

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"

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 апреля 2020 года № 165/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 6 мая 2020 года № 20581

ПРИКАЗЫВАЮ:

1. Внести 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 Реестре государственной регистрации нормативных правовых актов за № 16777, опубликован 24 апреля 2018 года в эталонном контрольном банке нормативных правовых актов Республики Казахстан) следующее изменение:

Правила интеграции объектов информатизации "электронного правительства", утвержденные указанным приказом, изложить в новой редакции согласно приложению к настоящему приказу.

2. Комитету государственных услуг Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательном порядке обеспечить:

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

2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа представление в Юридический департамент Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Приложение к приказу
Министра цифрового
развития, инноваций и
аэрокосмической
промышленности
Республики Казахстан
от 29 апреля 2020 года
№ 165/НК
Утверждены приказом
исполняющего обязанности
Министра информации и
коммуникаций
Республики Казахстан
от 29 марта 2018 года № 123

Правила интеграции объектов информатизации "электронного правительства"

Глава 1. Общие положения

1. Настоящие Правила интеграции объектов информатизации "электронного правительства" (далее – Правила) разработаны в соответствии с подпунктом 13) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и определяют порядок интеграции объектов информатизации "электронного правительства".

2. В настоящих Правилах используются следующие основные понятия:

1) объекты информатизации – электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура;

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

3) уполномоченный орган в сфере информатизации (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере информатизации и "электронного правительства";

4) информационная система (далее – ИС) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

5) бизнес-данные объекта информатизации – данные взаимодействия владельца и инициатора интеграционного сервиса, входящие в состав сообщений формата ШЭП, ВШЭП как блок, не проверяемый на стороне ШЭП, ВШЭП;

6) интеграция объектов информатизации – мероприятия по организации и обеспечению информационного взаимодействия между объектами информатизации на основании используемых в Республике Казахстан стандартных протоколов передачи данных;

7) 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;

8) протокол Деффи-Хеллмана – криптографический протокол, позволяющий двум и более сторонам обменяться заранее согласованным общим секретным ключом, используя пару публичных и частных ключей в незащищенном от прослушивания канале связи;

9) публичный Peer IP-адрес – уникальный IP-адрес устройства, терминирующего VPN-туннель и используемого в сети Интернет, на стороне инициатора и/или владельца объекта информатизации;

10) инициатор интеграционного сервиса – владелец объекта информатизации, инициирующий запрос на предоставление интеграционного сервиса;

11) интеграционный сервис – способ информационного взаимодействия объектов информатизации;

12) владелец интеграционного сервиса (далее – владелец сервиса) – собственник или владелец объекта информатизации, предоставляющий интеграционный сервис;

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

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

15) удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

16) клиент-коннектор – программное обеспечение, предоставляющее инициатору объекта информатизации возможность генерации точки подключения к интеграционному сервису, размещенному на ШЭП, ВШЭП с поддержкой форматов ШЭП, ВШЭП;

17) API с открытым правом доступа (OpenAPI) – API, выставленный в свободном доступе в сети Интернет, не требующий согласования или разрешения Владельца

электронного информационного ресурса для осуществления информационного взаимодействия;

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

19) единая транспортная среда государственных органов (далее – ЕТС ГО) – сеть телекоммуникаций, входящая в информационно-коммуникационную инфраструктуру "электронного 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 информатизации, определенных уполномоченным органом, с соблюдением требуемого уровня информационной безопасности;

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

21) реестр сервисов – перечень зарегистрированных в шлюзе "электронного правительства" и внешнем шлюзе "электронного правительства" сервисов, с описанием сервиса;

22) сервис-коннектор – программное обеспечение, позволяющее владельцу объекта информатизации создавать и размещать интеграционные сервисы на ШЭП;

23) электронное сообщение – электронный документ в формате XML, JSON, предназначенный для обмена информацией между объектами информатизации;

24) электронная цифровая подпись (далее – ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

25) оператор информационно-коммуникационной инфраструктуры "электронного правительства" (далее – оператор) – юридическое лицо, определяемое Правительством Республики Казахстан, на которое возложено обеспечение функционирования закрепленной за ним информационно-коммуникационной инфраструктуры "электронного правительства";

26) сервисный интегратор "электронного правительства" (далее – сервисный интегратор) – юридическое лицо, определяемое Правительством Республики Казахстан, на которое возложены функции по методологическому обеспечению развития архитектуры "электронного правительства" и типовой архитектуры "электронного акимата", а также иные функции, предусмотренные Законом;

27) шлюз "электронного правительства" (далее – ШЭП) – ИС, предназначенная для интеграции объектов информатизации "электронного правительства" с иными объектами информатизации "электронного правительства";

28) объекты информатизации "электронного правительства" – государственные электронные информационные ресурсы, программное обеспечение государственных органов, интернет - ресурс государственного органа, объекты инфраструктуры "электронного правительства", в том числе сервисный программный продукт, программное обеспечение и информационные системы иных лиц, предназначенные для формирования государственных электронных информационных ресурсов в рамках осуществления государственных функций и оказания государственных услуг;

29) внешний шлюз "электронного правительства" (далее – ВШЭП) – подсистема шлюза "электронного правительства", предназначенная для обеспечения взаимодействия информационных систем, находящихся в единой транспортной среде государственных органов, с информационными системами, находящимися вне единой транспортной среды государственных органов;

30) платежный шлюз "электронного правительства" (далее – ПШЭП) – ИС, автоматизирующая процессы передачи информации о проведении платежей в рамках оказания возмездных услуг, оказываемых в электронной форме;

31) Application programming interface (далее – API) – интерфейс программирования приложений, набор готовых программ, предоставляемых сервисом для информационного взаимодействия между объектами информатизации;

32) инкапсуляция АН (AuthenticationHeader) – инкапсуляция аутентифицирующего заголовка, которая позволяет аутентифицировать соседнего узла в туннеле VPN и обеспечить целостность передаваемых данных без шифрования. Значение в поле протокола заголовка IP – равное UDP порту 51;

33) ESP (Encapsulation Security Pay load) – инкапсуляция защищенных данных, который позволяет зашифровать весь кадр, передаваемый через VPN-канал, включая полезную нагрузку и IP-заголовки источника и назначения.

34) Hyper Text Transfer Protocol (далее – HTTP) — протокол прикладного уровня передачи данных изначально — в виде гипертекстовых документов в формате HTML, используемый для передачи произвольных данных;

35) IP (Internet Protocol) – сетевая модель передачи данных, представленных в цифровом виде;

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

37) Representational State Transfer (далее – REST) — стиль архитектуры программного обеспечения для взаимодействия компонентов распределенного приложения в сети. REST представляет собой согласованный набор ограничений, учитываемых при проектировании распределенных систем или взаимодействия сервисов, использующий стандарты, такие как HTTP, URL, JSON и XML;

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

39) TCP (Transmission Control Protocol) – один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных;

40) UDP (User Datagram Protocol) – протокол пользовательских датаграмм, один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета;

41) URL (Uniform Resource Locator) – единообразный локатор (определитель местонахождения) ресурса, указывает адрес сервиса объекта информатизации;

42) Virtual Private Network (далее – VPN) – виртуальная частная сеть для обмена информацией двух узлов;

3. Интеграции посредством ШЭП, ВШЭП не подлежат:

1) сервисы, предоставляемые удостоверяющими центрами;

2) объекты информатизации, которые содержат сведения, составляющие государственные секреты Республики Казахстан и служебную информацию ограниченного распространения;

3) объекты информатизации, размещенные на информационно-коммуникационной платформе "электронного правительства" и предназначенные для формирования единого пространства данных для целей предоставлений аналитической информации по деятельности Правительства Республики Казахстан;

4) сервисы 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.

4. Негосударственная ИС интегрируется с ИС государственного органа только через ВШЭП, введенный в промышленную эксплуатацию.

При интеграции также учитывается наличие договора совместных работ по информационной безопасности государственных и негосударственных ИС.

5. Мероприятия по интеграции объектов информатизации осуществляются посредством веб портала "электронного правительства" с учетом форматов данных, указанных в приложении 1 к настоящим Правилам.

6. Интеграция объектов информатизации осуществляется при условии наличия интеграционного сервиса в реестре сервисов на веб-портале "электронного правительства".

7. Оператор вносит изменения в сервис или исключает его из реестра сервисов по запросу Владельца сервиса или уполномоченного органа с уведомлением уполномоченного органа и сервисного интегратора.

8. При оказании услуг в электронном виде объект информатизации направляет сведения об использовании платежей в ПШЭП.

Все заявки и документы удостоверяются ЭЦП уполномоченных лиц участников интеграционного взаимодействия.

Если информационная система инициатора интеграционного сервиса относится к объектам информатизации, указанным в пункте 2 статьи 49 Закона, то к заявке на подключение к сервису или на публикацию сервиса инициатор интеграционного сервиса прилагает акт испытаний с положительным результатом испытаний на соответствие требованиям информационной безопасности.

9. Для разработки и размещения интеграционного сервиса на ШЭП, ВШЭП владелец интеграционного сервиса и инициатор интеграционного сервиса используют сервис-коннектор и клиент-коннектор для подключения к интеграционному сервису, при отсутствии иного интеграционного сервиса.

Глава 2. Порядок интеграции объектов информатизации "электронного правительства"

Параграф 1. Порядок публикации сервиса по инициативе инициатора интеграционного сервиса

10. При отсутствии сервиса в реестре сервисов инициатор интеграционного сервиса направляет посредством веб-портала "электронного правительства" запрос сервисному интегратору для предоставления рекомендаций по определению владельца объекта информатизации, в котором содержатся необходимые сведения.

11. При получении уведомления о поступлении заявки сервисный интегратор рассматривает запрос в течение 2 (двух) рабочих дней и предоставляет инициатору интеграционного сервиса рекомендации.

12. Инициатор интеграционного сервиса на основе рекомендаций сервисного интегратора авторизуется на веб-портале "электронного правительства" и направляет запрос в форме заявки на создание сервиса владельцу объекта информатизации.

13. Владелец объекта информатизации, получив уведомление о поступлении заявки на создание сервиса, в течение 2 (двух) рабочих дней рассматривает заявку. По результатам рассмотрения, согласовывает заявку либо возвращает ее на доработку инициатору, либо отказывает в создании сервиса с указанием причин.

14. В случае согласования заявки на создание сервиса, владелец объекта информатизации заполняет требования к взаимодействию с сервисом согласно приложению 2 к настоящим Правилам (далее – требования к взаимодействию с сервисом) и заявку на публикацию сервиса согласно приложению 3 к настоящим Правилам (далее – заявка на публикацию сервиса), прилагает к заявке файлы XSD сервиса, а также XML примеров запроса и ответа с тестовыми данными и направляет заявку инициатору интеграционного сервиса с уведомлением уполномоченного органа.

15. В случае возврата владельцем объекта информатизации заявки на создание сервиса на доработку инициатор интеграционного сервиса в течение 2 (двух) рабочих дней осуществляет доработку заявки и повторно направляет ее на рассмотрение владельцу объекта информатизации.

16. В случае отказа владельцем объекта информатизации в создании сервиса мероприятия по публикации сервиса прекращаются.

17. При поступлении заявки на публикацию сервиса оператором осуществляется проверка заявки на полноту и правильность заполнения в течение 3 (трех) рабочих дней. При отрицательном результате проверки заявки, оператор направляет заявку на доработку с указанием причин.

18. Владелец объекта информатизации в течение 2 (двух) рабочих дней дорабатывает заявку на публикацию сервиса и направляет заявку оператору на повторное рассмотрение.

19. При положительном результате проверки заявки оператор в течение 10 (десяти) рабочих дней предоставляет инициатору интеграционного сервиса доступ к тестовой среде ШЭП, ВШЭП и подключает инициатора интеграционного сервиса к сервису на тестовой среде ШЭП, ВШЭП для проведения тестирования интеграции.

20. Разработчики интеграционного сервиса со стороны владельца объекта информатизации, инициатора интеграционного сервиса вносят изменения в объекты информатизации для проведения тестирования по интеграции с объектами информатизации.

21. Совместно с разработчиками интеграционного сервиса со стороны владельца объекта информатизации, инициатора интеграционного сервиса и оператором проводится тестирование интеграционного сервиса в согласованные сроки.

22. Со стороны ШЭП, ВШЭП подтверждением реализации интеграционного сервиса является передача сообщений (для асинхронного сервиса – получение отправителем уникального идентификатора сообщения, для синхронного – получение ответного сообщения) между участниками взаимодействия, которая фиксируется в журнале логирования ШЭП, ВШЭП.

23. Со стороны участников взаимодействия (владельца сервиса и инициатора интеграционного сервиса) подтверждением реализации интеграционного сервиса является выполнение условий взаимодействия и обработка данных самими участниками взаимодействия.

24. В случае положительного результата тестирования интеграционного сервиса владелец сервиса формирует акт тестирования и ввода в эксплуатацию согласно приложению 4 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 тестирование интеграции продолжается до получения положительного результата.

25. Инициатор интеграционного сервиса при получении заявки и акта тестирования в течение 3 (трех) рабочих дней согласовывает акт тестирования, удостоверив его своей ЭЦП, и направляет акт тестирования на согласование оператору.

26. Оператор рассматривает акт тестирования в течение 3 (трех) рабочих дней с момента получения заявки и акта тестирования.

27. При отрицательном результате проверки оператор возвращает акт тестирования на доработку владельцу сервиса. Владелец сервиса в срок не более 3 (трех) рабочих дней осуществляет доработку акта тестирования и повторно направляет его на рассмотрение инициатору интеграционного сервиса.

При положительном результате проверки акта тестирования оператор согласовывает акт тестирования, публикует паспорт сервиса в реестре сервисов и предоставляет инициатору интеграционного сервиса доступ к сервису на промышленной среде ШЭП, ВШЭП. Уполномоченный орган и сервисный интегратор уведомляются о публикации интеграционного сервиса посредством веб-портала "электронного правительства".

Параграф 2. Порядок публикации сервиса по инициативе владельца объекта информатизации

28. Владелец сервиса авторизуется на веб-портале "электронного правительства" и запускает процесс по публикации сервиса, предварительно проверив отсутствие сервиса в опубликованном реестре сервисов. При формировании заявки владелец сервиса заполняет требования к взаимодействию с сервисом и заявку на публикацию сервиса, принимает условия интеграции, с приложением файлов XSD сервиса, а также XML примеров запроса и ответа с тестовыми данными.

29. Оператор, получив уведомление о поступлении заявки на публикацию сервиса, осуществляет проверку заявки на публикацию сервиса, заявки на организацию сетевого доступа на полноту и правильность заполнения в течение 3 (трех) рабочих дней. При отрицательном результате проверки заявки, оператор направляет заявки на доработку с указанием причин.

30. При положительном результате проверки заявки оператор в течение 10 (десяти) рабочих дней осуществляет публикацию сервиса и предоставляет владельцу сервиса доступ к тестовой и промышленной среде ШЭП, ВШЭП. Уполномоченный орган и сервисный интегратор уведомляются о публикации интеграционного сервиса посредством веб-портала "электронного правительства".

31. При указании владельцем сервиса подключающегося к сервису владельца объекта информатизации публикация сервиса проводится в порядке, установленном пунктами 14-27 настоящих Правил.

Параграф 3. Порядок подключения к интеграционному сервису

32. Инициатор интеграционного сервиса авторизуется на веб-портале "электронного правительства" и производит поиск необходимого сервиса в реестре сервисов.

33. Инициатор интеграционного сервиса инициирует заявку на подключение к сервису, заполняет требуемые поля согласно приложению 5 к настоящим Правилам, принимает условия интеграции. Подключение к интеграционному сервису осуществляется с учетом требований к взаимодействию с сервисом.

34. Владелец сервиса, получив уведомление о необходимости просмотра заявки посредством веб-портала "электронного правительства", в течение 2 (двух) рабочих дней направляет ответ по заявке на подключение к сервису. При отказе в интеграции указывает мотивированный ответ.

35. В случае согласования заявки владельцем сервиса оператор, получив уведомление о необходимости просмотра заявки посредством вебпортала "электронного правительства", в течение 3 (трех) рабочих дней осуществляет согласование и проверку заявки на подключение к сервису (интеграцию) на полноту и правильность заполнения. При отрицательном результате проверки заявки, оператор направляет заявку на доработку с указанием причин.

36. Инициатор интеграционного сервиса в течение 3 (трех) рабочих дней осуществляет доработку заявки и повторно направляет ее на рассмотрение Владельцу сервиса.

37. В случае согласования заявки оператор в течение 10 (десяти) рабочих дней предоставляет инициатору интеграционного сервиса доступ к тестовой среде ШЭП, ВШЭП для проведения тестирования интеграции.

38. Инициатор интеграционного сервиса, владелец сервиса, оператор в срок не более 3 (трех) месяцев проводят тестирование интеграции до получения положительного результата.

39. Совместно с разработчиками интеграционного сервиса со стороны владельца сервиса, инициатора интеграционного сервиса и оператором проводится тестирование интеграционного сервиса в согласованные сроки.

40. Со стороны ШЭП, ВШЭП подтверждением реализации интеграционного сервиса является передача сообщений (для асинхронного сервиса – получение отправителем уникального идентификатора сообщения, для синхронного – получение ответного сообщения) между участниками взаимодействия, которая фиксируется в журнале логирования ШЭП, ВШЭП.

41. Со стороны участников взаимодействия (владельца сервиса и инициатора интеграционного сервиса) подтверждением реализации интеграционного сервиса является выполнение условий взаимодействия и обработка данных самими участниками взаимодействия.

42. В случае положительного результата тестирования интеграционного сервиса инициатор интеграционного сервиса формирует акт тестирования и ввода в эксплуатацию, удостоверяет его своей ЭЦП и направляет ее на согласование владельцу сервиса.

При отрицательном результате тестирования интеграции продолжается до получения положительного результата.

43. Владелец сервиса при получении заявки и акта тестирования в течение 3 (трех) рабочих дней согласовывает акт тестирования, удостоверив его своей ЭЦП, и направляет акт тестирования на согласование оператору.

44. Оператор рассматривает акт тестирования в течение 3 (трех) рабочих дней с момента его получения.

45. При отрицательном результате проверки оператор возвращает акт тестирования на доработку инициатору интеграционного сервиса. Инициатор интеграционного сервиса в срок не более 3 (трех) рабочих дней осуществляет доработку акта тестирования и повторно направляет его на рассмотрение владельцу сервиса.

При положительном результате проверки акта тестирования оператор согласовывает акт тестирования и предоставляет инициатору интеграционного сервиса доступ к сервису на промышленной среде ШЭП, ВШЭП. Уполномоченный орган и сервисный интегратор уведомляются о подключении инициатора интеграционного сервиса к интеграционному сервису посредством веб-портала "электронного правительства".

Глава 3. Обеспечение эксплуатации и защиты интеграционного сервиса

46. ШЭП, ВШЭП работают на промышленной среде в круглосуточном режиме и принимают сообщения от объектов информатизации на постоянной основе за исключением технологических перерывов.

47. Время принятия сообщения ШЭП, ВШЭП не должно превышать 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.

48. Технологические перерывы в работе объекта информатизации заранее оговариваются и согласовываются владельцем сервиса, инициатором интеграционного

сервиса и оператором 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).

49. С целью проведения тестирования участниками взаимодействия обеспечивается работоспособность тестовой среды объектов информатизации.

50. В случае технической необходимости, оператор и/или владелец сервиса, инициатор интеграционного сервиса производит перезагрузку объекта информатизации, о чем уведомляют администраторов других объектов информатизации, в виде телефонограммы или по электронной почте, с указанием времени технических работ.

51. В случае если владелец сервиса, инициатор интеграционного сервиса не принимают соответствующие меры по исправлению технических ошибок по информационному взаимодействию в кратчайшие сроки, оператор отключает соответствующий интеграционный сервис владельца сервиса или приостанавливает подключение инициатора интеграционного сервиса, сообщив участникам реализации интеграционного сервиса.

52. В случае неисправности каналов связи, проведения провайдерами услуг связи плановых профилактических работ на линиях связи, срок устранения сбоя определяется регламентом провайдера.

53. Защита информации при реализации интеграционного сервиса обеспечивается:

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

2) авторизация субъектов информатизации на ШЭП, ВШЭП проходит по логину и паролю, которые выдаются оператором, и по транспортной подписи, за исключением сервисов с применением стиля архитектуры программного обеспечения для распределенных систем (REST);

3) журналированием всех событий на ШЭП, ВШЭП;

4) мероприятиями технического и организационного характера по защите информации в соответствии с Законом.

54. Подтверждением авторства сообщений является положительный результат проверки соответствия транспортной подписи регистрационным свидетельством ЭЦП участника интеграционного взаимодействия, направившего сообщение.

55. Транспортная подпись не содержит метку времени.

56. Проверка транспортной подписи в ЕТС ГО выполняется на ШЭП.

57. При вызове сервиса на ШЭП использование транспортной подписи осуществляется по сценарию использования транспортной подписи согласно приложению 6 к настоящим Правилам.

58. Проверка транспортной подписи в ЕТС ГО на ШЭП состоит из следующих процедур:

1) проверка принадлежности ЭЦП отправителю сообщения;

2) проверка действительности ЭЦП.

59. При информационном взаимодействии все электронные сообщения должны быть подписаны ЭЦП участников интеграционного взаимодействия.

60. При применении ЭЦП при информационном взаимодействии объектов информатизации необходимо руководствоваться Законом Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи".

61. Защиту информации от несанкционированного доступа на уровне прикладного программного обеспечения, своевременную передачу и неизменность передаваемых сведений обеспечивает ШЭП, ВШЭП.

62. В случае временного отключения интеграционного сервиса (модификации сервиса, модификации объекта информатизации, предоставляющей доступ к сервису) владелец сервиса уведомляет уполномоченный орган и всех пользователей интеграционного сервиса посредством веб портала "электронного правительства" за 3 (три) рабочих дня, в случае отключения сервиса или прекращения работы не позднее 1 (одного) месяца.

63. Владелец сервиса и инициатор интеграционного сервиса определяют ответственных лиц, которые обеспечивают информационную безопасность и постоянную готовность программных и технических средств.

64. В случае изменения состава ответственных лиц (перевода или прекращения трудового договора) в недельный срок владелец сервиса и инициатор интеграционного сервиса производят взаимное информирование об имеющихся изменениях, и сообщаются новые сведения об ответственных лицах по своевременному исполнению положений настоящих Правил.

Приложение 1 к Правилам
интеграции объектов
информатизации "электронного
правительства"

Форматы данных веб-сервисов SOAP

1. Описание сообщений асинхронного канала

1.1. Интерфейс сервиса на ШЭП, ВШЭП:

Метод для отправки сообщений на асинхронный канал ШЭП, ВШЭП (SendMessage)

:

Запрос на предоставление сервиса (SendMessageRequest) содержит следующие поля

: Формат данных SendMessageRequest

Поле	Тип	Обязательность	Описание
request	AsyncSendMessageRequest	Да	Запрос
messageInfo	AsyncMessageInfo	Да	Метаданные сообщения

messageId	xsd: string	Да	Идентификатор сообщения в системе получателя (заполняет система получателя запроса (система обрабатывающая сообщение))
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения в системе получателя запроса (если сообщения существует в рамках цепочки сообщений системы (отправителя) система обрабатывающая сообщение)
serviceId	xsd: string	Да	Идентификатор сервиса
messageType	xsd: string	Да	Тип сообщения : REQUEST - первое сообщения взаимодействия
routId	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	Да	Идентификатор сессии ШЭП. Заполняется на ШЭП, отправителю заполнять не надо.
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, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя)
key	xsd: int		Ключ свойства
value	xsd: int	Нет	Значение свойства
messageData	messagedata	Да	Объект передачи данных
data	xsd: Anytype	Нет	Объект данные сообщения (формат определяется системой получателя сообщения)

Ответ ШЭП, ВШЭП на сообщение (sendMessageResponse) представляет собой массив элементов со следующими полями: Формат данных SendMessageResponse

Поле	Тип	Обязанность	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 ШЭП

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

Поле	Тип	Обязанность	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

Метод отправки уведомления на ШЭП, ВШЭП о доставке или не доставке сообщения (SendDeliveryNotification):

Запрос на уведомление представляет собой массив элементов со следующими полями (sendDeliveryNotificationRequest): **Формат данных SendDeliveryNotificationRequest**

Поле	Тип	Обязанность	Описание
request	Async SendDeliveryNotificationRequest	Да	Запрос
notification	DeliveryNotification	Да	Уведомления о статусе доставки сообщения
messageId	xsd: string	Да	Идентификатор сообщения
serviceid	xsd: string	Да	Идентификатор сервиса
notificationDate	xsd: dateTime	Да	Дата создания уведомления
deliveryStatus	deliveryStatusInfo	Да	Статус доставки (приема сообщения)
receiveStatus	xsd: string	Да	Статус доставки сообщения: MESSAGE_NOT_ACCEPTED – сообщения не принято MESSAGE_ACCEPTED – сообщения принято
statusDate	xsd: dateTime	Да	Дата изменения статуса
resendMessage	xsd: string	Да	Повторное сообщение
error	ErrorInfo	Нет	Информация об ошибке
errorCode	xsd: string	Да	Код ошибки
errorData	xsd: string	Нет	Дополнительное описание ошибки
errorDate	xsd: dateTime	Да	Дата ошибки
subError	ErrorInfo	Нет	Дочерняя ошибка
sessionId	guid	Нет	Идентификатор сессии в которой произошла ошибка
requestDate	xsd: dateTime	Да	Дата запроса
sender	SenderInfo	Нет	Отправитель
senderId	xsd: string	Да	Идентификатор отправителя
password	xsd: string	Нет	Пароль отправителя

Ответ на уведомление (sendDeliveryNotificationResponse) представляет собой массив со следующими полями: **Формат данных SendDeliveryNotificationResponse**

Поле	Тип	Обязанность	Описание
Response	Async SendDeliveryNotificationResponse		Ответ
notificationId	xsd: string	Да	Идентификатор сообщения
responseDate	xsd: dateTime	Да	Дата ответа
sessionId	guid	Нет	Идентификатор сессии ШЭП

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

Поле	Тип	Обязанность	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

Метод получения статуса сообщения с ШЭП, ВШЭП (GetMessageStatus)

Запрос на статус сообщения (GetMessageStatusRequest) представляет собой массив элементов со следующими полями: Формат данных GetMessageStatusRequest

Поле	Тип	Обязанность	Описание
request	AsyncGetmessagestatus	Да	Запрос
messageId	xsd: string	Да	Идентификатор сообщения
requestDate	xsd: dateTime	Да	Дата запроса
sender	senderinfo	Да	Объект информация об отправителе (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Нет	Пароль отправителя
properties	property	Нет	Массив свойств запроса
key	xsd: int		Ключ свойства
value	xsd: int	Нет	Значение свойства

В ответе на запрос на статус (getMessageStatusResponse) должна быть возвращена структура следующего вида: Формат данных GetMessageStatusResponse

Поле	Тип	Обязанность	Описание
response	Async GetMessagestatusResponse		Ответ
messageState	messageState	Да	Состояние сообщения
responseDate	xsd: dateTime	Да	Дата ответа
sessionId	xsd: string	Нет	Идентификатор сессии на ШЭП
status	MessagestatusInfo		Объект "Информация о статусе"
statusCode	xsd: int	Да	Код статуса сообщения
statusmessage	xsd: string	Да	Сообщение статуса
statusDate	xsd: dateTime	Да	Дата изменения статуса

В случае возникновении ошибки в системе, передается сообщение об ошибке (SendMessageFault), которая представляет собой массив элементов со следующими полями: Формат данных SendMessageFault

Поле	Тип	Обязанность	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

Метод выборки сообщений с ШЭП (GetMessages) осуществляется по параметрам:
идентификатору сообщения + получателю (только для запросившего)+
идентификатору сервиса;

идентификатору цепочки сообщений + получателю (только для запросившего) +
идентификатору сервиса;
получателю (только для запросившего) + идентификатору сервиса.

Параметр GetMessageRequest

Запрос содержит следующие поля: Формат данных GetMessageRequest

Поле	Тип	Обязанность	Описание
request	А s y n c GetmessagesRequest	Да	Метаданные запроса
messageId	xsd: string	Да	Идентификатор сообщения
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения
requestdate	xsd: dateTime	Нет	Дата запроса
serviceId	xsd: string	Да	Идентификатор сервиса
sender	Senderinfo	Нет	Объект информация об отправителе (заполняется отправителем)
senderId	xsd: string		Идентификатор отправителя (системы отправителя)
password	xsd: string		Пароль отправителя
amount	xsd: int	Нет	Максимальное кол-во сообщений в выборке. Если данное поле отсутствует в запросе или равно 0, то будет принято настроенное на ШЭП значение
properties	Property	Да	Массив свойств, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя)
key	xsd: string	Да	Ключ свойства
value	xsd: string	Да	Значение свойства

Ответ getMessageResponse со следующими полями: Формат данных
GetMessageResponse

Поле	Тип	Обязанность	Описание
response	А s y n c GetmessageResponse	Да	Ответ
responseDate	xsd: dateTime	Да	Дата ответа
sessionId	xsd: string	Да	Идентификатор сессии на ШЭП
messages	Asynmessage	Нет	
messageInfo	Asynmessageinfo	Да	Метаданные сообщения
messageId	xsd: string	Нет	Идентификатор сообщения
correlationId	xsd: string	Да	Идентификатор цепочки
serviceId	xsd: string	Да	Идентификатор сервиса

messageType	xsd: string	Да	Т и п сообщения : REQUEST - первое сообщения взаимодействия
routeld	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 ШЭП. Заполняется на ШЭП, отправителю заполнять не надо.
Sender	SenderInfo	Да	Объект информация об отправителе (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Нет	Пароль отправителя
properties	property		Массив свойств, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя)
Key	xsd: string	Да	Ключ свойства
Value	xsd: string	Да	Значение свойства
messageData	messageData	Да	Объект передачи данных
Data	xsd: Anytype	Да	Объект данные сообщения (формат определяется системой получателя сообщения)

Ответ об ошибке (SendMessagefault) представляет собой массив элементов со следующими полями: Формат данных SendMessagefault

Поле	Тип	Обязанность	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 сервиса на стороне пользователей ШЭП, ВШЭП для работы с асинхронным каналом.

Сервис реализуется как на стороне провайдера сервиса, так и на стороне использующей сервис. Сервис реализуют в случае необходимости доставки ШЭП сообщений методом вызова сервиса получателя сообщения (PUSH).

Метод приема сообщений: (SendMessage)

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

Поле	Тип	Обязанность	Описание
request	А s y n c SendMessageRequest	Да	
messageInfo	А s y n c SendMessageInfo	Да	Мета данные сообщения

messageId	xsd: string	Да	Идентификатор сообщения. Генерируется ШЭП. В случае отправки сообщения на ШЭП данное поле должно быть пустым. В случае передачи сообщения получателю номер будет проставлен ШЭП.
correlationId	xsd: string	Нет	Идентификатор цепочки сообщений. Генерируется ШЭП. В случае отправки сообщения типа REQUEST на ШЭП данное поле должно быть пустым. При отправке сообщений других типов на ШЭП, данное поле ДОЛЖНО БЫТЬ ЗАПОЛНЕНО. В случае передачи сообщения получателю номер будет проставлен ШЭП.
serviceId	xsd: string	Да	Идентификатор взаимодействия. По реестру сервисов ШЭП.
messageType	xsd: string	Да	Т и п с о о б щ е н и я : 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 ШЭП. Заполняется на ШЭП, отправителю заполнять не надо.
sender	SenderInfo	Да	Объект информация об отправителе (заполняется отправителем)
senderId	xsd: string	Да	Идентификатор отправителя (системы отправителя)
password	xsd: string	Нет	Пароль отправителя
properties	Property	Нет	Массив дополнительных свойств сообщения
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 (формат определяется системой получателя сообщения)

Ответ ШЭП на сообщение (sendMessageResponse) представляет собой массив элементов со следующими полями: Формат данных SendMessageResponse

Поле	Тип	Обязанность	Описание
response	Async SendMessageResponse	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 ШЭП

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

Поле	Тип	Обязанность	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

Метод приема уведомлений об изменении статуса сообщения в ШЭП (ChangeMessageStatusNotification)

Запрос уведомления об изменении статуса сообщения (ChangeMessageStatusNotificationRequest) представляет собой массив элементов со следующими полями: Формат данных ChangeMessageStatusNotificationRequest

Поле	Тип	Обязанность	Описание
request	Async ChangeMessageStatusNotificationRequest	Да	
notification	ChangeStatusNotification	Да	Уведомления о статусе доставки сообщения
notificationid	xsd: string	Да	Идентификатор уведомления
messageId	xsd: string	Да	Идентификатор сообщения
notificationDate	xsd: dateTime	Да	Дата создания уведомления
messageState	messageState	Да	Состояние сообщения
Status	messageStatusinfo	Да	Статус доставки (приема сообщения)
statusCode	xsd: string	Да	Код статуса
statusMessage	xsd: string	Да	Сообщения статуса
statusDate	xsd: dateTime	Да	Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой отправителя)
error		Нет	Информация об ошибке
errorCode	xsd: string	Да	Код ошибки
errorMessage	xsd: string	Да	Сообщение ошибки
errorData	xsd: string	Да	Дополнительное описание ошибки
errorDate	xsd: dateTime	Да	Дата ошибки
subError	xsd: string	Нет	Дочерняя ошибка
sessionId	guid	Нет	Идентификатор сессии в которой произошла ошибка
requestdate	xsd: dateTime	Да	Дата запроса
sessionid	guid	Нет	Идентификатор сессии

Ответ о принятии уведомления (changeMessageStatusNotificationResponse) представляет собой массив элементов со следующими полями: Формат данных ChangeMessageStatusNotificationResponse

Поле	Тип	Обязанность	Описание
response	Async ChangeMessageStatusNotificationResponse	Да	Ответ
responseDate	xsd: dateTime	Да	Дата ответа

sessionId	guid	Да	Идентификатор сессии (указанное в запросе)
-----------	------	----	--

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

Поле	Тип	Обязанность	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 сервиса на ШЭП:

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	Обязанность	Описание
request	SyncSendMessageRequest	Да	Запрос
requestInfo	SyncMessageInfo	Да	Информация о сообщении запроса
messageId	xsd: string	Да	Идентификатор сообщения в системе получателя (генерирует ШЭП)
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения в системе получателя запроса (Генерирует ШЭП)
serviceid	xsd: string	Да	Идентификатор взаимодействия (ведется в реестре сервисов ШЭП)
messageDate	xsd: dateTime	Да	Дата создания сообщения в Системе Отправителя (Инициатора взаимодействия). Заполняется Отправителем (инициатором взаимодействия).
routeId	xsd: string	Нет	Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой Отправителя, т.е. Инициатора взаимодействия)
sessionId	guid	Нет	Идентификатор сессии на ШЭП. Устанавливается на ШЭП.
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, можно добавить дополнительные свойства запроса (по согласованию с ШЭП и системой получателя)
key	xsd: int		Ключ свойства
value	xsd: int		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	Обязанность	Описание
response	SyncsendMessageresponse	Да	Ответ
responseInfo	SyncMessageInfoResponse	Да	Информация об ответе
messageId	xsd: string	Да	Идентификатор сообщения в системе получателя (заполняет система получателя запроса (система обрабатывающая сообщение))
correlationId	xsd: string	Нет	Идентификатор цепочки сообщения в системе получателя запроса (если сообщения существует в рамках цепочки сообщений системы отправителя (система обрабатывающая сообщение))
responseDate	xsd: dateTime	Да	Дата ответа в системе получателя запроса (заполняется системой получателя запроса)
sessionId	guid	Нет	Идентификатор сессии на ШЭП. Устанавливается на ШЭП. При отправке ответа системой получателя запроса заполнять не нужно.
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 получателя сообщения)

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

Поле	Тип	Обязанность	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

Описание сообщений.

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

Поле	Тип	Обязанность	Описание
request	SyncsendMessagerequest	Да	Запрос
requestInfo	SyncMessageInfo	Да	Информация о сообщении запроса

messageId	string	Да	Идентификатор сообщения в системе получателя (генерирует ШЭП)
serviceid	string	Да	Идентификатор взаимодействия (ведется в реестре сервисов ШЭП)
messegeDate	dateTime	Да	Дата создания сообщения в Системе Отправителя (Инициатора взаимодействия) Заполняется Отправителем (инициатором взаимодействия)
routeId	string	Нет	Идентификатор маршрута сообщения (если есть необходимость в дополнительной маршрутизации, идентификатор по реестру, заполняется системой Отправителя, т.е. Инициатора взаимодействия)
sender	senderinfo	Да	Объект информация об отправителе (заполняется отправителем)
senderId	string	Да	Идентификатор отправителя (системы отправителя)
password	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	Обязанность	Описание
response	SyncsendMessageresponse	Да	Ответ
responseInfo	SyncMessageInfoResponse	Да	Информация об ответе
messageId	string	Да	Идентификатор сообщения в системе получателя (заполняет система получателя запроса (система обрабатывающая сообщение))
responseDate	dateTime	Да	Дата ответа в системе получателя запроса (заполняется системой получателя запроса)
message	string	Да	Сообщение о статусе
responseData	responsedata	Да	Объект "данные ответа"
data	Anytype	Нет	Объект данные сообщения (формат определяется системой получателя сообщения)

Приложение 2 к Правилам
интеграции объектов
информатизации "электронного
правительства"
Форма

Требования к взаимодействию с сервисом

Сведения о публикуемом сервисе (с учетом сведений на архитектурном портале "электронного правительства")	
1	Владелец сервиса
2	Наименование информационной системы
3	Контур взаимодействия

4	Ключ сервиса
5	Режим взаимодействия сервиса
6	Наименование сервиса, на русском языке
7	Наименование сервиса, на казахском языке
8	Назначение сервиса, на русском языке
9	Назначение сервиса, на казахском языке
10	Бизнес описание работы сервиса, на русском языке
11	Бизнес описание работы сервиса, на казахском языке
Рекомендуемые требования по производительности и надежности синхронного сервиса:	
Контролируемый показатель	
12	Максимальное время обработки запроса при синхронном взаимодействии
13	Среднее время обработки запроса
14	Пиковая нагрузка
15	Номинальная нагрузка
16	Среднее время работы без сбоев
17	Время на восстановление работоспособности
18	Требования по использованию ЭЦП Требования по информационной безопасности Требования к формату Журнала логирования Требования со стороны ШЭП/ВШЭП

В таблице 1 приведены требования по производительности и надежности синхронного сервиса.

Таблица 1 – Требования по производительности и надежности синхронного сервиса

№	Контролируемый показатель	Ограничение
1	Максимальное время обработки запроса при синхронном взаимодействии	до 30 секунд
2	Среднее время обработки запроса	10 секунд
3.	Пиковая нагрузка	2000 запросов в час
4.	Номинальная нагрузка	360 запросов в час
5	Среднее время работы без сбоев	365/7/24
6	Время на восстановление работоспособности	3 часа

Таблица 2 – 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	2000 запросов в час
3	Номинальная нагрузка	360 запросов в час
4	Среднее время работы без сбоев	365/7/24
5	Время на восстановление работоспособности	3 часа

Заявка на публикацию сервиса

1. Владелец сервиса	
1	Наименование организации
2	ИИН/БИН
3	Должностное лицо, ответственное за эксплуатацию
2. Информационная система Владельца сервиса	
4	Корневая категория сервиса
5	Контактные данные разработчика сервиса
6	Ресурс разработчика сервиса
7	Наименование системы
8	Логин системы
9	Пароль (тестовая среда)
10	Пароль (промышленная среда)
11	IP-адрес системы (тестовая среда)
12	Порт системы (тестовая среда)
13	Протокол (тестовая среда)
14	IP-адрес системы (промышленная среда)
15	Порт системы (промышленная среда)
16	Протокол (промышленная среда)
17	Сертификат открытого ключа транспортной ЭЦП системы (выданных Национальным удостоверяющим центром Республики Казахстан)
18	Акт по результатам испытаний на соответствие требованиям информационной безопасности
19	Имеется ли доступ до ШЭП (да/нет)
3. Электронный сервис	
20	Наименование сервиса
21	Описание сервиса
22	Ключ сервиса
23	Режим взаимодействия сервиса
24	Опубликовать сервис на ВШЭП (да/нет)
25	Опубликовать сервис на ШЭП (да/нет)
26	Сервис предоставляет персональные данные (да/нет)
26.1	XPath-путь к элементу, содержащему ИИН
26.2	Предусмотрена отправка SMS гражданам для получения разрешения на предоставление их персональных данных (да/нет)
27	Признак наличия маршрутизации сообщений (да/нет)
27.1	Ключ маршрута
27.2	Наименование URL сервиса, принимающего запросы (тестовая среда)
27.3	URL сервиса, принимающего запросы (тестовая среда)

27.4	Наименование URL сервиса, принимающего запросы (промышленная среда)
27.5	URL сервиса, принимающего запросы (промышленная среда)
28	Наличие авторизации на стороне сервиса (да/нет)
28.1	Метод авторизации
28.2	Логин
28.3	Пароль
29	Тип безопасности
30	SSL сертификат (выданных Национальным удостоверяющим центром Республики Казахстан)
31	XSD
32	Пример запроса
33	Пример ответа
4. Клиент сервиса	
34	Наименование организации, ИИН/БИН
5. Данные VPN-туннеля	
35	Имеется VPN-туннель для данной системы (да/нет)
36	Информация о шлюзе VPN
37	Режим туннеля
38	Публичный Peer IP-адрес
5.1 Свойства туннеля Фаза 1	
39	Метод аутентификации
40	Частный общий ключ
41	Тип криптографии
42	Протокол Деффи-Хеллмана
43	Криптографический алгоритм
44	Алгоритм хеширования
45	Срок действия (для пересмотра построения туннеля)
5.2 Свойства туннеля Фаза 2	
46	Инкапсуляция
47	Криптографический алгоритм
48	Метод алгоритма
49	Группа совершенной прямой секретности
50	Срок действия (для пересмотра построения туннеля)
51	Величина в Кб (для пересмотра построения туннеля)

Приложение 4 к Правилам
интеграции объектов
информатизации "электронного
правительства"

Акт тестирования и ввода в эксплуатацию

1.	Участники информационного взаимодействия:
1.1.	Наименование владельца сервиса
1.2.	Наименование инициатора интеграционного сервиса

2.	Информационные системы:
2.1.	Информационная система владельца сервиса
2.2.	Информационная система инициатора интеграционного сервиса
3.	Сервисы тестирования:
3.1.	Наименование сервиса
3.2.	Ключ сервиса
4	Сценарий тестирования
5	Решение по результатам тестирования
6	Дата перевода в промышленную среду

Приложение 5 к Правилам
интеграции объектов
информатизации "электронного
правительства"

Заявка на подключение/интеграцию к сервису

1. Владелец сервиса	
1	Наименование организации
2	ИИН/БИН
2. Инициатор интеграционного сервиса	
3	Наименование организации
4	ИИН/БИН
5	Основание для подключения
6	ФИО ответственного лица
7	Контактный телефон ответственного лица
8	Электронная почта ответственного лица
3. Информационная система инициатора интеграционного сервиса	
9	Наименование системы
10	Логин системы
11	Пароль (тестовая среда)
12	Пароль (промышленная среда)
13	IP-адрес системы (тестовая среда)
14	Порт системы (тестовая среда)
15	Протокол (тестовая среда)
16	IP-адрес системы (промышленная среда)
17	Порт системы (промышленная среда)
18	Протокол (промышленная среда)
19	Контур взаимодействия
20	Имеется ли доступ до ШЭП
21	Имеется ли VPN-туннель для данной системы
22	Прикрепите сертификат открытого ключа транспортной ЭЦП системы (выданных Национальным удостоверяющим центром Республики Казахстан)

23	Прикрепите акт по результатам испытаний на соответствие требованиям информационной безопасности (.doc, .docx, .pdf)
4. Электронный сервис	
24	Ключ сервиса
25	Режим взаимодействия сервиса
26	Сервис предоставляет персональные данные
27	Предусмотрена отправка SMS гражданам для получения разрешения на предоставление их персональных данных
5. Данные VPN-туннеля	
28	Информация о шлюзе VPN
29	Режим туннеля
30	Публичный Peer IP-адрес
5.1	Свойства туннеля Фаза 1:
31	Метод аутентификации
32	Частный общий ключ
33	Тип криптографии
34	Протокол Деффи-Хеллмана
35	Криптографический алгоритм
36	Алгоритм хеширования
37	Срок действия (для пересмотра построения туннеля)
5.2	Свойства туннеля Фаза 2:
38	Инкапсуляция
39	Криптографический алгоритм
40	Метод алгоритма
41	Группа совершенной прямой секретности
42	Срок действия (для пересмотра построения туннеля)
43	Величина в Кб (для пересмотра построения туннеля)

Приложение 6 к Правилам
интеграции объектов
информатизации "электронного
правительства"

Сценарий использования транспортной подписи

1. Сценарий приема сообщения с использованием транспортной подписи ШЭП:
 - 1) ШЭП проверяет сообщение (авторизацию, валидацию конверта сообщения, транспортную подпись объектов информатизации);
 - 2) ШЭП подписывает сообщение транспортной подписью;
 - 3) ШЭП передает подписанное сообщение ВШЭП (при взаимодействии с ИС вне ЕТС ГО);
 - 4) ВШЭП проверяет сообщение (авторизацию, валидацию конверта сообщения, транспортную подпись объектов информатизации).
- Данный сценарий используется при взаимодействии объектов информатизации.

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

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

2) ШЭП проверяет транспортную подпись сообщения:

проверяет соответствие ИИН/БИН указанного в ЭЦП ИИН/БИН-а, внесенного в систему при регистрации объекта информатизации;

проверяет транспортную подпись на действительность (онлайн проверка действительности подписи или проверка по списку отозванных сертификатов).

3. Сценарий приема сообщения с использованием транспортных подписей ШЭП, кроме сервисов, реализованных с использованием REST технологии, и вызывающей стороны, с использованием метода шифрования сообщений:

1) отправитель сообщения шифрует сообщение;

2) отправитель сообщения подписывает сообщения транспортной подписью и отправляет ШЭП;

3) ШЭП расшифровывает сообщение;

4) ШЭП проверяет транспортную подпись сообщения:

проверяет соответствие ИИН/БИН указанного в ЭЦП на ИИН/БИН-а, внесенного в систему при регистрации объекта информатизации;

проверяет транспортную подпись на действительность (онлайн проверка действительности подписи или проверка по списку отозванных сертификатов).