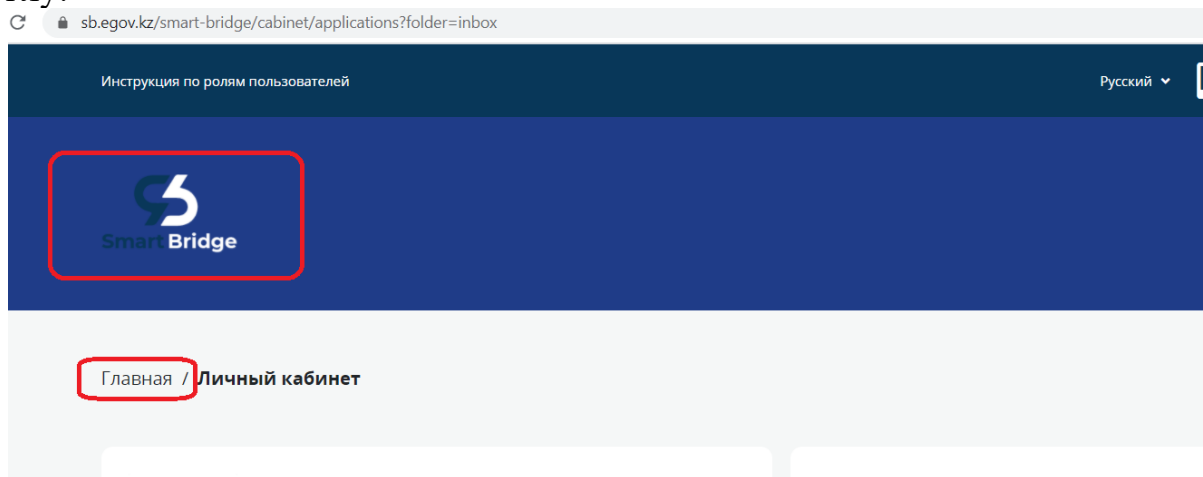


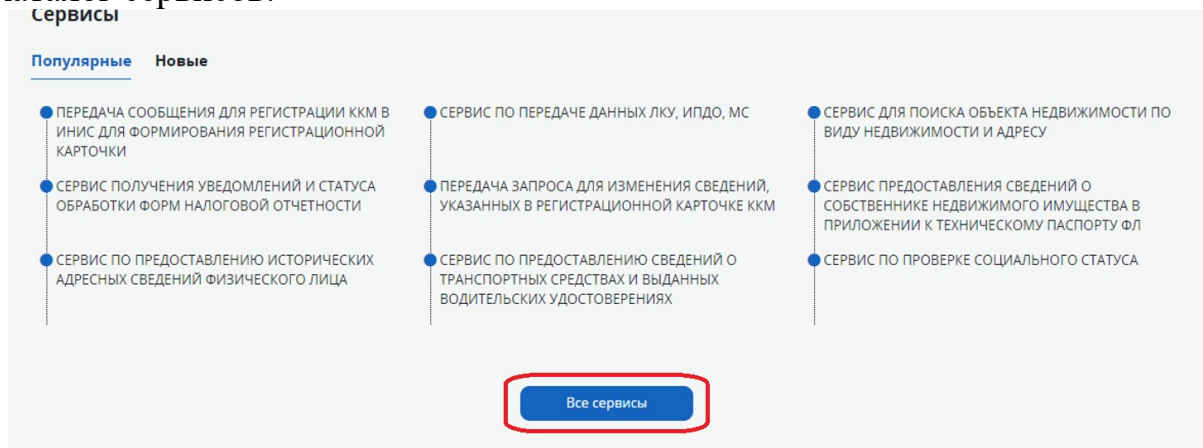
Инструкция по подаче заявки на подключение к сервису

Настоящая инструкция по подаче заявки на подключение к сервису предназначена для владельцев информационных систем (Клиентов сервиса).

Для подачи заявки на подключение к сервису необходимо найти его паспорт в Каталоге сервисов. Для этого следует открыть Главную страницу портала нажатием на кнопку «Главная» или иконку портала в левом верхнем углу:



На Главной странице с помощью кнопки «Все сервисы» перейти в Каталог сервисов:



В Каталоге сервисов следует найти паспорт нужного сервиса интеграции. Паспорт сервиса можно найти путем ввода в строку поиска слов из наименования/назначения сервиса или ключа сервиса (ключ сервиса – это уникальный идентификатор, под которым веб-сервис опубликован на ШЭП).

Также возможен поиск в Каталоге сервисов по категориям, по Владелецам и по информационным системам сервисов:

После того, как найден нужный паспорт сервиса, необходимо открыть его. В паспорте сервиса отображается общая информация о сервисе интеграции: наименование сервиса, организация-Владелец сервиса, контактные лица от Владельца и разработчика веб-сервиса, информационная система, назначение, ключ сервиса, режим взаимодействия (синхронный или асинхронный), контур взаимодействия (в ЕТС или вне ЕТС ГО), EPIR ID (уникальный идентификатор сервиса в ЕПИР, Единой платформе интернет-ресурсов ГО), а также файлы, необходимые для разработки веб-сервиса подключения – xsd, xml примеров запроса и ответа:

Если пользователь не авторизован на портале, то при попытке скачивания файлов xsd, xml портал Smart Bridge переведет пользователя на страницу авторизации (входа в личный кабинет).

Предполагается, что сначала из паспорта нужного сервиса скачиваются файлы xsd, xml, затем разрабатывается веб-сервис подключения к сервису,

далее подается заявка на подключение к сервису.

Для инициирования заявки на подключение к выбранному сервису необходимо в его паспорте нажать на кнопку «Подключиться»:

Гибридная электронная почта

Владелец АО «Казпочта»	Контактное лицо владельца АО Казпочта Департамент е-сервисов Баякеева Асель Сериковна (a.bayekeyeva@kazpost.kz)	Контактное лицо разработчика АО Казпочта Илья Культе, ПМ разработчиков(i.kulte@alabs.team)	Подключиться
Информационная система Гибридная электронная почта	Назначение сервиса Гибридная электронная почта это бумажная почта, доставляемая получателю с применением электронных средств	Ключ сервиса GEP_kazpost	Взаимосвязанные сервисы
Режим взаимодействия Синхронный	Контур взаимодействия Вне ETC ГО	EPIR ID KAZPOST-S-1901	

[Требования](#) [XSD](#) [Пример запроса](#) [Пример ответа](#) [Формат данных](#)

🚩 Сервис предоставляет персональные данные: Нет

Отобразится страница «Требования к взаимодействию с сервисом»:

Smart Bridge

Главная / Паспорт сервиса / Паспорт сервиса /

Требования к взаимодействию с сервисом

Сведения о сервисе

Владелец сервиса

Республиканское государственное учреждение "Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан"

Наименование информационной системы

Информационная система

Электронные сервисы

Сервис №1

Наименование сервиса

! Одностороннее выставление Требований со стороны Владельца сервиса, а также подписание на портале Smart Bridge акта тестирования заменяют заключение Соглашения между участниками интеграции.

Страница «Требования к взаимодействию с сервисом» содержит общую информацию о сервисе из его паспорта, а также требования к

интеграции с выбранным сервисом: рекомендуемые требования по производительности и надежности, требования по использованию ЭЦП, требования по информационной безопасности, требования к формату Журнала логирования, требования со стороны ШЭП:

Требования к взаимодействию с сервисом

Сведения о сервисе

Владелец сервиса

АО «Казпочта»

Наименование информационной системы

Гибридная электронная почта

Электронные сервисы

Гибридная электронная почта x | v

Сервис №1

Наименование сервиса

Гибридная электронная почта

Ключ сервиса

GEP_kazpost

Режим взаимодействия сервиса

Синхронный

Контур взаимодействия

вне ЕТС ГО

Назначение сервиса

Гибридная электронная почта это бумажная почта, доставляемая получателю с применением электронных средств

Бизнес описание работы сервиса

Рекомендуемые требования по производительности и надежности		
Контролируемый показатель	Шлюз «электронного правительства»	Информационная система
Максимальное время обработки запроса (заполняется только для синхронных)	30 сек.	30 сек.
Среднее время обработки запроса	10 сек.	10 сек.
Пиковая нагрузка (Максимальное допустимое количество запросов, принимаемых и обрабатываемых)	2000 запросов в час	2000 запросов в час
Номинальная нагрузка (Оптимальное количество запросов в час)	360 запросов в час	360 запросов в час
Среднее время работы без сбоев	365/7/24 доступность	365/7/24 доступность
Время на восстановление работоспособности	3 часов	1 часов

Требования по использованию ЭЦП

Проверка должна осуществляться в соответствии с требованиями Приказа Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи»;

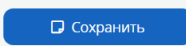
Электронные сообщения между участниками информационного обмена должны проверяться по следующим правилам:

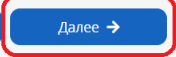
- Структура электронного документа должна соответствовать XML формату. Подпись документа должна осуществляться по стандарту XML design и спецификации консорциума W3C «XML — Signature Syntax and Processing» («Синтаксис и обработка подписи XML»), см. ссылку <http://www.w3.org/TR/xmlsig-core/>. В случае применения стандарта хранения юридически значимых документов (CadES), должен использоваться формат XadES (XML Advanced Electronic Signatures), спецификация которого отражена в технической документации ETSI TS 101 903 V1.2.2 (2004-04).
- При проверке электронной цифровой подписи в электронном документе должно использоваться подписанное сообщение, ключ проверки и параметры схемы ЭЦП и результатом которого должно являться заключение о правильности или ошибочности цифровой подписи (ГОСТ 34.310-2004, определение).
- Регистрационное свидетельство должно быть выдано на имя Отправителя. Должна производиться проверка ИИН/БИН Отправителя с ИИН/БИН в регистрационном свидетельстве.
- Срок действия проверяемого регистрационного свидетельства не должен истечь. Должна быть проверка полей NotBefore и NotAfter. Проверка должна осуществляться по времени Астаны.
- Должна быть проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого со всеми промежуточными регистрационными свидетельствами. Регистрационное свидетельство должно быть удостоверено ЭЦП (выпущено НУЦ РК).
- Проверяемое регистрационное свидетельство не должно быть отозванным. Проверка должна осуществляться с помощью получения OCSP квитанции, путем обращения к сервису НУЦ РК. При повторных проверках данного ЭЦП должна быть возможность использовать ранее полученную OCSP квитанцию – в этом случае проверка должна осуществляться на дату получения квитанции. В случае недоступности сервиса OCSP должна осуществляться проверка по списку отозванных регистрационных свидетельств в Base CRL и Delta CRL (Проверка наличия серийного номера регистрационного свидетельства в Base CRL и Delta CRL НУЦ РК). Base CRL и Delta CRL НУЦ необходимо подкачивать по пути указанному в проверяемом регистрационном свидетельстве.

На данной странице не требуется ничего вводить, следует согласиться с данными требованиями и нажать на кнопку «Далее»:

- Должна быть проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого со всеми промежуточными регистрационными свидетельствами. Регистрационное свидетельство должно быть удостоверено ЭЦП (выпущено НУЦ РК).
- Проверяемое регистрационное свидетельство не должно быть отозванным. Проверка должна осуществляться с помощью получения OCSP квитанции, путем обращения к сервису НУЦ РК. При повторных проверках данного ЭЦП должна быть возможность использовать ранее полученную OCSP квитанцию – в этом случае проверка должна осуществляться на дату получения квитанции. В случае недоступности сервиса OCSP должна осуществляться проверка по списку отозванных регистрационных свидетельств в Base CRL и Delta CRL (Проверка наличия серийного номера регистрационного свидетельства в Base CRL и Delta CRL НУЦ РК). Base CRL и Delta CRL НУЦ необходимо подкачивать по пути указанному в проверяемом регистрационном свидетельстве.

☒ **Соглашаюсь с данными требованиями**

 Сохранить

 Далее →

Отобразится страница «Заявка на подключение к сервису» для заполнения заявки:

Главная / Паспорт сервиса / Паспорт сервиса /

Заявка на подключение к сервису

Владелец сервиса

Наименование организации
Республиканское государственное учреждение

БИН/ИИН организации

Клиент сервиса

Наименование организации
Акционерное общество

На странице «Заявка на подключение к сервису» поля, выделенные заливкой серого цвета, заполнять не требуется (они получены автоматически из паспорта сервиса и ЭЦП сотрудника, инициировавшего заявку). Необходимо заполнить все обязательные поля, отмеченные красной звездочкой *. Ниже в настоящей инструкции приведены пояснения к заполнению полей заявки.

При частичном заполнении заявки возможно сохранить заявку (кнопка «Сохранить»). Черновик (проект) заявки сохранится в папке «Проекты» вкладки «Мои заявки» в личном кабинете. Проект заявки позже можно заполнить и подписать ЭЦП. **При этом проект заявки отображается только для сотрудника, инициировавшего ее.** Проект заявки можно удалить с помощью кнопки в виде корзины:

	Входящие	Исходящие	На ознакомление	Рассмотренные	На доработке	Исполненные	Проекты
Мои заявки							10
	№ проекта	Дата создания	Дата обновления	Инф. система	Сервис	Вид заявки	
Мои сервисы	1	D202000932951	2020-11-30 15:35	2020-11-30 15:35	Гибридная электронная почта	KAZPOST-S-1901	Подключение

После заполнения всех обязательных полей становится активной кнопка «Далее» для перехода на страницу проверки введенных данных. В случае корректного заполнения нажать на кнопку «Подписать ЭЦП».

После подписания заявка переместится в папку «Исходящие» вкладки «Мои заявки»:

Опубликовать	Входящие	Исходящие	На ознакомление	Рассмотренные	На доработку	Исполненные	Проекты
Мои заявки							10
Мои сервисы	№ заявки	Дата создания заявки	Инф. система	Сервис	Заявитель	Вид заявки	Тип заявки
Мои подключения	1	202000915824 2020-11-24 17:30		MON-A-0384		Подключение	Продуктив
							МОН РК

Подписанные заявки отображаются в личном кабинете организации всем сотрудникам, которые имеют ЭЦП сотрудника юридического лица.

! На портале Smart Bridge имеется возможность самостоятельного отслеживания заявки, подробнее описано в соответствующей инструкции раздела Помощь портала.

После подписания заявка на подключение к сервису поступает на рассмотрение к Владелцу сервиса.

Владелец сервиса должен рассмотреть заявку в течение двух рабочих дней. При этом, Владелец сервиса имеет возможность отказать или отправить заявку на доработку с указанием причины, а также согласовать реализацию интеграции.

После согласования Владелцем сервиса заявка поступает на рассмотрение в АО «НИТ». В случае корректного заполнения заявка принимается в работу АО «НИТ», проводятся работы по проверке технической возможности интеграции, организации доступа по сети и подключению Клиента к сервису на тестовой среде ШЭП/ВШЭП.

Затем Клиент и Владелец сервиса проводят тестирование, в рамках текущей заявки подписывают акт тестирования (инициирует Клиент сервиса). Далее АО «НИТ» на основании акта тестирования и наличия сообщений на тестовом ШЭП/ВШЭП подключает Клиента к сервису. После жизненный цикл заявки завершается, и она переходит в папку «Исполненные» в личном кабинете инициатора заявки.

Пояснения к заполнению полей заявки

«*Основание для подключения*» – это документ, на основании которого реализуется данная интеграция, т.е. протокол, официальное письмо, дорожная карта, приказ и т.д. Например, письмо МЦРИАП РК исх. № 12345 от 05.05.2020 г. касательно интеграции ИС ЕСЭДО и ИС ГС, протокол совещания №1 от 10.10.2020 г.

«*Прикрепить основание для подключения (.doc, .docx, .pdf, .zip, .7z, .gz, .tar)*» – это не обязательное поле, в нем прикрепляется файл основания, например, файл с письмом в формате MS Word. Поддерживается прикрепление файлов с расширениями: .doc, .docx, .pdf, .zip, .7z, .gz, .tar.

«Контактный телефон», «Email» – здесь указываются данные лица, которое компетентно ответить на вопросы по данным в подаваемой заявке:

«Наименование информационной системы» – необходимо выбрать из выпадающего списка информационную систему, которая будет взаимодействовать с выбранным веб-сервисом:

При отсутствии информационной системы в выпадающем списке необходимо добавить ее с помощью кнопки «Добавить инф.систему». Процесс добавления информационной системы описан подробнее в соответствующей инструкции раздела Помощь портала Smart Bridge.

В случае возникновения ошибки следует направить текст, которым заполняются поля в окне добавления системы, а также БИН, который отображается в личном кабинете Smart Bridge, на почту поддержки sb.egov@nitech.kz для добавления системы вручную.

«Логин системы» – это логин системы, под которым она будет заведена на ШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Логин системы должен быть идентичным в тестовой и промышленной среде ШЭП. Логин должен содержать как минимум 3 символа, допускается использование только строчных и прописных букв латинского алфавита и цифр.

«Пароль (тест)» – это пароль системы для ее авторизации в тестовой

среде ШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Пароль должен содержать как минимум 8 символов.

«Пароль (продуктив)» – это пароль системы для ее авторизации в промышленной среде ШЭП, необходимо придумать его и ввести в поле (также сохранить у себя для информации). Пароль должен содержать как минимум 8 символов.

! Если ранее до внедрения портала «Smart Bridge» уже публиковались веб-сервисы данной системы на ШЭП либо проводилось ее подключение к веб-сервисам на ШЭП, то у нее уже имеются авторизационные данные, их необходимо ввести в полях логина и паролей системы.

Следует отметить, что после проведения работ на тестовой среде ШЭП по данной заявке логин системы сохраняется на портале «Smart Bridge». Логин будет отображаться при выборе системы как нередактируемое поле, а поля паролей отображаться не будут:

Информационная система клиента сервиса

* Наименование информационной системы

SmartBridge

Добавить инф. систему

* Логин системы

smartbridge

* IP-адрес системы (тест)

* IP-адрес системы (продуктив)

«IP-адрес системы (тест)» – это IP-адрес системы в тестовой среде. Необходимо указать **IP-адрес**, это должен быть IP-адрес сервера тестовой системы, с которого будут отправляться сообщения типа «запрос».

«IP-адрес системы (продуктив)» – это IP-адрес системы в тестовой среде. Необходимо указать **IP-адрес**, это должен быть IP-адрес сервера промышленной системы, с которого будут отправляться сообщения типа «запрос».

Примечание: Нужно обязательно выбрать контур взаимодействия.

Тестовая среда

☒ в ЕТС ☐ вне ЕТС ☐ хостинг НИТ

* Публичный IP-адрес системы

* Порт

* Протокол

Добавить дополнительный IP (тест)

Продуктивная среда

☒ в ЕТС ☐ вне ЕТС ☐ хостинг НИТ

* Публичный IP-адрес системы

* Порт

* Протокол

Добавить дополнительный IP (прод)

! В соответствии с требованиями информационной безопасности контуры взаимодействия тестовой и промышленной сред системы

должны совпадать (и тестовая и промышленная системы должны располагаться в одном контуре). В противном случае заявка будет отправлена АО «НИТ» на доработку.

«Порт системы (тест)» – это порт, по которому для Клиента будет организовываться доступ к сервису по сети в тестовой среде ШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения.

«Порт системы (продуктив)» – это порт, по которому для Клиента будет организовываться доступ к сервису по сети в промышленной среде ШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения.

При наличии нескольких портов возможно указание их через запятую без символа пробела (пример: 80,8080,8090).

«Протокол (тест)» – это протокол, по которому для Клиента будет организовываться доступ к сервису по сети в тестовой среде ШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения, чаще используется TCP протокол.

«Протокол (продуктив)» – это протокол, по которому для Клиента будет организовываться доступ к сервису по сети в промышленной среде ШЭП. Это поле заполняется на усмотрение разработчика веб-сервиса подключения, обычно используется TCP протокол.

При указании контура взаимодействия Вне ЕТС будут доступны поля для заполнения данных по VPN- туннелю.

«Имеется VPN-туннель для данной системы?» – Переключатель «нет»/«да». В случае отсутствия VPN-туннеля отображается ссылка на «Технические условия для организации VPN соединения».

Блок полей Данные VPN-туннеля. Большая часть полей данного

блока заполняется системой автоматически. Данные для заполнения полей предоставляет специалист, обладающий знаниями сетевой инфраструктуры.

«*Информация о шлюзе VPN*» – **обязательное поле**, это модель оборудования, где будет организован VPN-туннель. Например, CISCO ASA123.

«*Режим туннеля*» – заполняется автоматически значением «TUNNEL».

«*Публичный Peer IP-адрес*» – **обязательное поле**, это публичный (белый) IP-адрес устройства, на котором будет организован VPN-туннель.

«*Фаза 1: Метод аутентификации*» – заполняется автоматически значением «PSK(Pre-shared key)».

«*Фаза 1: Частный общий ключ*» – сложный пароль для получения доступа к VPN-туннелю. Способ его передачи указывается по умолчанию, заполняется автоматически значением «Нарочно».

«*Фаза 1: Тип криптографии*» – заполняется автоматически значением IKEv2 .

«*Фаза 1: Протокол Деффи-Хеллмана*» – заполняется автоматически согласно типу криптографии: IKEv2 - Group 14.

«*Фаза 1: Криптографический алгоритм*» – алгоритм преобразования данных, заполняется автоматически значением AES-256.

«*Фаза 1: Алгоритм хеширования*» – алгоритм хэширования данных, заполняется автоматически значением SHA256.

«*Фаза 1: Срок действия (для пересмотра построения туннеля)*» – заполняется автоматически значением «default». Это время жизни ключа сеанса – сколько времени должно пройти до смены ключа. Значение по умолчанию равно 86400 секунд.

«*Фаза 2: Инкапсуляция*» – заполняется автоматически значением «ESP (Encapsulating Security Payload)».

«*Фаза 2: Криптографический алгоритм*» – алгоритм преобразования данных, заполняется автоматически значением AES-256.

«*Фаза 2: Метод алгоритма*» – алгоритм хэширования данных, заполняется автоматически значением SHA256.

«*Фаза 2: Группа совершенной прямой секретности*» – заполняется автоматически согласно типу криптографии: IKEv2 - Group 14.

«*Фаза 2: Срок действия (для пересмотра построения туннеля)*» – заполняется автоматически значением «default». Это время жизни ключа сеанса – сколько времени должно пройти до смены ключа. Значение по умолчанию равно 86400 секунд.

«*Фаза 2: Величина в Кб (для пересмотра построения туннеля)*» – заполняется автоматически значением «default».

«*Имеется ли доступ до ШЭП?*» – переключатель следует передвинуть в активное положение, если система ранее была заведена на ШЭП (публиковались сервисы системы на ШЭП либо проводилась интеграция посредством ШЭП):

«*Прикрепите сертификат открытого ключа транспортной ЭЦП*

системы (.cer; .crt)» - файл с расширением .cer или .crt, скачанный на сайте Национального удостоверяющего центра РК pki.gov.kz.

Если у ИС отсутствует транспортная подпись, то в качестве транспортной может быть выбрана ЭЦП первого руководителя или любого сотрудника с правом подписи документов. Необходимо из ключа GOST для подписания извлечь открытую (публичную) часть на сайте НУЦ РК. Подробнее процесс извлечения открытой части транспортной ЭЦП описан в соответствующей инструкции раздела Помощь портала Smart Bridge.

«Прикрепите акт по результатам испытаний на соответствие требованиям информационной безопасности (.doc, .docx, .pdf)» - необязательное поле, обязательно для государственных ИС.

Блок полей «Электронные сервисы».

«Наименование сервиса» – наименование сервиса в его паспорте, поле для информации заявителю, заполняется автоматически.

«Ключ сервиса» – ключ сервиса на ШЭП/ВШЭП, поле для информации заявителю, заполняется автоматически.

«Режим взаимодействия сервиса» – синхронный или асинхронный, поле для информации заявителю, заполняется автоматически.

«Сервис предоставляет персональные данные» – признак использования персональных данных граждан при передаче данных сервисом. Поле для информации заявителю, заполняется автоматически

«Предусмотрена отправка SMS гражданам для получения разрешения на предоставление их персональных данных» – признак использования механизма отправки SMS при отправке запроса на получение разрешения на предоставление персональных данных. Поле для информации заявителю, заполняется автоматически

«Режим отправки сообщений» – выберите метод PULL или PUSH. Метод PULL – система Клиента самостоятельно извлекает из ШЭП/ВШЭП адресованные ей сообщения.

Метод PUSH – ШЭП/ВШЭП отправляет ответы на запросы системе Клиента. В случае выбора метода отправки сообщений PUSH, необходимо заполнить следующие поля:

«Признак наличия маршрутизации сообщений» – переключатель «нет»/«да». Указывается «да», если по одному сервису есть несколько адресов доставки. В случае наличия признака маршрутизации сообщений необходимо заполнить поле:

«Ключ маршрута» – условное обозначение ключа маршрута для дальнейшей идентификации. Заполнять на латинице с использованием цифр.

«Наименование URL сервиса, принимающего ответы (тест)» – заполняется автоматически.

«URL сервиса, принимающего ответы (тест)» – необходимо указать URL системы, принимающей ответы в тестовой среде.

«Наименование URL сервиса, принимающего ответы (прод)» – заполняется автоматически.

«URL сервиса, принимающего ответы (прод)» – необходимо указать URL системы, принимающей ответы в промышленной среде.

В случае наличия нескольких адресов доставки по одному сервису необходимо нажать кнопку  и заполнить отобразившиеся поля.

«Наличие авторизации на стороне сервиса» – переключатель «нет»/«да». В случае наличия авторизации на стороне сервиса необходимо заполнить поля:

«Метод авторизации» – необходимо выбрать «Basic» или «Digest» авторизация;

«Логин» – следует указать логин для авторизации ИС;

«Пароль» – следует указать пароль для авторизации ИС.

«Тип безопасности» – тип безопасности, который будет использоваться при передаче данных, выбрать «По логину и паролю» или «Транспортная подпись ГОСТ».

«Необходимость получения уведомления ИС-отправителей сообщений об изменении статусов сообщений от ШЭП» – переключатель «нет»/«да».

«Необходимость получения дополнительного уведомления о доставке от ШЭП» – переключатель «нет»/«да». Указать «да» в случае необходимости получения от ШЭП уведомлений о доставке запросов системы Клиента в систему Владельца сервиса.

«Прикрепите SSL сертификат» – прикрепите открытую часть сертификата безопасности (ключа GOST), файл с расширением .cer или .crt.