**Методические рекомендации по работе**

**с электронным сервисом**

**Интеграционного шлюза**

Версия 2.0

На 23 листах

**2021**

**ОГЛАВЛЕНИЕ**

[1 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОГЛАШЕНИЯ 4](#_Toc69131830)

[2 ОСНОВЫ ВЗАИМОДЕЙСТВИЯ 6](#_Toc69131831)

[2.1 Типы сообщений 6](#_Toc69131832)

[2.1.1 Сообщения типа «Запрос» 6](#_Toc69131833)

[2.1.2 Сообщения типа «Ответ» 6](#_Toc69131834)

[3 ТРЕБОВАНИЯ К СТРУКТУРЕ СООБЩЕНИЙ 7](#_Toc69131835)

[3.1 Общие положения 7](#_Toc69131836)

[3.2 Структура сообщения с запросом, которое ИС потребителя передает в Шлюз 8](#_Toc69131837)

[3.2.1 Блок данных запроса 8](#_Toc69131838)

[3.2.2 Электронная подпись органа власти 9](#_Toc69131839)

[3.3 Структура с ответом, которое ИС потребителя получает из Шлюза 9](#_Toc69131840)

[3.3.1 Блок данных СМЭВ-конверта 10](#_Toc69131841)

[3.3.2 Блок данных ответа 11](#_Toc69131842)

[3.3.3 Электронная подпись Шлюза 12](#_Toc69131843)

[4 ЭЛЕКТРОННЫЕ ПОДПИСИ 13](#_Toc69131844)

[4.1 Виды электронных подписей 13](#_Toc69131845)

[4.2 Порядок использования электронных подписей при передаче запроса 13](#_Toc69131846)

[4.3 Правила формирования ЭП 14](#_Toc69131847)

[4.4 Электронные подписи субъектов взаимодействия – физических лиц 15](#_Toc69131848)

[4.4.1 Общие требования к электронной подписи, формируемой от имени должностных лиц органов власти при межведомственном информационном обмене 15](#_Toc69131849)

[4.4.2 Электронная подпись при межведомственном взаимодействии 15](#_Toc69131850)

[4.5 Электронные подписи субъектов взаимодействия – информационных систем 16](#_Toc69131851)

[4.5.1 Общие требования электронной подписи, формируемой от имени органа власти при межведомственном информационном обмене 16](#_Toc69131852)

[4.5.2 Общие требования к электронной подписи, формируемой Шлюзом 16](#_Toc69131853)

[4.5.3 Правила формирования электронной подписи информационной системы 17](#_Toc69131854)

[5 СЦЕНАРИЙ АСИНХРОННОГО ВЗАИМОДЕЙСТВИЯ 18](#_Toc69131855)

[6 ПРИЛОЖЕНИЯ 20](#_Toc69131856)

[6.1 Приложение 1. Адреса 20](#_Toc69131857)

[6.2 Приложение 2. Виды сведений 20](#_Toc69131858)

[6.3 Приложение 3. Перечень ошибок, возвращаемых Шлюзом 21](#_Toc69131859)

**ИЗМЕНЕНИЯ**

| **Версия** | **Дата** | **Автор** | **Изменения** |
| --- | --- | --- | --- |
| 1.0 | 13.11.2018 | Цыренжапова С.Б. | Первая версия документа |
| 1.1 | 25.02.2019 | Цыренжапова С.Б. | Обновлен раздел 6.1  Добавлен раздел 6.2  Добавлен раздел 6.3 |
| 1.2 | 18.04.2019 | Цыренжапова С.Б. | Обновлен раздел 6.2 (ссылки на ВС версии 2.1)  Удален раздел 6.3  Добавлен раздел «Изменения» |
| 1.3 | 24.06.2019 | Цыренжапова С.Б. | Обновлен раздел 6.2 (ссылки на ВС версии 2.1.1) |
| 2.0 | 12.04.2021 | Кугаева Д.С. | Обновлен раздел 6.2 (ссылки на ВС версии 2.2.0) |

# ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОГЛАШЕНИЯ

В документе используются следующие термины и определения:

|  |  |
| --- | --- |
| Веб-сервис (электронный сервис) | Идентифицируемая веб-адресом программная система со стандартизированными интерфейсами. См. также http://www.w3.org/2002/ws/ |
| Электронный сервис Интеграционного шлюза (Шлюз) | Веб-сервис, предназначенный для обеспечения информационного взаимодействия Шлюза с ИС Потребителей посредством сообщений, основанных на протоле SOAP, в соответствии с настоящими Методическими рекомендациями |
| ИС | Информационная система |
| СМЭВ | Система межведомственного электронного взаимодействия |
| ОВ | Орган власти |
| ОИВ | Органы исполнительной власти |
| Отправитель сообщения | Информационная система, отправляющая сообщение через СМЭВ |
| Очередь доставки ответов потребителей | Очередь СМЭВ хранящая ответы на запросы в адрес потребителя. |
| Получатель сообщения | Информационная система, получающая сообщение из СМЭВ. |
| Потребитель сведений | Участник взаимодействия, запрашивающий сведения у поставщика сведений. |
| Прикладная схема (поставщика) | XML-схема, описывающая состав структурированных сведений, передаваемых в рамках запросов и ответов, в соответствии с требованиями поставщика. |
| РФ | Российская Федерация |
| Технологический портал СМЭВ3 | Справочный интернет-ресурс, посвященный СМЭВ, функционирующей согласно настоящим Методическим рекомендациям; доступен по адресу – https://smev3.gosuslugi.ru |
| УВ | Участник взаимодействия – орган или организация, участвующая в электронном обмене через СМЭВ. |
| ЭП | Электронная подпись |
| ЭП-ОВ | Электронная подпись органа власти |
| ЭП-Шлюз | Электронная подпись Шлюза |
| ЭП-СП | Электронная подпись для служебного пользования (должностного лица) |
| Namespace, пространство имен | Логическая группировка уникальных идентификаторов (имён), подробнее см.  <http://www.w3.org/TR/2009/REC-xml-names-20091208/> |
| SOAP | Simple Object Access Protocol версии 1.1 – протокол обмена структурированными сообщениями в распределённой вычислительной среде. См. также   http://www.w3.org/TR/2000/NOTE-SOAP-20000508/ |
| Target namespace, пространство имен XML-схемы | Логическая группировка уникальных идентификаторов (имён) элементов и атрибутов в схеме XML-документа, подробнее см. <http://www.w3.org/TR/2012/REC-xmlschema11-1-20120405/> |
| Qualified name, полное имя (XML элемента) | Пара, состоящая из префикса в виде [пространства имен](#Namespace) и [локального имени](http://www.w3.org/TR/2009/REC-xml-names-20091208/#dt-localname) XML-элемента. См. [http://www.w3.org/TR/2009/REC-xml-names-20091208/#ns-qualnames](http://www.w3.org/TR/2009/REC-xml-names-20091208/%23ns-qualnames) |
| URI | Unified Resource Identifier, уникальный идентификатор ресурса. Может быть либо URL – уникальным локатором ресурса, либо URN – уникальным именем ресурса. См. также <http://tools.ietf.org/html/rfc3986> |
| WSDL | Язык описания веб-сервисов и доступа к ним версии 1.1, основанный на языке XML. Смотри также http://www.w3.org/TR/wsdl |
| XSD | Файл, содержащий XML Schema |
| XML Schema | Язык описания структуры XML-документа. См. также:  <http://www.w3.org/TR/xmlschema-0/>  <http://www.w3.org/TR/xmlschema-1/>  http://www.w3.org/TR/xmlschema-2/ |
| XML | Расширяемый язык разметки. См. также  http://www.w3.org/TR/xml11/ |
| XML-binary Optimized Packaging | Соглашение, определяющее правила сериализации бинарных данных, передаваемых в XML-сообщениях  <https://www.w3.org/TR/2005/REC-xop10-20050125/> |

# ОСНОВЫ ВЗАИМОДЕЙСТВИЯ

## Типы сообщений

### Сообщения типа «Запрос»

Сообщения типа «запрос» проходят контроль корректности данных в два этапа – **синхронная** и **асинхронная** (необязательная) проверка.

Первый этап – синхронная проверка. После выполнения всех синхронных проверок, запрос помещается в очередь на асинхронную проверку. Если проверка прошла успешно, то в ответе возвращается сообщение об успешной проверке, при наличии ошибок метод {urn://x-artefacts-smev-gov-ru/services/message-exchange/1.1:SendRequest} возвращает fault.

Асинхронная проверка осуществляется после успешного завершения этапа синхронной проверки. При передаче сообщения в асинхронную проверку Шлюза в ответ на запрос возвращает в синхронном режиме сообщение, где в блоке MessageMetadata содержится следующий тег: <ns2:Status>requestIsQueued</ns2:Status>.

Если какая-либо асинхронная проверка показала ошибку, Шлюз помещает во входящую очередь ответов отправителя запроса сообщение об ошибке. Сообщение об ошибке будет получено отправителем запроса при очередном запросе GetResponse.

### Сообщения типа «Ответ»

Сообщения типа «Ответ» (далее – **ответ**) могут содержать либо запрошенные данные, либо мотивированный отказ в приеме запроса к исполнению. Запросы, представляющие собой широковещательные рассылки, не требуют ответов.

Сообщения типа «Ответ» проходят контроль корректности данных аналогично сообщениями типа «Запрос».

# ТРЕБОВАНИЯ К СТРУКТУРЕ СООБЩЕНИЙ

## Общие положения

Электронные сообщения в системе межведомственного электронного взаимодействия передаются в формате XML в кодировке UTF-8 с указанием кодировки в заголовке сообщения. Соответствующие им WSDL и XSD файлы также должны использовать кодировку UTF-8 с указанием кодировки в заголовке сообщения.

Общие требования и ограничения, связанные с использованием языка XML Schema, соблюдение которых обязательно при проектирования XSD-схем видов сведений, приведены в документе «Требования к XML-схемам, регистрируемым в СМЭВ», размещаемом на Технологическом портале СМЭВ3.

ИС участников взаимодействия в теле электронных сообщений должны поддерживать применение блоков и элементов данных, а также электронных подписей, описанных в данном документе. Использование других блоков и элементов, отличных от описанных в данном документе, **не допускается**.

Для именования пространств имен элементов в сообщениях зарезервированы два источника со схемой URN (базовые URI):

* urn://x-artefacts-smev-gov-ru/;
* urn://smev-gov-ru/.

Процесс отправки ИС потребителя запроса и получения ответа на запрос от Шлюза представляет собой последовательность вызовов электронного сервиса Шлюза информационной системой потребителя:

* передача в Шлюз запроса из ИС потребителя (//SendRequestRequest);
* получение из Шлюза ответа либо ответа со статусом в ИС потребителя (//GetResponseResponse)
* подтверждение потребителем получения ответа из Шлюза (//AckRequest).

Перечисленные в скобках элементы являются, по своему назначению, **конвертами сообщений** (далее – **СМЭВ-конверты**), так как представляют собой «оболочку» для передачи сообщений в Шлюзе, включающих блоки и элементы служебных и бизнес данных, а также электронные подписи.

Метод Get реализован в соответствии со стандартом http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/.

*Наименования перечисленных элементов образуются из слов Send/Get и Request/Response, соответствующих назначению элемента. Первый слог в имени элемента образуется словом «Send» или «Get», которое соответствует выполняемому действию с точки зрения ИС участника взаимодействия. Например, с точки зрения потребителя, он посылает (Send) запрос, а с точки зрения поставщика, он получает (Get) этот же запрос. Второй слог образуется словом «Request» или «Response» и определяет назначение сообщения с точки зрения бизнес-логики: слово «Request» означает запрос от потребителя к поставщику, а слово «Response» означает ответ от поставщика к потребителю. Третий слог образуется также словом «Request» или «Response», но несет другой смысл: слово «Request» соответствует SOAP-запросу, а слово «Response» SOAP-ответу.*

Элемент AckRequest (от acknowledgement request) является запросом на подтверждение и содержит ссылку на сообщение (идентификатор сообщения), получение которого подтверждается методом Ack.

## Структура сообщения с запросом, которое ИС потребителя передает в Шлюз

Структура сообщения, соответствующая передаче в Шлюз запроса от ИС потребителя, приведена на рисунке ниже (**Рисунок 1**).



Рисунок – Структура сообщения с запросом сведений, которое ИС потребителя передает в Шлюз

СМЭВ-конверт с запросом сведений (//SendRequestRequest), направляемый ИС потребителя в Шлюз, включает следующие элементы:

* **блок данных запроса** (//SenderProvidedRequestData), который включает структурированные сведения в соответствии с требованиями поставщика, а также служебные данные, заполняемые потребителем сведений;
* **электронная подпись органа власти** (ЭП-ОВ) (//CallerInformationSystemSignature).

### Блок данных запроса

Блок данных запроса может включать от двух до шести элементов, которые заполняются в ИС потребителя:

* идентификатор сообщения (//MessageID), обязательный элемент, идентификатор сообщения в виде UUID, основанного на времени, сгенерированный отправителем. UUID необходимо генерировать по версии 1 (см. п. 4.2 «Algorithms for Creating a Time-Based UUID» RFC 4122 <http://rfc.askapache.com/rfc4122/rfc4122.html#section-4.2>). Шлюз использует метку времени, содержащуюся в UUID, для проверки срока годности сообщения, к которому относится данный UUID. Для Шлюза срок годности одного сообщения составляет 24 часа;
* идентификатор первичного сообщения (//ReferenceMessageID), опциональный элемент, указывающий на первичный MessageID в цепочке запросов одной бизнес-транзакции. При отправке первичного запроса ReferenceMessageID и MessageID совпадают.
* блок структурированных сведений в соответствии с требованиями поставщика (//MessagePrimaryContent), обязательный элемент, представляющий собой XML документ, заполненный по формату, разработанному поставщиком сведений. Поставщик, для которого предназначен запрос, определяется в Шлюзе по полному имени корневого элемента в этом блоке.
* электронная подпись должностного лица (далее - ЭП-СП) (//PersonalSignature). По требованиям поставщика сведений эта подпись может быть обязательной для подписи блока сведений по форматам поставщика. С помощью ЭП-СП подписывается элемент, находящийся в //MessagePrimaryContent (между открывающим и закрывающим тегами);
* блок атрибутов бизнес-процесса (//BusinessProcessMetadata). Состав данных этого блока расширяемый и описывается отдельной XML-схемой urn://x-artefacts-smev-gov-ru/services/message-exchange/business-process-metadata/1.0.
* признак тестового взаимодействия (//TestMessage). Если этот элемент присутствует, то это означает, что запрос – тестовый. Данный признак используется для тестирования видов сведений.

Блок данных запроса подписывается ЭП-ОВ.

### Электронная подпись органа власти

Электронная подпись ЭП-ОВ, формируемая от имени органа власти, участвующего в межведомственном взаимодействии и выступающего в роли потребителя сведений, подписывает блок данных запроса. С помощью ЭП-ОВ обеспечивается целостность запроса и идентификация ИС отправителя.

## Структура с ответом, которое ИС потребителя получает из Шлюза

При получении из Шлюза SOAP-ответа, ИС потребителя проверяет в СМЭВ-конверте наличие элемента //ResponseMessage (присутствует, если очередь ответов не пуста). Элемент //ResponseMessage включает два элемента (**Рисунок 2**):

* блок данных СМЭВ-конверта (//Response);
* электронная подпись Шлюза (//SMEVSignature).



Рисунок – Общая структура сообщения с ответом, которое ИС потребителя получает из Шлюза (без указания элементов RequestRejected, RequestStatus или AsyncProcessingStatus)

### Блок данных СМЭВ-конверта

Блок данных СМЭВ-конверта //Response содержит элементы:

* идентификатор запроса (//OriginalMessageId), заполняемый Шлюзом значением идентификатора запроса, на который пришел ответ.
* идентификатор первичного запроса (//ReferenceMessageID), заполняемый Шлюзом значением идентификатора запроса, являющегося источником цепочки запросов. Если в цепочке запросов всего один запрос, то этот элемент заполняется значением элемента //OriginalMessageId.
* блок данных ответа //SenderProvidedResponseData, сформированный отправителем ответа (см. п. 2.3.2);
* блок маршрутной информации Шлюза (//MessageMetaData) с метаданными, включающими элементы:
* тип сообщения (ответ «RESPONSE») (//MessageType);
* информация об отправителе сообщения (//Sender), включающая вычисляемую на основе анализа сертификата ЭП-ОВ мнемонику отправителя, предназначенную для машинной обработки (Mnemonic);
* метка времени получения в Шлюз сообщения от ИС отправителя (//SendingTimeStamp). Содержит дату и время, начиная с которого отсчитывается срок исполнения запроса;
* информация об отправителе сообщения (//Recipient), определенная маршрутизатором и включающая мнемонику получателя, предназначенную для машинной обработки (//Mnemonic);
* дата и время доставки сообщения получателю (//DeliveryTimeStamp);
* ЭП-ОВ, которой ИС отправителя подписан блок данных ответа (//SenderInformationSystemSignature).

### Блок данных ответа

Блок данных ответа может включать три элементов, которые заполняются в Шлюзе:

* идентификатор сообщения (//MessageID), обязательный элемент, идентификатор сообщения в виде UUID, основанного на времени, сгенерированный отправителем. UUID необходимо генерировать по версии 1 (см. п. 4.2 «Algorithms for Creating a Time-Based UUID» RFC 4122 http://rfc.askapache.com/rfc4122/rfc4122.html#section-4.2). Шлюз использует метку времени, содержащуюся в UUID, для проверки срока годности сообщения, к которому относится данный UUID. Для Шлюза срок годности одного сообщения составляет 24 часа;
* адрес доставки ответа (//To), обязательный элемент, в который должно быть скопировано содержимое элемента //GetRequestResponse/RequestMessage/ Request/ReplyTo запроса, на который отправляется ответ;
* блок структурированных сведений в соответствии с требованиями поставщика (//MessagePrimaryContent), обязательный элемент, представляющий собой XML документ, заполненный по формату, разработанному поставщиком сведений. Этот блок не предназначен для передачи вложений, при возникновении такой необходимости следует использовать блоки содержимого вложений, заголовков и ЭП-СП вложений;

А также дополнительные (//choice) элементы:

* Статус запроса (//RequestStatus), который может быть использован ИС поставщика для информирования ИС потребителя о статусе обработки его запроса. Содержит код бизнес-статуса запроса (//StatusCode), который заполняется ИС поставщика, и описание бизнес-статуса запроса, в человекочитаемом виде (//StatusDescription), которое также заполняется ИС поставщика.
* Статус обработки сообщения в Шлюзе (//AsyncProcessingStatus). Данный элемент предназначен для использования только Шлюзом для информирования ИС о статусе обработки их сообщений в Шлюзе. Блок данных статуса сообщения (//AsyncProcessingStatus) содержит элементы:
* идентификатор сообщения (//OriginalMessageId), сформированный отправителем сообщения;
* категория статуса (//StatusCategory), содержащий одно из следующих возможных значений:
* requestIsQueued (Сообщение находится в очереди асинхронной обработки / Сообщение помещено в очередь получателя (запрос или ответ));
* requestIsRejectedBySmev (Сообщение не прошло асинхронную обработку);
* messageIsArchived (Сообщение, получение которого не подтверждено получателем, переведено в архив);
* messageIsDelivered (Сообщение получено получателем, т.е. получение сообщения подтверждено получателем).
* уведомление об описании статуса сообщения (//StatusDetails), содержащий описание статуса сообщения;
* элемент типа //SmevFault, содержащий в себе элемент //Code, определяющий код ошибки, и элемент //Description, содержащий описание ошибки.

### Электронная подпись Шлюза

С помощью ЭП-Шлюза (//SMEVSignature) подписываются блок данных запроса (вместе с ЭП-ОВ), а также добавленные в Шлюзе блок маршрутной информации Шлюза и обратный адрес.

С помощью ЭП-Шлюза обеспечивается целостность сообщения с ответом на всем пути от отправителя до получателя, подтверждение поступления ответа из Шлюза во время, указанное в метке времени, и право на обращение ИС потребителя за ответом.

# ЭЛЕКТРОННЫЕ ПОДПИСИ

## Виды электронных подписей

В электронных сообщениях, передаваемых через Шлюз, применяются следующие усиленные квалифицированные электронные подписи:

* электронная подпись, формируемая от имени должностного лица органа власти, участвующего в межведомственном взаимодействии (далее - **ЭП-СП**);
* электронная подпись, формируемая от имени органа власти, участвующего в межведомственном взаимодействии (далее - **ЭП-ОВ**);
* электронная подпись, формируемая в Шлюзе при обработке электронных сообщений, передаваемых через Шлюз (далее - **ЭП-Шлюз**).

Формирование ЭП-ОВ аналогично простановке печати организации на подписанном должностным лицом документе. ЭП-Шлюз в этом случае можно считать аналогом печати почтовой организации на конверте, в котором передается документ.

Электронная подпись ЭП-СП является **необязательной**, а ее включение в состав сообщения может быть обусловлено наличием соответствующего нормативно закрепленного требования, в котором поставщик устанавливает необходимость подписания запроса уполномоченным лицом. Соответствующее требование должно быть отражено в Описании поставляемого вида сведений.

Электронные подписи ЭП-ОВ и ЭП-Шлюз являются **обязательными**.

## Порядок использования электронных подписей при передаче запроса

Передача запроса от потребителя к Шлюзу сопровождается операциями по формированию и проверке электронных подписей.

Перед отправкой сообщения с запросом, должностное лицо ОВ может подписать (при необходимости) с помощью ЭП-СП следующий элемент в сообщении:

* блок структурированных сведений в соответствии с требованиями поставщика (подписывается содержимое элемента //MessagePrimaryContent, заключенное между открывающим и закрывающим тегами элемента). ЭП-СП хранится в элементе //PersonalSignature.

Перед подписанием запроса с помощью ЭП-СП должна осуществляться проверка наличия и действительности у должностного лица ОВ его сертификата. Ответственным за легитимность использования ЭП-СП является участник взаимодействия, отправляющий электронное сообщение.

Сформированные и подписанные, при необходимости, электронной подписью ЭП-СП сведения, заполненные в соответствии с требованиями поставщика, дополняются служебной информацией и вместе образуют блок данных запроса (элемент //SenderProvidedRequestData). Этот блок данных запроса подписывается ЭП-ОВ (элемент //CallerInformationSystemSignature).

На этом формирование электронных подписей запроса на стороне ИС потребителя завершается. Запрос, подписанный ЭП-ОВ и, при необходимости, ЭП-СП, поступает в Шлюз.

Шлюз автоматически осуществляет:

* проверку ЭП-ОВ, в том числе входящего в состав ЭП-ОВ сертификата;
* идентификацию ИС отправителя запроса по сертификату ЭП-ОВ;
* проверку по реестру прав доступа Шлюза (далее – матрица доступа) возможности обращения ИС отправителя к ИС получателя электронного сообщения;
* добавление блока маршрутной информации (в том числе метки времени получения запроса в Шлюз).

## Правила формирования ЭП

При формировании ЭП всех видов должны использоваться алгоритмы, представленные в таблице ниже (Таблица 1).

Таблица 1 – Алгоритмы

|  |  |  |
| --- | --- | --- |
|  | Наименование | URI |
| Расчет хеш-суммы | ГОСТ Р 34.11-94 (планируется переход на ГОСТ Р 34.11-2012 до конца 2018г., при этом ГОСТ Р 34.11-94 также будет поддерживаться) | <http://www.w3.org/2001/04/xmldsig-more#gostr3411> |
| Формирование подписи | ГОСТ Р 34.10-2001 (планируется переход на ГОСТ Р 34.10-2012 до конца 2018г., при этом ГОСТ Р 34.10-2001 также будет поддерживаться) | <http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411> |
| Канонизация (для XMLDSig) | Exclusive XML Canonicalization от 18 июля 2002 | http://www.w3.org/2001/10/xml-exc-c14n# |
| Дополнительная трансформация (для XMLDSig) | [Нормализация СМЭВ](#_Приложение_1:_Аглоритм) | urn://smev-gov-ru/xmldsig/transform |

Далее по тексту этого раздела, если имя элемента указано без пространства имен, подразумевается пространство имен urn://x-artefacts-smev-gov-ru/services/message-exchange/types/1.1.

## Электронные подписи субъектов взаимодействия – физических лиц

### Общие требования к электронной подписи, формируемой от имени должностных лиц органов власти при межведомственном информационном обмене

ЭП-СП аналогичны собственноручным подписям этих сотрудников и подтверждают, в том числе, факт формирования электронного документа конкретным сотрудником ОВ в ИС ОВ.

Ответственность за хранение и использование ключа подписи ЭП-СП несет должностное лицо. Порядок хранения и использования ключа подписи ЭП-СП контролируется представителями органов власти.

Перевыпуск существующих сертификатов ключей ЭП-СП должностных лиц ОВ для использования при межведомственном взаимодействии не является обязательным: возможно использовать ранее выданные и действительные сертификаты ключей подписи должностных лиц при условии, что они выданы одним из аккредитованных удостоверяющих центров, входящих в единое пространство доверия ЭП, формируемое Минкомсвязью РФ.

### Электронная подпись при межведомственном взаимодействии

ЭП-СП подписывает бизнес-данные сообщения, представленные в XML, а также приложенные файлы. Поскольку вложения передаются отдельно от бизнес-данных, ЭП-СП ставится отдельно на бизнес-данные, отдельно на каждый приложенный файл.

Правила формирования электронной подписи сообщений представлены в таблице ниже (Таблица 2).

Таблица 2 – Правила формирования электронной подписи сообщений

|  |  |
| --- | --- |
| Формат подписи | XMLDSig detached (https://www.w3.org/TR/xmldsig-core/) |
| Трансформация, дополнительно к канонизации | urn://smev-gov-ru/xmldsig/transform |
| Требования к форматированию | В XML-структуре подписи между элементами **не допускается** наличие текстовых узлов, в том числе переводов строки. |
| Подписываемый элемент | Для запросов и ответов - корневой элемент XML-документа, представляющего бизнес-данные запроса или ответа. |
| Размещение в сообщении | //SenderProvidedRequestData/ PersonalSignature/dsig:Signature (для запросов),  //SenderProvidedResponseData/PersonalSignature/dsig:Signature  (для ответов), |
| Способ помещения подписи в сообщение | Передается **клиентом веб-сервиса** в структуре параметров методов SendRequest, SendResponse. |
| Способ извлечения подписи для проверки | ЭП извлекается и проверяется **клиентом веб-сервиса**. |

## Электронные подписи субъектов взаимодействия – информационных систем

### Общие требования электронной подписи, формируемой от имени органа власти при межведомственном информационном обмене

ЭП-ОВ аналогичны гербовой печати организации и подтверждают:

* факт формирования межведомственного запроса в информационной системе ОВ, подписавшего межведомственный запрос (далее – запрос);
* факт наличия у лица, сформировавшего в ИС ОВ электронный документ (запрос либо ответ), соответствующих полномочий по подписанию/проверке ЭП на момент формирования электронного документа.

Орган власти, отправляющий электронный документ с использованием Шлюза другому участнику взаимодействия, гарантирует наличие соответствующих полномочий у своего должностного лица на обращение к информационному ресурсу другого ведомства либо на подготовку ответа на поступивший запрос (в случае если ответ формируется не автоматически в ИС).

Ответственность за хранение и использование ключа подписи ЭП-ОВ несет должностное лицо. Порядок хранения и использования ключа подписи ЭП-ОВ контролируется представителями органов власти.

### Общие требования к электронной подписи, формируемой Шлюзом

Общие требования к электронной подписи, формируемой Шлюзом, представлены в таблице ниже (Таблица 3).

ЭП-Шлюз подтверждает:

* факт прохождения электронного сообщения через Шлюз;
* факт аутентификации и авторизации в соответствии с правилами, указанными в реестре прав доступа к электронным сервисам (матрице доступа);
* неизменность сведений, внесенных в электронное сообщение Шлюз.

Ответственность за хранение и использование ключа подписи ЭП-Шлюза обеспечивается организационно-техническими мероприятиями оператора Шлюза.

Таблица 3 – Общие требования к электронной подписи, формируемой Шлюзом

|  |  |
| --- | --- |
| Формат подписи | XMLDSig detached |
| Трансформация, дополнительно к канонизации | urn://smev-gov-ru/xmldsig/transform |
| Требования к форматированию | В XML-структуре подписи, между элементами **не допускается** наличие текстовых узлов, в том числе переводов строки. |
| Подписываемый элемент | Для запросов – элемент //SendRequestResponse  Для ответов – элемент //MessageMetadata  При выборке сообщения из очереди – элемент //Request  При подтверждении получения сообщения – ЭП Шлюза отсутствует. |
| Размещение во входящем сообщении | Тело SOAP конверта, элемент //CallerInformationSystemSignature |

### Правила формирования электронной подписи информационной системы

Общие требования к электронной подписи, формируемой Шлюзом представлены в таблице ниже (Таблица 4).

Таблица 4 – Правила формирования электронной подписи информационной системы

|  |  |
| --- | --- |
| Формат подписи | XMLDSig detached |
| Трансформация, дополнительно к канонизации | urn://smev-gov-ru/xmldsig/transform |
| Требования к форматированию | В XML-структуре подписи, между элементами **не допускается** наличие текстовых узлов, в том числе переводов строки. |
| Подписываемый элемент | Для запросов – элемент //SenderProvidedRequestData   1. Для ответов – элемент //SenderProvidedResponseData   При выборке сообщения из очереди – элемент //MessageTypeSelector  При подтверждении получения сообщения – элемент //AckTargetMessage |
| Размещение в исходящем сообщении | Элемент //CallerInformationSystemSignature, см. схему smev-message-exchange-types-1.2.xsd. |
| Размещение во входящем сообщении | ЭП-ОВ отправителя попадает к получателю только при вызове методов GetRequest, GetResponse (выборка сообщения из очереди).  Она находится в теле SOAP-конверта, элемент //SenderInformationSystemSignature. |

# СЦЕНАРИЙ АСИНХРОННОГО ВЗАИМОДЕЙСТВИЯ

Упрощенно типовой сценарий взаимодействия включает одно сообщение – запрос и одно сообщение – ответ (Рисунок 3).



Рисунок – Типовой сценарий межведомственного взаимодействия (упрощенно)

Обмен сообщениями между ИС потребителя и Шлюзом, осуществляется путем вызова соответствующих методов веб-сервиса **SMEVMessageExchangeService**, предоставляемого Шлюзом. Веб-сервис SMEVMessageExchangeService предоставляет восемь методов.

Три методов используются для передачи запроса от ИС потребителя к Шлюзу и ответа от Шлюза к ИС потребителя:

* **SendRequest** (послать запрос), служит для передачи запроса от ИС потребителя в Шлюз;
* **GetResponse** (получить ответ), служит для получения из Шлюза ответа на запрос от ИС потребителя;
* **Ack** (подтвердить получение), служит для подтверждения получения сообщения из очереди, должен вызываться после получения сообщения методом GetResponse.

На протяжении жизненного цикла запрос проходит ряд состояний (статусов).

Перед отправкой в Шлюз запроса сведений ИС потребителя должна подготовить этот запрос. Подготовка запроса включает корректное заполнение блока структурированных данных запроса //SenderProvidedRequestData, в том числе блока сведений по форматам поставщика //MessagePrimaryContent (правильность заполнения элемента //MessagePrimaryContent будет потом проверяться в Шлюзе на соответствие схеме XSD и, при наличии, Schematron, разработанными поставщиком), добавление ЭП-ОВ для элемента //SenderProvidedRequestData.

Затем запрос сведений передается в Шлюз с помощью метода SendRequest, в Шлюзе последовательно выполняется следующие операции:

* **форматно-логический контроль (далее - ФЛК) СМЭВ-конверта** по схеме XSD. Под ФЛК понимается проверка формата данных, а также контроль логики заполнения данных, осуществляемые путем проверки соответствия этих данных документам на языке XSD и, при необходимости, Schematron (пример проверки: срок лишения специального права не может быть менее одного месяца и более трех лет). Как синоним ФЛК, в указанном значении, далее используется также термин **валидация**;
* **проверка ЭП-ОВ** на предмет корректности и на предмет действительности соответствующих сертификатов ключей подписи. ЭП-ОВ также используется для идентификации потребителя сервиса, приславшего запрос;
* **помещение запроса в очередь асинхронной обработки** с формированием отправителю данного запроса синхронного статусного сообщения категории «requestIsQueued» (сообщение находится в очереди асинхронной обработки);
* **получение запроса из очереди асинхронной обработки**;
* **валидация бизнес-данных** по схеме XSD и, при наличии, Schematron, разработанными поставщиком сервиса. Также проверяется полное имя корневого элемента блока структурированных сведений //MessagePrimaryContent для идентификации ИС поставщика - получателя запроса;
* **проверка ЭП-СП** (в элементе //PersonalSignature и в блоке заголовков вложений //AttachmentHeaderList);
* **помещение запроса в очередь доставки запросов**.

Затем ИС потребителя вызывает метод GetResponse и передает в Шлюз подготовленный и подписанный ЭП-ОВ запрос очередного ответа. Шлюз по ЭП-ОВ идентифицирует ИС потребителя и, при наличии недоставленных ответов, возвращает в ИС потребителя очередной ответ, предварительно подписав его ЭП-Шлюз. ИС потребителя при получении ответа проверяет ЭП-Шлюз, сохраняет у себя этот ответ и подтверждает получение ответа вызовом метода Ack. Шлюз, получив от ИС потребителя подтверждение получения ответа, формирует статусное сообщение категории «messageIsDelivered» (сообщение получено получателем), которое помещается в очередь доставки ответов отправителя ответа.

# ПРИЛОЖЕНИЯ

## Приложение 1. Адреса

Для начала тестирования взаимодействия, следует обратиться к Администратору Системы, чтобы внесли вашу ИС в список разрешенных ИС, иначе будет возникать ошибка, что «Информационная система не зарегистрирована в СМЭВ».

Адрес электронного сервиса Интеграционного шлюза в тестовой среде:

http://138.201.122.181:7500/ws?wsdl

Адрес электронного сервиса Интеграционного шлюза в продуктивной среде:

[адрес-сервера:7500/ws?wsdl](http://smev3-n0.test.gosuslugi.ru:7500/ws?wsdl)

## Приложение 2. Виды сведений

Адреса на виды сведений ГИС ГМП на Технологическом портале СМЭВ:

|  |  |
| --- | --- |
| **1** | **Прием необходимой для уплаты информации (начисления)** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202088&zone=fed&page=1&dTest=false> |
| **2** | **Прием информации об уплате (информации из распоряжения плательщика)** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202090&zone=fed&page=1&dTest=false> |
| **3** | **Прием информации о возврате** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202066&zone=fed&page=1&dTest=false> |
| **4** | **Предоставление необходимой для уплаты информации** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202070&zone=fed&page=1&dTest=false> |
| **5** | **Предоставление информации об уплате** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202186&zone=fed&page=1&dTest=false> |
| **6** | **Предоставление информации о возврате** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202284&zone=fed&page=1&dTest=false> |
| **7** | **Предоставление информации о результатах квитирования** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202258&zone=fed&page=1&dTest=false> |
| **8** | **Прием информации о погашении начисления** |
| Версия 2.2 | <https://smev3.gosuslugi.ru/portal/inquirytype_one.jsp?id=202092&zone=fed&page=1&dTest=false> |

## Приложение 3. Перечень ошибок, возвращаемых Шлюзом

Таблица – Перечень ошибок, возвращаемых Шлюзом отправки сообщения методом sendRequest

|  |  |
| --- | --- |
| **Исключение** | **Текст ошибки** |
| AccessDeniedException | Доступ запрещён |
| InvalidContentException | "Нарушен формат бизнес-конверта."  "Бизнес-данные сообщения не соответствуют схеме, зарегистрированной в СМЭВ. MessageId = " + @Message\_Id |
| SenderIsNotRegisteredException | "Информационная система не зарегистрирована в СМЭВ."  "Сертификат сотрудника не зарегистрирован в СМЭВ." |
| SignatureVerificationFaultException | "Отсутствует ЭП-ОВ"  "Срок действия сертификата истёк. Сертификат действителен до " + @validUntil  "Срок действия сертификата не начался. Сертификат действителен с " + @validSince  "Сертификат сотрудника не действителен."  "Проверка подписи на вложении " + @id\_вложения + ": срок действия сертификата истёк."  "Проверка подписи на вложении " + @id\_вложения + ": " + @error  "Срок действия сертификата " + @signatureTypeAsString + " истёк."  @signatureTypeAsString + " не соответствует подписанным данным: "  @signatureTypeAsString + " отсутствует в сообщении " + @MessageId  "Cертификат отозван. Код ответа в ГУЦ:" + @code |

Таблица – Перечень ошибок, возвращаемых Шлюзом после запроса на получение сообщения методом GetResponse

|  |  |
| --- | --- |
| **Исключение** | **Текст ошибки** |
| InvalidContentException | "Нарушен формат бизнес-конверта."  "Бизнес-данные сообщения не соответствуют схеме, зарегистрированной в СМЭВ. MessageId = " + @MessageId |
| SenderIsNotRegisteredException | "Отправитель не зарегистрирован в СМЭВ"  "Предъявленный сертификат пользователя " +                    @CallerCertificate.getSubjectX500Principal().getName(X500Principal.RFC1779) + " не зарегистрирован в СМЭВ" |
| SignatureVerificationFaultException | "<getResponse> Отсутствует ЭП-ОВ"  "Срок действия сертификата истёк. Сертификат действителен до " + @validUntil  "Срок действия сертификата не начался. Сертификат действителен с " + @validSince  "Срок действия сертификата " + @signatureTypeAsString + " истёк."  @signatureTypeAsString + " не соответствует подписанным данным: "  @signatureTypeAsString + " отсутствует в сообщении " + @MessageId  "Cертификат отозван. Код ответа в ГУЦ:" + @code |

Таблица – Перечень ошибок, возвращаемых Шлюзом после отправки подтверждения получения сообщения методом ack

|  |  |
| --- | --- |
| **Исключение** | **Текст ошибки** |
| InvalidContentException | "Нарушен формат бизнес-конверта."  "Бизнес-данные сообщения не соответствуют схеме, зарегистрированной в СМЭВ. MessageId = " + @MessageId |
| SenderIsNotRegisteredException | "Информационная система не зарегистрирована в СМЭВ."  "Предъявленный сертификат пользователя " +  @CallerCertificate.getSubjectX500Principal().getName(X500Principal.RFC1779) + " не зарегистрирован в СМЭВ" |
| SignatureVerificationFaultException | " Отсутствует ЭП-ОВ"  "Срок действия сертификата истёк. Сертификат действителен до " + @validUntil  "Срок действия сертификата не начался. Сертификат действителен с " + @validSince  "Срок действия сертификата " + @signatureTypeAsString + " истёк."  @signatureTypeAsString + " не соответствует подписанным данным: "  @signatureTypeAsString + " отсутствует в сообщении " + @MessageId  "Cертификат отозван. Код ответа в ГУЦ:" + @code |
| TargetMessageIsNotFoundException | "Сообщение " + @AckTargetMessage " не найдено среди неподтверждённых." |