Да	Идентификатор цепочки сообщения
responseDate	xsd: dateTime	Да	Дата ответа
sessionId	Guid	Нет	Идентификатор сессии ШЦП

Ответ об ошибке SendMessageFault представляет собой массив элементов со следующими полями: Формат данных SendMessageFault

Поле	Тип	Обязательность заполнения	Описание
ErrorInfo	ErrorInfo		Информация об ошибке
errorCode	xsd: string	Да	Код ошибки
errorData	xsd: string	Да	Дополнительное описание ошибки
errorDate	xsd: dateTime	Да	Дата ошибки
subError	ErrorInfo	Нет	Дочерняя ошибка
sessionId	guid	Нет	Идентификатор сессии в которой произошла ошибка

1.2. Интерфейс для реализации интеграционного сервиса на стороне пользователей ШЦП, ВШЦП для работы с асинхронным каналом.

Сервис реализуется на стороне владельца или инициатора интеграционного сервиса . Сервис реализуют в случае необходимости доставки ШЦП сообщений методом вызова сервиса получателя сообщения (PUSH).

Используется метод отправки сообщений SendMessage.

Запрос на предоставление сообщения SendMessageRequest содержит следующие поля: Формат данных SendMessageRequest

Поле	Тип	Обязательность заполнения	Описание
request	AsyncSendMessageRequest	Да	

messageInfo	Async SendMessageInfo	Да	Мета данные сообщения
messageId	xsd: string	Да	Идентификатор сообщения. Генерируется ШЦП. В случае отправки сообщения на ШЦП данное поле остается пустым. В случае передачи сообщения получателю номер будет проставлен ШЦП.
correlationId	xsd: string	Нет	Идентификатор цепочки сообщений. Генерируется ШЦП. В случае отправки сообщения типа REQUEST на ШЦП данное поле остается пустым. При отправке сообщений других типов на ШЦП, данное поле заполняется в обязательном порядке. В случае передачи сообщения получателю номер будет проставлен ШЦП.
serviceId	xsd: string	Да	Идентификатор взаимодействия. По реестру сервисов ШЦП.
messageType	xsd: string	Да	Тип сообщения: REQUEST - первое сообщения взаимодействия
routeId	xsd: string	Нет	Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя)
messageDate	xsd: dateTime	Да	Дата создания сообщения
sessionId	guid	Нет	Идентификатор сессии ШЦП. Заполняется на ШЦП, отправителю заполнять не надо.
sender	SenderInfo	Да	Объект "информация об отправителе"
senderId	xsd: string	Да	Идентификатор системы отправителя
password	xsd: string	Нет	Пароль отправителя

properties	Property	Нет	Массив, определяющий дополнительные свойства запроса по согласованию с ШЦП, системой получателя и отправителя.
key	xsd: int	Да	Ключ свойства
value	xsd: int	Да	Значение свойства
messageData	messageData	Да	Объект передачи данных
data	xsd: Anytype	Да	Объект "данные сообщения"

Ответ ШЦП на сообщение SendMessageResponse представляет собой массив элементов со следующими полями: Формат данных SendMessageResponse

Поле	Тип	Обязательность заполнения	Описание
response	AsyncSendMessageResponse	Да	Ответ
messageId	xsd: string	Да	Идентификатор сообщения
correlationId	xsd: string	Да	Идентификатор цепочки сообщения
responseDate	xsd: dateTime	Да	Дата ответа
sessionId	guid	Нет	Идентификатор сессии ШЦП

Ответ об ошибке SendMessageFault представляет собой массив элементов со следующими полями: Формат данных SendMessageFault

Поле	Тип	Обязательность заполнения	Описание
ErrorInfo	ErrorInfo		Информация об ошибке
errorCode	xsd: string	Да	Код ошибки
errorData	xsd: string	Да	Дополнительное описание ошибки
errorDate	xsd: dateTime	Да	Дата ошибки
subError	ErrorInfo	Нет	Дочерняя ошибка
sessionId	guid	Нет	Идентификатор сессии в которой произошла ошибка

2. Описание сообщений синхронного канала

2.1. Интерфейс интеграционного сервиса на стороне ШЦП:

Используется метод отправки сообщений по синхронному каналу SendMessage.

Запрос на предоставление сервиса SendMessageRequest представляет собой массив элементов со следующими полями: Формат сообщения типа SendMessageRequest

Поле	Тип	Обязательность заполнения	Описание
request	SyncSendMessageRequest	Да	Запрос

requestInfo	SyncMessageInfo	Да	Информация о сообщении запроса
messageId	xsd: string	Да	Идентификатор сообщения в системе получателя (генерирует ШЦП)
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения в системе получателя запроса (генерирует ШЦП)
serviceid	xsd: string	Да	Идентификатор взаимодействия (ведется в реестре сервисов ШЦП)
messegeDate	xsd: dateTime	Да	Дата создания сообщения в системе инициатора интеграционного сервиса (Заполняется системой).
routeId	xsd: string	Нет	Идентификатор маршрута сообщения (при необходимости в дополнительной маршрутизации, идентификатор по реестру, заполняется системой инициатора интеграционного сервиса)
sessionId	guid	Нет	Идентификатор сессии на ШЦП. Устанавливается на ШЦП.
sender	senderinfo	Да	Информация об отправителе (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Да	Пароль отправителя
properties	property	Нет	Массив, определяющий дополнительные свойства запроса по согласованию с ШЦП, системой получателя и отправителя.
key	xsd: string		Ключ свойства
value	xsd: string		Значение свойства
requestData	requestData	Да	Объект передачи данных запроса
data	xsd: Anytype	Нет	Данные сообщения (формат определяется

		системой получателя сообщения)
--	--	--------------------------------

Ответное сообщение на запрос SendMessageResponse представляет собой массив элементов со следующими полями: Формат сообщения типа SendMessageResponse

Поле	Тип	Обязательность заполнения	Описание
response	SyncSendMessageResponse	Да	Ответ
responseInfo	SyncMessageInfoResponse	Да	Информация об ответе
messageId	xsd: string	Да	Идентификатор сообщения в системе получателя (генерирует система владельца интеграционного сервиса)
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения в системе получателя запроса (при существовании сообщения в рамках цепочки сообщений системы отправителя, генерирует система владельца интеграционного сервиса)
responseDate	xsd: dateTime	Да	Дата ответа в системе владельца интеграционного сервиса (заполняется системой владельца интеграционного сервиса)
sessionId	guid	Нет	Идентификатор сессии на ШЦП. Устанавливается на ШЦП. Не заполняется при отправке ответа системой владельца интеграционного сервиса .
status	StatusInfo	Да	Объект "Информация о статусе"
code	xsd: int	Да	Код статуса (проставляется системой получателя запроса)
message	xsd: string	Да	Сообщение о статусе
responseData	responsedata	Да	Объект "данные ответа"
data	xsd: Anytype	Нет	Объект данные сообщения (формат определяется системой владельца

			интеграционного сервиса)
--	--	--	------------------------------

Сообщение об ошибке SendMessageFault1_SendMessageFault представляет собой массив элементов со следующими полями: Формат сообщения типа SendMessageFault

Поле	Тип	Обязательность заполнения	Описание
errorCode	xsd: string	Да	Код ошибки
errorMessage	xsd: string	Да	Сообщение ошибки
errorData	xsd: string	Нет	Дополнительное описание ошибки
errorDate	xsd: dateTime	Нет	Дата ошибки
subError	ErrorInfo	Нет	Дочерняя ошибка
sessionId	Guid	Нет	Идентификатор сессии в которой произошла ошибка

Форматы данных сервисов REST

Запрос на предоставление сервиса представляет собой массив элементов со следующими полями:

Поле	Тип	Обязательность заполнения	Описание
request	SyncsendMessagerequest	Да	Запрос
requestInfo	SyncMessageInfo	Да	Информация о сообщении запроса
messageId	xsd: string	Да	Идентификатор сообщения в системе владельца интеграционного сервиса (генерирует ШЦП)
serviceid	xsd: string	Да	Идентификатор взаимодействия (ведется в реестре сервисов ШЦП)
messegeDate	dateTime	Да	Дата создания сообщения в системе инициатора интеграционного сервиса (заполняется владельцем интеграционного сервиса)
routeId	xsd: string	Нет	Идентификатор маршрута сообщения (при необходимости в дополнительной маршрутизации, идентификатор по реестру, заполняется системой владельца интеграционного сервиса)

sender	senderinfo	Да	Информация об отправителе (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Да	Пароль отправителя
requestData	requestData	Да	Объект передачи данных запроса
data	Anytype	Нет	Данные сообщения (формат определяется системой получателя сообщения)

Ответное сообщение на запрос представляет собой массив элементов со следующими полями:

Поле	Тип	Обязательность заполнения	Описание
response	SyncsendMessageresponse	Да	Ответ
responseInfo	SyncMessageInfoResponse	Да	Информация об ответе
messageId	xsd: string	Да	Идентификатор сообщения в системе владельца интеграционного сервиса (заполняет система владельца интеграционного сервиса)
responseDate	dateTime	Да	Дата ответа в системе владельца интеграционного сервиса (заполняется системой владельца интеграционного сервиса)
message	string	Да	Сообщение о статусе
responseData	responsedata	Да	Объект "данные ответа"
data	Anytype	Нет	Объект данные сообщения (формат определяется системой владельца интеграционного сервиса)

Приложение 2
к Правилам интеграции цифровых
объектов "цифрового
правительства"
Форма

Заявка на публикацию интеграционного сервиса на цифровой платформе "Smart bridge"

1. Общая информация	
2.	Наименование сервиса на русском языке
3.	Наименование сервиса на казахском языке
4.	Назначение сервиса на русском языке
5.	Назначение сервиса на казахском языке
6.	Должностное лицо, ответственное за эксплуатацию (на русском языке)
7.	Должностное лицо, ответственное за эксплуатацию (на казахском языке)
8.	Контактный телефон
9.	Контактный адрес электронной почты
10.	Контактные данные разработчика сервиса (на русском языке)
11.	Контактные данные разработчика сервиса (на казахском языке)
12.	Контактный телефон
13.	Контактный адрес электронной почты
14.	Наименование сопровождающей организации
15.	Теги
16.	Корневая категория сервиса
17.	Режим взаимодействия сервиса
18.	Формат сервиса
19.	Кому доступен сервис
20. Рекомендуемые требования по производительности и надежности	
21. Контролируемый показатель	
22.	Максимальное время обработки запроса (заполняется только для синхронных сервисов)
23.	Среднее время обработки запроса (заполняется только для синхронных сервисов)
24.	Пиковая нагрузка (максимальное допустимое количество принимаемых и обрабатываемых запросов)
25.	Номинальная нагрузка (оптимальное количество запросов в час)
26.	Среднее время работы без сбоев
27.	Время на восстановление работоспособности
28.	Требования по кибербезопасности Требования к формату журнала событий Требования со стороны шлюза "цифрового правительства" и (или) внешнего шлюза "цифрового правительства"
29.	Подтверждение о согласии с данными требованиями
30. Параметры сервиса	
31. Цифровая система владельца интеграционного сервиса	
32.	Наименование цифровой системы

33.	Логин системы
34.	Пароль (тестовая среда)
35.	Пароль (среда эксплуатации)
36.	Ключ сервиса
37.	Метод безопасности
38.	Сертификат открытого ключа транспортной подписи (.cer; .crt) (выданный Национальным удостоверяющим центром Республики Казахстан)
39.	Тип сертификата (общий/для тестовой среды/для среды эксплуатации)
40.	Протокол испытаний на кибербезопасность
41.	Схема информационного взаимодействия
42.	Признак наличия маршрутизации сообщений (да/нет)
43.	Сервис предоставляет персональные данные (да/нет)
44.	Сервис уведомительного характера (да/нет)
45.	Опубликовать сервис на внешнем шлюзе "цифрового правительства" (да/нет)
46.	Наименование URL сервиса, принимающего запросы (тестовая среда)
47.	Наименование URL сервиса, принимающего запросы (среда эксплуатации)
48.	URL сервиса, принимающего запросы (тестовая среда)
49.	URL сервиса, принимающего запросы (среда эксплуатации)
50.	SSL сертификат (.cer; .crt) (выданный Национальным удостоверяющим центром Республики Казахстан)
51.	Тип сертификата (общий/для тестовой среды/для среды эксплуатации)
52.	Авторизация на стороне сервиса (да/нет)
53.	Метод авторизации
54.	Логин
55.	Пароль
56.	Публикация с клиентом (да/нет)
57. Клиент сервиса	
58.	Наименование организации
59. Сетевые параметры и схемы сервиса	
60. Тестовая среда	
61.	В единой транспортной среде государственных органов (да/нет)
62.	Вне единой транспортной среды государственных органов (да/нет)

63.	Данные VPN-туннеля (общий/раздельный)
64.	Информация о шлюзе VPN
65.	Публичный Peer IP-адрес системы
66.	Имеется VPN-туннель для данной системы? (да/нет)
67.	Хостинг оператора "цифрового правительства" (да/нет)
68.	Публичный IP-адрес системы
69.	Порт
70.	Протокол
71. Среда эксплуатации	
72.	В единой транспортной среде государственных органов (да/нет)
73.	Вне единой транспортной среды государственных органов (да/нет)
74.	Данные VPN-туннеля (общий/раздельный)
75.	Информация о шлюзе VPN
76.	Публичный Peer IP-адрес системы
77.	Имеется VPN-туннель для данной системы? (да/нет)
78.	Хостинг оператора "цифрового правительства" (да/нет)
79.	Публичный IP-адрес системы
80.	Порт
81.	Протокол
82.	Схемы сервиса
83.	XSD (.zip)
84.	Пример запроса (.xml)
85.	Пример ответа (.xml)

Приложение 3
к Правилам интеграции цифровых
объектов "цифрового
правительства"

Акт тестирования и ввода в эксплуатацию интеграционного сервиса

1.	Участники информационного взаимодействия:
2.	Наименование владельца интеграционного сервиса:
3.	Наименование инициатора интеграционного сервиса:
4.	Цифровые системы:
5.	Цифровая система владельца интеграционного сервиса:
6.	Цифровая система инициатора интеграционного сервиса:
7.	Сервисы тестирования:
8.	Наименование сервиса:

9.	Ключ сервиса:
10.	Заключение:
11.	Сценарий тестирования:
12.	Решение по результатам тестирования:
13.	Протоколы испытаний на соответствие требованиям кибербезопасности:
14.	Дата перевода в промышленную среду:

Приложение 4
к Правилам интеграции
цифровых объектов "цифрового
правительства"
Форма

Требования к взаимодействию с интеграционным сервисом

Валидация X.509 сертификата включает в себе следующие проверки:

- 1) срок действия сертификата;
- 2) цепочки сертификатов;
- 3) на отозванность сертификата;
- 4) проверка бизнес-идентификационного номера организации на принадлежность.

Описание и форматы значений свойств и настроек объекта (далее – properties) в рамках взаимодействия с государственным сервисом контроля доступа к персональным данным.

Для взаимодействия с сервисами предоставляющие персональные данные, со стороны шлюза "цифрового правительства" осуществляется проверка токена верификации.

Отправителю необходимо указать два объекта properties в запросе.

Публичный ключ и сгенерированный токен верификации предоставляется государственным сервисом контроля доступа к персональным данным.

В случае неуспешной валидации публичного ключа и токена верификации, отправитель получит информативную ошибку от шлюза "цифрового правительства" и процесс отправки запроса прерывается.

Массив	Обязательное значение поля key	Тип поля key	Тип поля value	Обязательность	Описание
Properties	kdp_public_key	xsd: string	xsd: string	Да	Публичный ключ для доступа к данным в токене верификации
Properties	kdp_token	xsd: string	xsd: string	Да	Сгенерированный токен верификации

Требования по производительности и надежности синхронного сервиса

--	--	--

№	Контролируемый показатель	Ограничение
1	Максимальное время обработки запроса при синхронном взаимодействии	до 60 секунд
2	Среднее время обработки запроса	10 секунд
3.	Пиковая нагрузка	2000 запросов в секунду
4.	Номинальная нагрузка	1500 запросов в секунду
5	Среднее время работы без сбоев	365/7/24
6	Время на восстановление работоспособности	3 часа

Требования по производительности и надежности асинхронного сервиса

№	Контролируемый показатель	Ограничение
1	Максимальное время обработки запроса при асинхронном взаимодействии	Время предоставления результата по запросу на асинхронном сервисе, зависит от реализации каждого интеграционного сервиса
2	Пиковая нагрузка	100 запросов в секунду
3	Номинальная нагрузка	70 запросов в секунду
4	Среднее время работы без сбоев	365/7/24
5	Время на восстановление работоспособности	3 часа

Приложение 5
к Правилам интеграции
цифровых объектов "цифрового
правительства"
Форма

Заявка на подключение к интеграционному сервису

1. Владелец интеграционного сервиса	
2.	Наименование организации
3.	Индивидуальный идентификационный номер/ бизнес-идентификационный номер
4. Клиент интеграционного сервиса	
5.	Наименование организации
6.	Индивидуальный идентификационный номер/ бизнес-идентификационный номер
7.	Основание для подключения
8.	Файл основания для подключения
9.	Совместный приказ
10.	Приказ о пилотном проекте (да/нет)
10.1	Срок действия приказа о пилотном проекте
10.2	Файл пилотного приказа
11.	ФИО ответственного лица
12.	Контактный телефон ответственного лица

13.	Электронная почта ответственного лица
14. Цифровая система клиента	
15.	Наименование цифровой системы
16.	Логин системы
17.	Пароль (тестовая среда)
18.	Пароль (среда эксплуатации)
19.	Сертификат открытого ключа транспортной подписи цифровой системы (выданный национальным удостоверяющим центром Республики Казахстан)
20.	Протоколы испытаний на соответствие требованиям кибербезопасности (.doc, .docx, .pdf, заполняется при организации доступа к сервису на среде эксплуатации шлюза "цифрового правительства", внешнего шлюза "цифрового правительства")
21. Тестовая среда	
21.1	В единой транспортной среде государственных органов
21.2	Вне единой транспортной среды государственных органов
21.2.1	Данные VPN-туннеля
21.2.2	Информация о шлюзе VPN
21.2.3	Тип туннеля (общий/среда эксплуатации)
21.2.4	Публичный Peer IP-адрес системы
21.2.5	Имеется ли VPN-туннель для данной системы
21.3.	Хостинг оператора "цифрового правительства"
22. Продуктивная среда	
22.1	В единой транспортной среде государственных органов
22.2	Вне единой транспортной среды государственных органов
22.2.1	Данные VPN-туннеля
22.2.2	Информация о шлюзе VPN
22.2.3	Тип туннеля (общий/среда эксплуатации)
22.2.4	Публичный Peer IP-адрес системы
22.2.5	Имеется ли VPN-туннель для данной системы
22.3	Хостинг оператора "цифрового правительства"
23. Электронный сервис	
24.	Наименование сервиса
25.	Ключ сервиса
26.	Режим взаимодействия сервиса
27.	Формат сервиса
28.	Признак наличия маршрутизации сообщений
29.	Ключ маршрута

30.	Наименование URL сервиса, принимающего запросы (тестовая среда)
31.	URL сервиса, принимающего запросы (тестовая среда)
32.	Наименование URL сервиса, принимающего запросы (среда эксплуатации)
33.	URL сервиса, принимающего запросы (среда эксплуатации)
34.	SSL сертификат (выданный национальным удостоверяющим центром Республики Казахстан)
35.	Тип сертификата (общий/тестовая среда)

Приложение 6
к Правилам интеграции цифровых
объектов "цифрового
правительства"

Соглашение об использовании интеграционных сервисов собственниками или владельцами негосударственных цифровых систем для оказания государственных услуг

" ____ " _____ года
_____ (наименование государственного органа) (_____
_____) (наименование государственной услуги), далее именуемое "Сторона 1", с
одной стороны, и _____ (наименование организации), далее
именуемое "Сторона 2", и _____ (наименование
государственного органа), далее именуемое "Сторона 3", вместе именуемые "Стороны"
, заключили настоящее Соглашение об использовании интеграционных сервисов (далее
по тексту – Соглашение) о нижеследующем.

Глава 1. Область применения

1. Настоящее Соглашение определяет уровень обслуживания при использовании сервиса интеграции Стороны 1 в целях обеспечения доступности государственных услуг, предоставляемых в электронном виде, осуществления деятельности государственных органов и принятия обязательств Стороной 2 по бесперебойному предоставлению государственных услуг через внешние платформы. При этом, устанавливаются индексы доступности сервиса интеграции, а также Сторона 1 обеспечивает на этапе промышленной эксплуатации доступность сервиса интеграции в соответствии с установленным индексом доступности.

Глава 2. Определения и сокращения

2. В настоящем Соглашении используются следующие основные понятия:

1) AC SD – Автоматизированная система "Service Desk", предназначенная для публикации инцидентов и отображение процесса хода исполнения;

2) ЕСМ – Единая система мониторинга;

3) ресурс – мобильное приложение или портал, используемый для оказания государственной услуги;

4) Цифровая система мониторинга оказания государственных услуг – цифровая система, предназначенная для автоматизации и мониторинга процесса оказания государственных услуг, в том числе оказываемых через Государственную корпорацию "Правительство для граждан".

Глава 3. Содержание соглашения

3. Сторона 1:

Обеспечивает внесение данных услугодателями в цифровую систему мониторинга оказания государственных услуг о стадии оказания государственной услуги в порядке, установленном правилами внесения данных в цифровую систему мониторинга оказания государственных услуг о стадии оказания государственных услуг утвержденных приказом исполняющего обязанности Министра транспорта и коммуникаций Республики Казахстан от 14 июня 2013 года № 452 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 8555).

4. Сторона 2:

1) обеспечивает подключение негосударственных цифровых систем, используемых для оказания государственных услуг, к цифровой системе мониторинга оказания государственных услуг;

2) создает собственный оперативный центр кибербезопасности и обеспечивает его функционирование или приобретает услуги оперативного центра кибербезопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан, а также обеспечивает взаимодействие его с Национальным координационным центром кибербезопасности;

3) соблюдает конфиденциальность и осуществляет защиту, не разглашает и не передает третьим лицам, не публикует персональные данные и конфиденциальную информацию, переданную в сервис Стороной 1, за исключением случаев, предусмотренных законодательством Республики Казахстан;

4) обеспечивает техническую поддержку;

5) для использования интеграционного(-ых) сервиса(-ов) подтверждает популярность своего ресурса наличием мобильного приложения в маркетплейсах;

6) обеспечивает на своем ресурсе бесперебойность оказываемых государственных услуг, при условии доступности всех сервисов других участников интеграционного взаимодействия;

7) предоставляет пользователям при использовании мобильного приложения средства биометрической идентификации либо использует сервис биометрической

идентификации личности Министерства искусственного интеллекта и цифрового развития Республики Казахстан для авторизации и подписания документов;

8) до запуска государственной услуги в промышленную эксплуатацию на внешнюю платформу обеспечивает демонстрацию государственной услуги уполномоченному органу, владельцу интеграционного сервиса и услугодателю;

9) оказывает государственную услугу в срок, установленный подзаконным нормативным правовым актом, определяющим порядок ее оказания.

5. Сторона 3:

В случае несоблюдения сторонами требований настоящего Соглашения принимает меры по отключению сервисов, используемых для оказания государственных услуг, сообщив участникам реализации интеграционного сервиса.

6. Под Сторонами понимается:

Сторона 1 – уполномоченный орган, разработчик нормативного правового акта в сфере государственных услуг;

Сторона 2 – сторонняя организация, банки второго уровня, организующие прием заявок на оказание государственных услуг;

Сторона 3 – Министерство искусственного интеллекта и цифрового развития Республики Казахстан;

Стороны:

6.1 обеспечивают бесперебойную работоспособность и доступность сервисов интеграции и принимают сообщения от цифровых объектов в круглогодичном режиме (кроме плановых, внеплановых работ по обновлению, технических сбоев аппаратных средств, каналов связи и неработоспособности услуг по причине проблем на стороне цифровых систем государственных органов);

6.2 ШЦП, ВШЦП работают на промышленной среде в круглосуточном режиме и принимают сообщения от цифровых объектов на постоянной основе за исключением технологических перерывов;

6.3 время принятия сообщения ШЦП, ВШЦП не превышает одной минуты с момента его получения по универсальному синхронному каналу и асинхронному каналу. Время предоставления ответа по запросу на асинхронном канале, зависит от реализации каждого интеграционного сервиса;

6.4 технологические перерывы в работе сервиса интеграции заранее оговариваются и согласовываются Сторонами за 3 (три) рабочих дня до начала их проведения (по умолчанию технологические перерывы приходятся на ночное время с 21:00 до 6:00 часов, а также в выходные и праздничные дни);

6.5 с целью проведения тестирования участниками взаимодействия обеспечивается работоспособность тестовой среды цифровых объектов;

6.6 в случае технической необходимости, производят перезагрузку цифрового объекта, о чем уведомляют администраторов других цифровых объектов, в виде телефонограммы или по электронной почте, с указанием времени технических работ;

6.7 в случае, если Стороны не принимают соответствующие меры по исправлению технических ошибок по информационному взаимодействию в кратчайшие сроки, оператор "цифрового правительства" отключает соответствующий интеграционный сервис Владельца интеграционного сервиса или приостанавливает подключение Стороны 2, сообщив участникам реализации интеграционного сервиса;

6.8 в случае неисправности каналов связи, проведения провайдерами услуг связи плановых профилактических работ на линиях связи, срок устранения сбоя определяется регламентом провайдера;

6.9 осуществляют меры по защите цифровых объектов;

6.10 принимают меры по соответствию Единым требованиям в области информационно-коммуникационных технологий и обеспечения кибербезопасности, утвержденные постановлением Правительства от 20 декабря 2016 года № 832;

6.11 соблюдают законодательство Республики Казахстан в сфере цифровизации, персональных данных и их защите, кибербезопасности и пункты настоящего Соглашения.

7. Взаимодействия сторон:

7.1 основанием для исполнения любых, оговоренных Соглашением услуг, являются :

1) запрос на устранение инцидента;
2) задача на исполнение плановых работ;
3) регистрация Запросов (Заявок) происходит при приеме Обращения Стороны 1 и (или) Стороны 2 при регистрации сообщений в ЕСМ и управления службами в АС SD.

4) графики и состав плановых работ оговариваются в соответствующих политиках процесса управления инцидентами/изменениями/запросами в работе сервисов Стороны 1;

5) при запросе персональных данных субъект или его законный представитель дает (отзывает) согласие на сбор, обработку персональных данных посредством государственного сервиса контроля доступа к персональным данным.

8. Индекс доступности.

Расчет: индекс доступности рассчитывается по формуле, указанной ниже.

Формула состоит из:

И – индекс доступности сервиса, %;

Т – период возможной доступности сервиса, часы;

Р – период недоступности сервиса*, часы.

*Недоступность сервиса – время простоя, в которое авторизованные пользователи не имеют возможности получить доступ к ресурсам, информации, сервисам,

предоставляемым цифровыми системами. Состоит из сбоев цифровых систем, плановых и внеплановых работ, проводимых с отключением цифровых систем.

Формула по расчету доступности цифровых систем выглядит следующим образом:
$$(T-P)/T*100= XX \%$$

8.1 индекс доступности каждого сервиса высчитывается самостоятельно Владелец интеграционного сервиса для дальнейшей публикации на своих ресурсах.

Глава 4. Уведомление

9. Любое уведомление, которое одна сторона направляет другой стороне в соответствии с настоящим Соглашением, направляется нарочно, с дополнительным направлением посредством электронной почты или факса.

10. Уведомление вступает в силу после доставки или в указанный день вступления в силу (если указано в уведомлении), в зависимости от того, какая из этих дат наступит позднее.

Глава 5. Решение спорных вопросов

11. Сторона 1 и Сторона 2 прилагают все усилия к тому, чтобы разрешать в процессе прямых переговоров все разногласия или споры, возникающие между ними по настоящему Соглашению или в связи с ним.

12. Если после таких переговоров Сторона 1 и Сторона 2 не могут разрешить спор по настоящему Соглашению, любая из Сторон может потребовать решения этого вопроса в соответствии с законодательством Республики Казахстан.

Глава 6. Прочие условия

13. Срок действия настоящего Соглашения вступает в силу с момента подписания Сторонами и действует до его расторжения.

14. Любые изменения и дополнения к настоящему Соглашению совершаются в той же форме, что и заключение настоящего Соглашения, посредством подписания Сторонами дополнительного(ых) соглашения(ий) к настоящему Соглашению.

15. Настоящее Соглашение составлено на казахском и русском языках в двух экземплярах. Все экземпляры идентичны и имеют одинаковую юридическую силу. У каждой из Сторон находится по одному экземпляру настоящего Соглашения на казахском и русском языках. Все приложения к настоящему Соглашению являются его неотъемлемой частью.

16. В части, неурегулированной настоящим Соглашением, Стороны руководствуются законодательством Республики Казахстан.

17. Настоящее Соглашение может быть расторгнуто по соглашению Сторон либо по инициативе одной из Сторон в случае, если другая Сторона не выполняет условия соблюдения пунктов настоящего Соглашения.

Приложение 7
к Правилам интеграции цифровых
объектов "цифрового
правительства"
Форма

Заявка на актуализацию интеграционного сервиса

1. Владелец интеграционного сервиса	
2.	Наименование организации
3.	Индивидуальный идентификационный номер/ бизнес-идентификационный номер
4.	Ключ сервиса
5.	Назначение сервиса
6.	Режим взаимодействия
7.	Наименование цифровой системы
8. Цифровая система владельца интеграционного сервиса	
9.	Наименование цифровой системы владельца интеграционного сервиса
10.	Логин системы
11.	Пароль (тестовая среда)
12.	Пароль (среда промышленной эксплуатации)
13. Тестовая среда	
13.1	В единой транспортной среде государственных органов
13.2	Вне единой транспортной среды государственных органов
13.2.1	Данные VPN-туннеля
13.2.2	Тип туннеля (общий/тестовая среда)
13.2.3	Информация о шлюзе VPN
13.2.4	Публичный Peer IP-адрес системы
13.2.5	Имеется VPN-туннель для данной системы? (да/нет)
13.3	Хостинг оператора "цифрового правительства" (да/ нет)
14.	Публичный Peer IP-адрес системы
15.	Порт
16.	Протокол
17. Продуктивная среда	
17.1	В единой транспортной среде государственных органов

17.2	Вне единой транспортной среды государственных органов
17.2.1	Данные VPN-туннеля
17.2.2	Тип туннеля (общий/среда эксплуатации)
17.2.3	Информация о шлюзе VPN
17.2.4	Публичный Peer IP-адрес системы
17.2.5	Имеется VPN-туннель для данной системы? (да/нет)
17.3	Хостинг оператора "цифрового правительства" (да/нет)
18.	Публичный Peer IP-адрес системы
19.	Порт
20.	Протокол
21.	Комментарий к изменениям по сети
22. Электронный сервис	
23.	Признак наличия маршрутизации сообщений (да/нет)
24.	Наименование URL сервиса, принимающего запросы (тестовая среда)
25.	URL сервиса, принимающего запросы (тестовая среда)
26.	Наименование URL сервиса, принимающего запросы (среда эксплуатации)
27.	URL сервиса, принимающего запросы (среда эксплуатации)
28.	SSL сертификат (выданный национальным удостоверяющим центром Республики Казахстан)
29.	Тип сертификата
30.	Метод авторизации
31.	Логин
32.	Пароль
33.	Тип безопасности
34.	XSD
35.	Пример запроса
36.	Пример ответа

Приложение 8
к Правилам интеграции цифровых
объектов "цифрового
правительства"
Форма

Заявка на актуализацию подключения к интеграционному сервису

1. Владелец интеграционного сервиса	
2.	Наименование организации

3.	Индивидуальный идентификационный номер/ бизнес-идентификационный номер
4.	Ключ сервиса
5.	Назначение сервиса
6.	Режим взаимодействия
7.	Наименование цифровой системы владельца интеграционного сервиса
8. Клиент сервиса	
9.	Наименование организации
10.	Индивидуальный идентификационный номер/ бизнес-идентификационный номер
11.	Основание для подключения
12.	ФИО ответственного лица
13.	Контактный телефон ответственного лица
14.	Электронная почта ответственного лица
15. Цифровая система клиента сервиса	
16.	Наименование цифровой системы
17.	Логин системы
18.	Пароль (тестовая среда)
19.	Пароль (среда эксплуатации)
20.	Сертификат открытого ключа транспортной подписи системы (выданный национальным удостоверяющим центром Республики Казахстан)
21.	Тип сертификата (общий/тестовая среда)
22.	Протоколы испытаний на соответствие требованиям кибербезопасности
23. Тестовая среда	
23.1	В единой транспортной среде государственных органов
23.2	Вне единой транспортной среды государственных органов
23.2.1	Данные VPN-туннеля
23.2.2	Тип туннеля (общий/тестовая среда)
23.2.3	Информация о шлюзе VPN
23.2.4	Публичный Peer IP-адрес системы
23.2.5	Имеется VPN-туннель для данной системы? (да/нет)
23.3	Хостинг оператора "цифрового правительства" (да/ нет)
24. Среда эксплуатации	
24.1	В единой транспортной среде государственных органов
24.2	Вне единой транспортной среды государственных органов
24.2.1	Данные VPN-туннеля

24.2.2	Тип туннеля (общий/ среда эксплуатации)
24.2.3	Информация о шлюзе VPN
24.2.4	Публичный Peer IP-адрес системы
24.2.5	Имеется VPN-туннель для данной системы? (да/нет)
24.3	Хостинг оператора "цифрового правительства" (да/нет)
25.	Публичный IP-адрес системы
26.	Порт
27.	Протокол
28.	Комментарий к изменениям по сети
29. Электронный сервис	
30.	Ключ сервиса
31.	Режим взаимодействия сервиса -
32.	Формат сервиса
33.	Признак наличия маршрутизации сообщений
34.	Сервис предоставляет персональные данные

Приложение 9
к Правилам интеграции цифровых
объектов "цифрового
правительства"

Сценарий использования транспортной подписи

1. Сценарий приема сообщения с использованием транспортной подписи шлюзом "цифрового правительства" (далее – ШЦП), используемый при взаимодействии цифровых объектов:

1) ШЦП проверяет сообщение (авторизацию, валидацию пакета с сообщением, транспортную подпись цифровых объектов);

2) ШЦП подписывает сообщение транспортной подписью;

3) ШЦП передает подписанное сообщение внешнему шлюзу "цифрового правительства" (далее – ВШЦП) (при взаимодействии с цифровых систем вне единой транспортной среды государственных органов);

4) ВШЦП передает сообщение цифровому объекту (при взаимодействии с цифровых систем вне единой транспортной среды государственных органов).

2. Сценарий приема сообщения с использованием транспортных подписей ШЦП и вызывающей стороны:

1) отправитель подписывает сообщение транспортной подписью и отправляет на ШЦП;

2) ШЦП проверяет соответствие бизнес-идентификационного номера, указанного в электронной цифровой подписи юридического лица, внесенного в систему при регистрации цифрового объекта;

3) ШЦП проверяет транспортную подпись на действительность или отозванность.

3. Сценарий использования механизма взаимной аутентификации mTLS:

1) отправитель и ШЦП в процессе взаимной TLS-аутентификации обмениваются X.509 сертификатами, выпущенными национальным удостоверяющим центром Республики Казахстан;

2) отправитель и ШЦП проводят валидацию полученных сертификатов;

3) при успешном прохождении взаимной TLS-аутентификации устанавливается аутентифицированное защищенное соединение.

4. Сценарий проверки токена верификации в рамках взаимодействия с государственным сервисом контроля доступа к персональным данным:

1) ШЦП проверяет наличие kdp_token и kdp_public_key в составе запроса (в массиве properties);

2) ШЦП проводит валидацию kdp_token и kdp_public_key;

3) ШЦП сопоставляет параметр sid внутри токена верификации и поле service id в составе запроса;

4) ШЦП проверяет оторванность токена верификации в государственном сервисе контроля доступа к персональным данным;

5) в случае успешного прохождения всех проверок осуществляется дальнейшая обработка запроса, включая его передачу в интеграционный сервис.

Приложение к приказу
Заместитель Премьер-Министра –
Министр искусственного интеллекта
и цифрового развития
Республики Казахстан
от 1 июля 2026 года № 368/НК

Перечень утративших силу некоторых приказов

1. Приказ и.о. Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 19 апреля 2018 года № 16777);

2. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 22 апреля 2019 года № 48/НК "О внесении изменений и дополнения в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 26 апреля 2019 года № 18588);

3. Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 31 июля 2019 года № 183/НК "О внесении изменений и дополнения в приказ исполняющего обязанности Министра информации и

коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 31 июля 2019 года № 19148);

4. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2020 года № 165/НҚ "О внесении изменения в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 6 мая 2020 года № 20581);

5. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 28 января 2022 года № 21/НҚ "О внесении изменения в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 31 января 2022 года № 26688);

6. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 2 сентября 2022 года № 307/НҚ "О внесении изменений и дополнений в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 9 сентября 2022 года № 29478);

7. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 5 декабря 2023 года № 603/НҚ "О внесении изменений и дополнений в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 7 декабря 2023 года № 33737);

8. Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 26 июля 2024 года № 444/НҚ "О внесении изменений и дополнений в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 31 июля 2024 года № 34838);

9. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 12 марта 2025 года № 104/НК "О внесении изменения в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 12 марта 2025 года № 35804);

10. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 10 сентября 2025 года № 465/НК "О внесении изменений и дополнения в приказ исполняющего обязанности Министра информации и коммуникаций Республики Казахстан от 29 марта 2018 года № 123 "Об утверждении Правил интеграции объектов информатизации "электронного правительства" (зарегистрирован в Министерстве юстиции Республики Казахстан 13 сентября 2025 года № 36831).