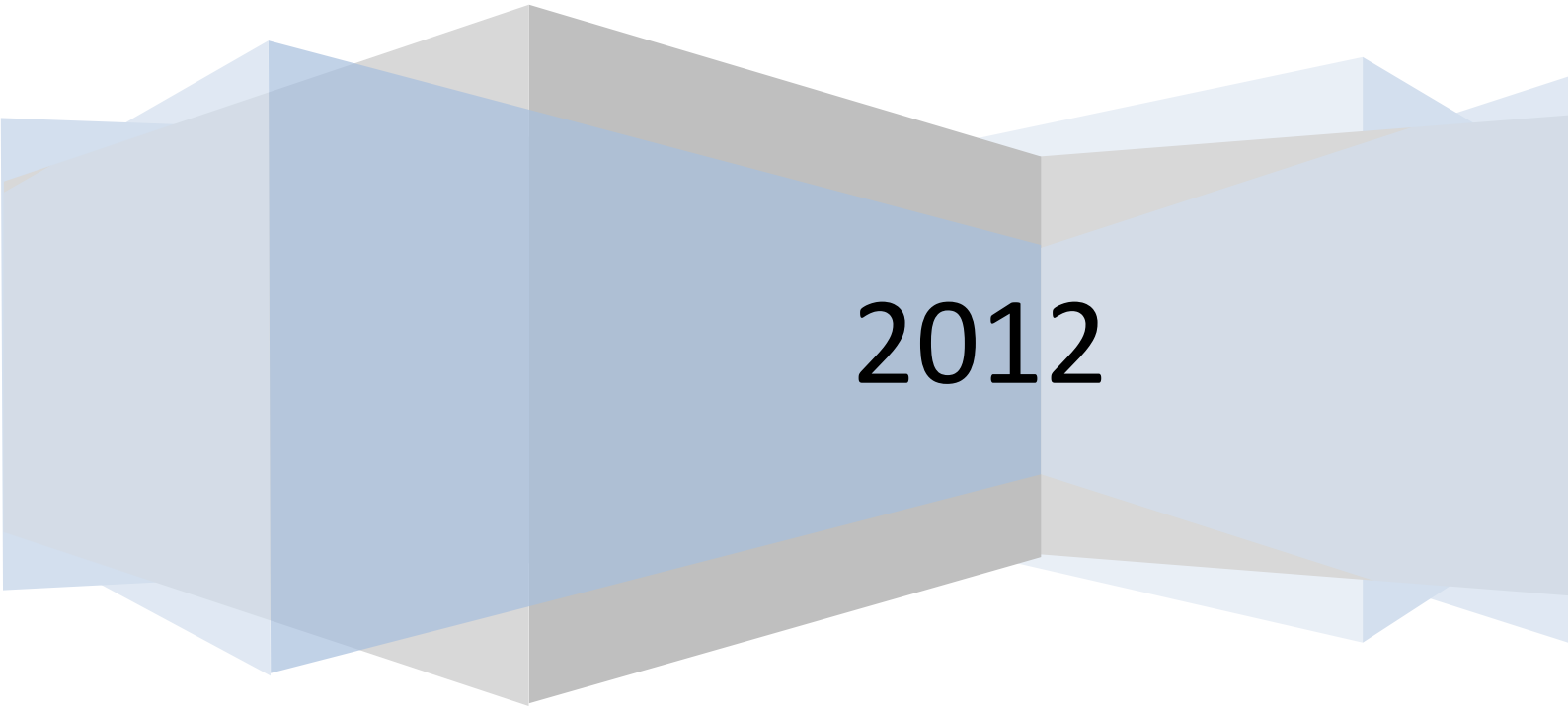
СИСТЕМА МЕЖВЕДОМСТВЕННОГО
ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

Методические рекомендации по разработке электронных сервисов и применению технологии электронной подписи при межведомственном электронном взаимодействии

Версия 2.5.6



2012

СОДЕРЖАНИЕ

ТАБЛИЦА ИЗМЕНЕНИЙ

Версия	Изменение
2.3.4	Добавлен атрибут ID/IDREF для идентификатора вложения.
2.3.4	Поля вложения «CodeDocument» и «Number» помечены как необязательные.
2.3.4	Поле Message «Originator» помечено как необязательное.
2.3.4	ReferenceType выставлен атрибут mixed="true".
2.3.4	К AppData добавлено объявление «any» атрибутов.
2.3.4	Из AppData удалено специальное объявление ds:Signature.
2.3.4	В объявление схем добавлен атрибут version="1.1".
2.3.4	Исправлено предложение по тексту, неверно описывающее положение клиентской подписи в структуре документа.
2.3.4	Элемент BinarySecurityToken вынесен из содержимого тега Signature в примерах сообщений.
2.4	Раздел 2. Изменены описания служебных элементов в сообщениях СМЭВ
2.4	Раздел 4. Изменения в части применения ЭП-ПГУ при подписании вложений, отправляемых от лица заявителя.
2.4	Добавлен раздел 7. Правила заполнения служебных элементов электронных сообщений в СМЭВ
2.4	Приложение 2. Изменены классификаторы для заполнения служебных элементов сообщений СМЭВ.
2.5	2.2. Блок электронной подписи информационной системы отправителя. Дополнены формулировки для региональных участников взаимодействия.
2.5	2.3. Блоки электронной подписи федерального и региональных узлов СМЭВ. Переименован блок. Дополнены формулировки для региональных узлов СМЭВ.
2.5	2.4. Унифицированные служебные заголовки федерального и региональных узлов СМЭВ. Переименован блок. Дополнены формулировки для региональных узлов СМЭВ.
2.5	2.5. Унифицированный служебный блок атрибутов сообщения СМЭВ. Дополнены формулировки для региональных узлов СМЭВ. Сведения об элементе для описания сведений об вызываемом сервисе smev:ServiceName.
2.5	2.10. Ограничение размера электронных сообщений. Описаны требования к ограничению размера электронных сообщений.
2.5	3.1. Виды электронных подписей. Дополнены формулировки для региональных узлов СМЭВ.
2.5	3.3. Межведомственное взаимодействие на уровне одного узла СМЭВ. Описаны особенности формирования электронной подписи ИС на уровне одного узла СМЭВ.
2.5	3.4. Межуровневое взаимодействие через различные узлы СМЭВ. Описаны особенности формирования электронной подписи ИС на уровне различных узлов СМЭВ.
2.5	3.5. Проверка сертификатов и подписей. Дополнены формулировки, касающие сервиса проверки электронной подписи.
2.5	3.5.1. Проверка электронной подписи ИС при межуровневом взаимодействии через СМЭВ. Описаны особенности проверки электронной подпсии ИС при межуровневом взаимодействии.
2.5	5.2. Общие требования к электронной подписи, формируемой узлами СМЭВ. Переименован блок. Дополнены формулировки для региональных узлов СМЭВ.
2.5	5.4. Правила формирования электронной подписи информационной системы. Дополнены формулировки в части формирования подписи ИС в транзитном формате.
2.5	5.9. Пример электронного сообщения, содержащего технологическую подпись информационной системы (ЭП-ОВ) и нескольких узлов СМЭВ (ЭП-СМЭВ/ЭП-РСМЭВ). Добавлен пример, содержащий электронную подпись нескольких узлов СМЭВ.
2.5	6.1. Модель синхронного взаимодействия. Переформатирование существовавшего материала по блокам.
2.5	6.2. Модели асинхронного взаимодействия. Переформатирование существовавшего материала по блокам.

2.5	6.5. Модель взаимодействия с передачей пакетов сообщений. Описаны правила межведомственного обмена с использованием пакетов сообщений.
2.5	7.3.5. Взаимодействие в пакетном режиме. Добавлено описание правил для проставления статусов при взаимодействия в пакетном режиме.
2.5	7.6. Принципы расчета статистики обмена в рамках межведомственного взаимодействия. Описаны принципы расчета статистики для взаимодействия в пакетном режиме.
2.5	7.7. Правила кодификации объектов. В подразделах добавлены правила кодификации объектов для мнемоник федеральных и региональных участников, информационных систем различного типа, кодов регионов, электронных сервисов и точек подключения.
2.5	Приложение 2. Классификатор «Мнемоники статусов сообщения». Статусы отсортированы по алфавиту. Добавлен статус для пакетного взаимодействия.
2.5	Приложение 3. Схема данных служебных элементов в электронных сообщениях СМЭВ. Дополнена схема данных электронного сообщения СМЭВ.
2.5	Приложение 5. Правила кодификации объектов. Добавлены классификаторы федеральных участников, ИС ИЭП, ИС кредитных организаций или поставщиков начислений, кодов регионов.
2.5	В разделе 1.1 добавлено описание правил формирования номера версии Методических рекомендаций.
2.5.6	В smev:Message добавлено поле ОКТМО
2.5.6	Добавлен раздел 8. Правила разработки муниципальных сервисов по предоставлению типовых сведений
2.5.6.	Добавлен раздел 5.2.1. Метка времени в электронной подписи узла СМЭВ
2.5.6.	Добавлено приложение 6. Коды ошибок СМЭВ с учетом меток времени
2.5.6.	Элемент smev:ServiceName заменен на элемент smev:Service в описании блока служебных атрибутов сообщения
2.5.6.	В схему добавлен отсутствовавший ранее элемент smev:Service. Сохранена поддержка старого элемента smev:ServiceName.
2.5.6.	Добавлено указание о заполнении поля smev:Recipient Потребителями при предоставлении типовых сведений

1. ВВЕДЕНИЕ

1.1. НАЗНАЧЕНИЕ ДОКУМЕНТА

Настоящий документ описывает правила разработки электронных сервисов поставщиков, предназначенных для регистрации в системе межведомственного электронного взаимодействия (далее – СМЭВ), в части применения служебных блоков данных, передаваемых в электронных сообщениях, а также форматов электронной подписи в сообщениях и передаваемых в них электронных документах-вложениях.

Требования, указанные в документе, следует рассматривать в дополнение к требованиям, содержащимся в приказе Министерства связи и массовых коммуникаций Российской Федерации от 27 декабря 2010 г. № 190 «Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия».

В рамках документа рассматриваются следующие вопросы:

- Структура электронного сообщения, служебные блоки данных в передаваемых в СМЭВ сообщениях;
- Правила применения и форматы электронной подписи, формируемой от лица пользователя Единого портала государственных и муниципальных услуг (функций) при заказе услуг в электронном виде;
- Правила применения и форматы электронной подписи, формируемой от имени должностных лиц органов власти при межведомственном информационном обмене;
- Правила применения и форматы электронной подписи, формируемой от имени органа власти при межведомственном информационном обмене;
- Правила применения и форматы электронной подписи, формируемой системой межведомственного электронного взаимодействия при обработке электронных сообщений, передаваемых через нее;
- Правила применения и форматы электронной подписи, формируемой единым порталом государственных услуг (функций) при передаче заявлений на оказание услуг в электронном виде;
- Правила заполнения служебных элементов электронных сообщений СМЭВ, определяемые необходимостью формирования целостных отчетов об истории обмена электронными сообщениями через СМЭВ в рамках оказания государственных услуг или выполнения государственных функций, а также формирования аналитических отчетов по межведомственному взаимодействию.

Описываемые в документе правила являются обязательными к применению участниками информационного обмена с использованием системы межведомственного электронного взаимодействия.

Документ содержит описание примеров сообщений и пошаговых алгоритмов формирования различных типов электронной подписи, применяемой в электронных сообщениях, передаваемых в СМЭВ.

В данный момент номер Методических рекомендации формируется по шаблону X.Y.Z, где:

X - номер поколения документа - Изменение данного номера означает значительные изменения в структуре и содержании документа.

Y - Номер основного релиза документа в рамках поколения. - Документ может содержать освещение новых и/или незначительную переработку содержащихся в предыдущей версии документа тем. Плановая подготовка основного релиза документа осуществляется раз в квартал. Основные релизы утверждаются Подкомиссией по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления.

Z - номер технологического релиза в рамках основного релиза. - Может содержать в себе стилистические, редакционные, незначительные технические изменения. Данные тип релизов выпускается по необходимости и не проходит специализированной процедуры утверждения Подкомиссией по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления.

В соответствии с требованиями приказа Минкомсвязи РФ N 190 от 27.12.2010 года, документированный способ доступа к информационной системе, подключаемой к системе взаимодействия, должен быть реализован в виде электронного сервиса. Одним из частных случаев электронных сервисов являются веб-сервисы.

1.2. ЦЕЛИ И ТРЕБОВАНИЯ

Данный документ разработан в целях реализации и во исполнение:

- Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
- Постановления Правительства Российской Федерации от 8 сентября 2010 г. № 697

«О единой системе межведомственного электронного взаимодействия» (далее Постановление № 697);

а также в рамках реализации:

- соглашений о взаимном признании электронных подписей, заключенных между Минкомсвязью РФ и федеральными органами исполнительной власти;
- соглашений о взаимодействии при обеспечении оказания (исполнения) государственных (муниципальных) услуг (функций) федеральными органами исполнительной власти, заключенных между Минкомсвязью РФ и федеральными органами исполнительной власти.

1.3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В документе используются следующие термины и определения:

ИС	Информационная система
ИЭП	Инфраструктура электронного правительства
Оператор СМЭВ	Министерство связи и массовых коммуникаций Российской Федерации (в соответствии с постановлением Правительства РФ N 697 от 08.09.2010)
ПО	Программное обеспечение
ЕПД	Единое пространство доверия
ЕПГУ	Единый портал государственных и муниципальных услуг (функций)
СМЭВ	Система межведомственного электронного взаимодействия
РСМЭВ	Региональная система межведомственного электронного взаимодействия
УЦ	Удостоверяющий центр
ОИВ	Органы исполнительной власти
ЭП	Электронная подпись
ИС ГУЦ	Информационная система Главного Удостоверяющего Центра

2. ТРЕБОВАНИЯ К СТРУКТУРЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ В СМЭВ

2.1. ОБЩИЕ ТРЕБОВАНИЯ

Электронные сообщения в системе межведомственного электронного взаимодействия передаются в формате XML.

Согласно спецификации WS-I Basic Profile 1.1 все WSDL и XSD файлы должны быть кодированы в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке XML) (Приказ Минкомсвязи РФ N 190 от 27.12.2010 года).

Кодировка электронных сообщений в СМЭВ должна быть UTF-8.

Для межведомственного информационного обмена кодировка вложений должна быть UTF-8.

Кодировка вложений в сообщениях в рамках подачи заявлений с ЕПГУ в электронном виде должна быть UTF-8 или UTF-16 при условии наличия соответствующей нотации:

```
<?xml version='1.0' encoding='UTF-8'?> или <?xml version="1.0" encoding="UTF-16LE"?>
```

Предпочтительным во вложениях, передаваемых в электронных сообщениях в рамках подачи заявлений с ЕПГУ в электронном виде является использование кодировки UTF-8, но выбор используемой кодировки Unicode определяется поставщиком самостоятельно.

Дополнительные требования к электронным сообщениям, указанные в документе, расширяют требования, содержащиеся в приказе Министерства связи и массовых коммуникаций Российской Федерации от 27 декабря 2010 г. № 190 «Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия», и предназначены для:

- обеспечения единых правил для участников межведомственного информационного обмена, осуществляемого через СМЭВ, в части структуры сообщений и технологий электронной подписи;
- усовершенствования механизмов контроля и мониторинга информационных потоков, реализующихся через передачу электронных сообщений от информационных систем потребителей к информационным системам поставщиков сервисов с использованием СМЭВ, как для обеспечения заказа услуг в электронном виде с Единого портала государственных услуг (функций) и их исполнения, так и для межведомственного взаимодействия между участниками информационного обмена.

В электронных сообщениях, передаваемых через СМЭВ, должны содержаться унифицированные блоки данных, описанные в данном документе.

Общая структура электронного сообщения включает в себя (приказ Минкомсвязи РФ N 190 от 27.12.2010 года):

заголовок электронного сообщения системы взаимодействия (soap:Header);

тело электронного сообщения системы взаимодействия (soap:Body);

сообщение об ошибке (soap:Fault).

Интерфейсы ИС участников взаимодействия, подключаемые к СМЭВ, в заголовке электронных сообщений должны поддерживать применение:

– Блока электронной подписи информационной системы отправителя (в рамках описания текущего документа это либо ЭП-ПГУ – при взаимодействии для заказа услуг в электронном виде, либо ЭП-ОВ – при межведомственном взаимодействии);

– Блока электронной подписи СМЭВ;

– Унифицированного служебного заголовка СМЭВ.

Интерфейсы ИС участников взаимодействия, подключаемые к СМЭВ, в теле электронных сообщений должны поддерживать применение:

– Унифицированного служебного блока атрибутов сообщения СМЭВ;

– Унифицированного служебного блока-обертки данных сообщения СМЭВ;

– Унифицированного служебного блока структурированных сведений в соответствии с требованиями поставщика;

– Унифицированного служебного блока вложений (включающий элементы для обеспечения передачи вложений в формате бинарных данных или в формате ссылки на вложение, передаваемое вне конверта)

Использование других блоков данных, отличных от описанных в данном документе, в заголовке и теле электронных сообщений не допускается.

Пример структуры электронного сообщения, содержащего унифицированные блоки данных, содержится в приложении 3.

Описание унифицированных элементов в сообщениях обеспечивает версионность, предполагающую дальнейшее развитие формата сообщений при условии поддержания совместимости с предыдущими версиями.

Для именования пространства имен унифицированных элементов в сообщениях СМЭВ, регламентирующихся Оператором СМЭВ, в документе применяется нотация xmlns:smev.

Для того чтобы можно было отличить одну версию формата от другой, применяется следующее правило кодирования пространства имен:

```
xmlns:smev="http://smev.gosuslugi.ru/revYYMMDD"
```

где YYMMDD указывает на дату принятия актуальной версии, соответственно:

- YY соответствует двум последним цифрам в номере года;
- MM – номер месяца;
- DD – номер числа в месяце.

Для обозначения версии методических рекомендаций для схем данных применяется атрибут корневого элемента xsd:schema:

```
version="A.B.C"
```

Схема электронного сообщения, передаваемого в СМЭВ с учетом унифицированных блоков, представлена на рисунке.

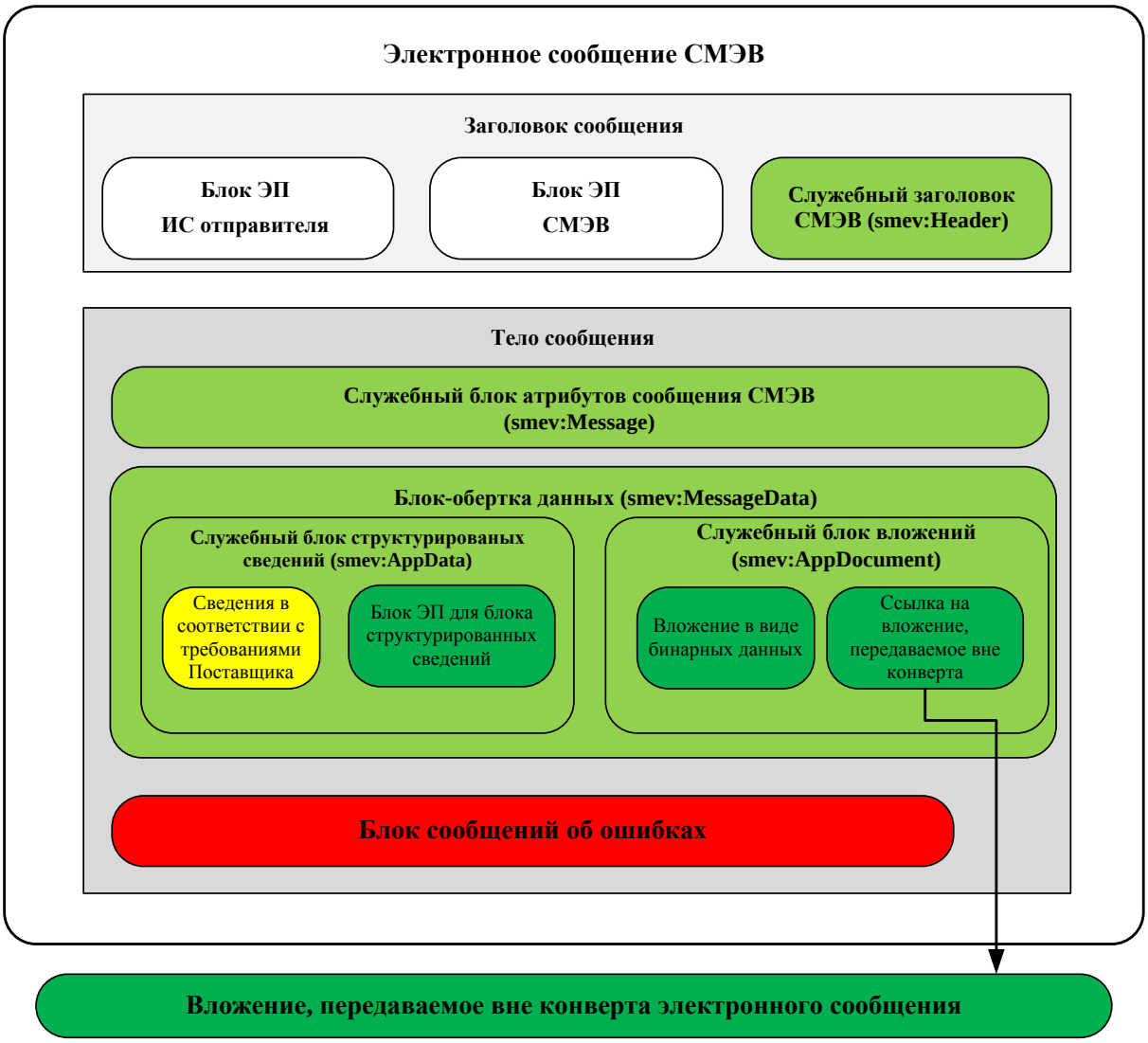


Рисунок 1 - Схема электронного сообщения СМЭВ

2.2. БЛОК ЭЛЕКТРОННОЙ ПОДПИСИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТПРАВИТЕЛЯ

Блок электронной подписи информационной системы отправителя предназначен для передачи значений электронной подписи в формате, описываемом в разделе 5 «Электронные подписи субъектов взаимодействия – информационных систем».

Сведения этого блока помимо хранения собственно самой подписи информационной системы отправителя используются СМЭВ/РСМЭВ для аутентификации и авторизации обращений к электронным сервисам.

Конструкция блока совпадает для информационных систем инфраструктуры электронного правительства (таких как Единый портал государственных услуг (функций)) и информационных систем участников (в том числе, органов власти), подключаемых к федеральному или региональным узлам системы межведомственного электронного взаимодействия.

2.3. БЛОКИ ЭЛЕКТРОННОЙ ПОДПИСИ ФЕДЕРАЛЬНОГО И РЕГИОНАЛЬНЫХ УЗЛОВ СМЭВ

Блоки электронной подписи федерального и региональных узлов СМЭВ предназначены для передачи значений электронной подписи, формируемой федеральными или региональными узлами системы межведомственного электронного взаимодействия в формате, описываемом в разделе 5 «Электронные подписи субъектов взаимодействия – информационных систем».

Электронная подпись, передаваемая в этих блоках, используется для подписания сведений в электронном сообщении, добавляемых при передаче узлами системы межведомственного электронного взаимодействия.

2.4. УНИФИЦИРОВАННЫЕ СЛУЖЕБНЫЕ ЗАГОЛОВКИ ФЕДЕРАЛЬНОГО И РЕГИОНАЛЬНЫХ УЗЛОВ СМЭВ

Унифицированные служебные заголовки федерального и региональных узлов СМЭВ предназначены для размещения в сообщении сведений, добавляемых соответствующим узлом системы межведомственного электронного взаимодействия.

Информационные системы участников взаимодействия должны корректно осуществлять обработку входящих сообщений, содержащих унифицированные служебные заголовки узлов СМЭВ. В одном сообщении, проходящем при доставке через несколько узлов СМЭВ, могут содержаться несколько унифицированных служебных заголовков, соответствующих разлым узлам.

Состав элементов, входящих в служебные заголовки, не является жестко специфицированным. С развитием формата сообщений, передаваемых через СМЭВ, возможно расширение состава элементов.

Минимальный набор элементов в служебных заголовках содержит сведения о метке времени прохождения сообщения через СМЭВ, коде узла системы межведомственного взаимодействия и уникальном идентификаторе сообщения в пределах узла системы взаимодействия.

Для обозначения унифицированных служебных заголовков СМЭВ применяется элемент *smev:Header* в пространстве имен xmlns:smev.

Отличить служебный заголовок СМЭВ, проставляемый одним узлом, от служебного заголовка, проставляемого другими узлами, можно по атрибуту *actor* и элементу *smev:NodeId*.

Состав элементов, являющихся дочерними по отношению к элементу *smev:Header*, представлен в таблице ниже*:*

Код узла СМЭВ	*smev:NodeId.*	Уникальный идентификатор узла СМЭВ, состоящий из двух символов
Идентификатор электронного сообщения	*smev:MessageId*	Представляет собой уникальный идентификатор электронного сообщения (запроса или ответа) в рамках узла СМЭВ. Представляет собой GUID унифицированной структуры (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx).
Метка времени гарантированной доставки	*smev:TimeStamp*	Дата и время создания сообщения в формате UTC 'yyyy-MM-dd'T'HH:mm:ss.SSSZ’
Класс электронного сообщения	*smev:MessageClass*	Идентификатор, указывающий является ли электронное сообщение запросом от потребителя к поставщику или ответом от поставщика потребителю. Может принимать значения в соответствии с

		классификатором, определенным в приложении 2.
Идентификаторы прикладных сообщений	*smev:PacketIds*	Список идентификаторов прикладных сообщений, передаваемых в пакете

В зависимости от значений атрибута *actor* различается:

- локальный формат служебного заголовка - в случае, если взаимодействие осуществляется внутри узла;
- транзитный вариант служебного заголовка - в случае, если взаимодействие осуществляется между различными узлами СМЭВ.

Для локального формата значение атрибута имеет вид *actor=”http://smev.gosuslugi.ru/actors/recipient”,* а для транзитного формата - *actor=”http://smev.gosuslugi.ru/actors/smevXX”* (где XX соответствует коду региона, куда осуществляется транзит сообщения).

Пример служебного заголовка федерального узла СМЭВ (локальный формат) представлен ниже:

```
<smev:Header wsu:Id="smev-header" actor=”http://smev.gosuslugi.ru/actors/recipient” xmlns:smev="http://smev.gosuslugi.ru/rev120315">
    <smev:NodeId>00</smev:NodeId>
    <smev:MessageId>3F0FF45C-F99E-00CD-F374-9D8807EB5BD4</smev:MessageId>
   <smev:TimeStamp>2011-11-21T18:18:21.805+03:00</smev:TimeStamp>
   <smev:MessageClass>REQUEST</smev:MessageClass>
 </smev:Header>
```

Пример служебного заголовка регионального узла СМЭВ (транзитный формат) представлен ниже:

```
<smev:Header wsu:Id="smev-header" actor=”http://smev.gosuslugi.ru/actors/smev00” xmlns:smev="http://smev.gosuslugi.ru/rev120315">
    <smev:NodeId>63</smev:NodeId>
```

```
        <smev:MessageId>3F0FF45C-F99E-00CD-F374-9D8807EB5BD4</smev:MessageId>
      <smev:TimeStamp>2011-11-21T18:18:21.805+03:00</smev:TimeStamp>
      <smev:MessageClass>RESPONSE</smev:MessageClass>
 </smev:Header>
```

Для пакетного режима взаимодействия элемент smev:Header расширяется и принимает вид, содержащий в том числе сведения о прикладных сообщениях, передаваемых в пакете:

```
<smev:Header wsu:Id="smev-header" actor=”http://smev.gosuslugi.ru/actors/recipient” xmlns:smev="http://smev.gosuslugi.ru/rev120315">
        <smev:NodeId>00</smev:NodeId>
        <smev:MessageId>3F0FF45C-F99E-00CD-F374-9D8807EB5BD4</smev:MessageId>
      <smev:TimeStamp>2011-11-21T18:18:21.805+03:00</smev:TimeStamp>
      <smev:MessageClass>REQUEST</smev:MessageClass>
     <smev:PacketIds>
       <smev:Id>
                <smev:MessageId>B3BF3037-99E4-4EEB-A15B-1937BCFF0C65</smev:MessageId>
                <smev:SubRequestNumber>1</smev:SubRequestNumber>
       </smev:Id>
       <smev:Id>
                <smev:MessageId>20FC331D-C019-4EA0-A5DF-531CBF3FD3BF</smev:MessageId>
                <smev:SubRequestNumber>2</smev:SubRequestNumber>
       </smev:Id>
      ...
       <smev:Id>
                <smev:MessageId>9F09D8C5-CDA8-4FBB-AA8B-E1ECBDF35A48</smev:MessageId>
```

```
            <smev:SubRequestNumber>n</smev:SubRequestNumber>
        </smev:Id>
    </smev:PacketIds>
</smev:Header>
```

2.5. УНИФИЦИРОВАННЫЙ СЛУЖЕБНЫЙ БЛОК АТРИБУТОВ СООБЩЕНИЯ СМЭВ

Унифицированный служебный блок атрибутов сообщения СМЭВ предназначен для передачи атрибутивных сведений об участниках и назначении сообщения в рамках информационного обмена через СМЭВ.

Унифицированный служебный блок атрибутов сообщения СМЭВ формируется в сообщении на стороне информационной системы, отправляющей сообщение в СМЭВ.

Унифицированный служебный заголовок атрибутов сообщения СМЭВ используется для формирования отчетности о взаимодействии, осуществляемом информационными системами участников через СМЭВ.

Информационные системы участников взаимодействия должны корректно осуществлять обработку входящих сообщений, содержащих унифицированный служебный блок атрибутов сообщения СМЭВ, а также осуществлять корректное заполнение сведений в данном блоке, размещаемом в исходящих сообщениях, в соответствии с подробно изложенными в разделе 7 правилами.

Минимальный состав сведений, передаваемых в данном блоке, может включать:

- Данные о системе-инициаторе взаимодействия (Потребителе) (обязательно);
- Данные о системе-получателе сообщения (Поставщике) (обязательно);
- Данные о системе, инициировавшей цепочку из нескольких запросов-ответов, объединенных единым процессом в рамках взаимодействия (опционально);
- Данные о вызываемом сервисе (обязательно);
- Тип сообщения по классификатору сообщений в СМЭВ (обязательно);
- Дата создания сообщения (обязательно);
- Идентификатор сообщения-запроса, инициировавшего взаимодействие (опционально);
- Идентификатор сообщения-запроса, инициировавшего цепочку из нескольких запросов-ответов, объединенных единым процессом в рамках взаимодействия (опционально);

– Код государственной услуги, в рамках оказания которой осуществляется информационный обмен (опционально);

– Номер дела в информационной системе-отправителе (опционально);

– Статус сообщения (обязательно);

– Категория взаимодействия (обязательно);

– Признак тестового взаимодействия (опционально).

Для обозначения унифицированного служебного блока атрибутов сообщения СМЭВ применяется элемент *smev:Message* в пространстве имен xmlns:smev.

Состав элементов, являющихся дочерними по отношению к элементу *smev:Message,* представлен в таблице ниже, все эти элементы определяются в пространстве имен *xmlns:smev.*

Данные о системе-инициаторе взаимодействия (Потребителе)	*smev:Sender*	Структура данных, содержащая сведения об информационной системе: идентификатор системы и краткое наименование системы.
Данные о системе-получателе сообщения (Поставщике)	*smev:Recipient*	Структура данных, содержащая сведения об информационной системе: идентификатор системы и краткое наименование системы.
Данные о системе, инициировавшей цепочку из нескольких запросов-ответов, объединенных единым процессом в рамках взаимодействия	*smev:Originator*	Структура данных, содержащая сведения об информационной системе: идентификатор системы и краткое наименование системы. Наиболее вероятным значением в этом поле в настоящее время будет ПГУ, но в зависимости от правил взаимодействия

		через СМЭВ, инициаторами смогут выступать и другие информационные системы.
Данные о вызываемом сервисе	*smev:Service*	Структура данных, содержащая мнемонику сервиса и номер его версии. Значения элементов данной структуры используются сервисом динамической маршрутизации для определения конечной точки маршрутизации сообщения.
Тип сообщения	*smev:TypeCode*	Значение по классификатору типов сообщений, передаваемых через узел СМЭВ, размещенному в приложении 2.
Статус сообщения	*smev:Status*	Сведения о статусе электронного сообщения. Классификатор статусов сообщения приведен в приложении 2.
Дата создания сообщения	*smev:Date*	Дата и время создания сообщения в формате UTC 'yyyy-MM-dd'T'HH:mm:ss.SSSZ’
Идентификатор сообщения-запроса, инициировавшего взаимодействие	*smev:RequestIdRef*	Заполнение поля необходимо для сообщений, не являющихся инициатором взаимодействия.

		Для ответа на запрос инициатором взаимодействия является сообщение запрос от потребителя к поставщику. Указывается только в электронных сообщениях, являющихся ответами на запросы.
Идентификатор сообщения-запроса, инициировавшего цепочку из нескольких запросов-ответов, объединенных единым процессом в рамках взаимодействия	*smev:OriginRequestIdRef*	Заполнение поля необходимо для сообщений, не являющихся инициатором взаимодействия в случае, если цепочка взаимодействия состоит из более чем одного запроса-ответа. Не указывается только в электронном сообщении, инициирующем цепочку из нескольких запросов-ответов.
Код государственной услуги, в рамках оказания которой осуществляется информационный обмен	*smev:ServiceCode*	Код государственной услуги указывается в соответствии с правилами кодификации, установленными в ИС Сводного реестра государственных услуг (функций). Указание данного элемента в заголовке является обязательным, если в контексте информационного взаимодействия такая сущность присутствует.
Номер дела в	*smev:CaseNumber*	Номер дела указывается в

информационной системе-отправителе		соответствии с правилами, установленными в информационной системе-отправителя. В случае заказа с ЕПГУ, код дела совпадает с номером заявки в едином личном кабинете. Указание данного элемента в заголовке является обязательным, если в контексте информационного взаимодействия такая сущность присутствует.
Категория взаимодействия	*smev:ExchangeType*	Признак принадлежности электронного сообщения различным категориям взаимодействия, возникающим при межведомственном обмене. Классификатор категорий взаимодействия приведен в приложении 2.
Признак тестового взаимодействия	*smev:TestMsg*	Признак тестового электронного сообщения: запроса или ответа. Не указывается при продуктивном взаимодействии.
Код муниципального образования по ОКТМО	*smev:OKTMO*	Код муниципального образования по ОКТМО используется для динамической маршрутизации вызова в данное муниципальное образование

Для пакетного режима взаимодействия элемент smev:Message расширяется дополнительным необязательным полем *smev:SubMessages* - коллекцией из 1 или больше элементов *smev:SubMessage*.

Элемент *smev:SubMessage* имеет следующую структуру:

Уникальный идентификатор сообщения внутри пакета	*smev:SubRequestNumber*	Уникальный идентификатор сообщения внутри пакета назначается инициатором взаимодействия.
Статус сообщения	*smev:Status*	Сведения о статусе электронного сообщения. Классификатор статусов сообщения приведен в приложении 2.
Данные о системе, инициировавшей цепочку из нескольких запросов-ответов, объединенных единым процессом в рамках взаимодействия	*smev:Originator*	Структура данных, содержащая сведения об информационной системе: идентификатор системы и краткое наименование системы. Наиболее вероятным значением в этом поле в настоящее время будет ПГУ, но в зависимости от правил взаимодействия через СМЭВ, инициаторами смогут выступать и другие информационные системы.
Дата создания сообщения	*smev:Date*	Дата и время создания сообщения в формате UTC 'yyyy-MM-dd'T'HH:mm:ss.SSSZ’
Идентификатор сообщения-запроса, инициировавшего цепочку из нескольких запросов-ответов,	*smev:OriginRequestIdRef*	Заполнение поля необходимо для сообщений, не являющихся инициатором

объединенных единым процессом в рамках взаимодействия		взаимодействия в случае, если цепочка взаимодействия состоит из более чем одного запроса-ответа. Не указывается только в электронном сообщении, инициирующем цепочку из нескольких запросов-ответов.
Идентификатор сообщения-запроса, инициировавшего взаимодействие	*smev:RequestIdRef*	Заполнение поля необходимо для сообщений, не являющихся инициатором взаимодействия. Для ответа на запрос инициатором взаимодействия является сообщение запрос от потребителя к поставщику. Указывается только в электронных сообщениях, являющихся ответами на запросы.
Код государственной услуги, в рамках оказания которой осуществляется информационный обмен	*smev:ServiceCode*	Код государственной услуги указывается в соответствии с правилами кодификации, установленными в ИС Сводного реестра государственных услуг (функций). Указание данного элемента в заголовке является обязательным, если в контексте информационного взаимодействия такая сущность присутствует.

Номер дела в информационной системе-отправителе	*smev:CaseNumber*	Номер дела указывается в соответствии с правилами, установленными в информационной системе-отправителя. В случае заказа с ЕПГУ, код дела совпадает с номером заявки в едином личном кабинете. Указание данного элемента в заголовке является обязательным, если в контексте информационного взаимодействия такая сущность присутствует.

2.6. УНИФИЦИРОВАННЫЙ СЛУЖЕБНЫЙ БЛОК-ОБЕРТКА ДАННЫХ СООБЩЕНИЯ В СМЭВ

Унифицированный служебный блок-обертка данных (smev:MessageData) сообщения в СМЭВ является группирующим элементом, содержащим внутри себя унифицированные служебные блоки: блок структурированных сведений (в соответствии с требованиями поставщика) и блок вложений.

Сообщение, отправляемое в систему межведомственного взаимодействия, может содержать как блок структурированных сведений в соответствии с требованиями поставщика (smev:AppData), так и блок вложений (smev:AppDocument).

При информационном обмене в рамках межведомственного взаимодействия, не предусматривающем передачу вложений, блок вложений в электронном сообщении отсутствует.

При информационном обмене, предусматривающем передачу вложений, в блоке структурированных сведений передаются сведения технологического характера (например, статус заявления или обработки межведомственного запроса), а в блоке вложений передается архив, содержащий заявление и сопутствующие вложения. В случае, если какие-то сведения технологического характера являются обязательными для формы заявления, которая определяется поставщиком сервиса с учетом требований Минкомсвязи, то в блоке структурированных сведений может происходить дублирование этих сведений для обеспечения взаимодействия информационных систем, участвующих во взаимодействии через СМЭВ.

При подаче заявлений с ЕПГУ применяется формат электронной подписи субъекта взаимодействия - физического лица, при котором подпись к заявлению и подписи для вложений хранятся в отдельных файлах в формате PKCS#7 detached (http://tools.ietf.org/html/rfc2315).

При межведомственном взаимодействии в случае, если форматом запроса услуги не предусмотрено наличие вложений, то сведения, переданные в блоке структурированных сведений, могут быть подписаны ЭП в формате XMLDsig.

При межведомственном взаимодействии в случае, если электронное сообщение содержит вложения, то блок передачи вложений является обязательным и должен содержать как подписанные сведения, так и электронную подпись, сформированную в соответствии с требованиями в разделе 4 «Электронные подписи субъектов взаимодействия – физических лиц».

Для обозначения унифицированного служебного блока-обертки данных сообщения в СМЭВ применяется элемент *smev:MessageData* в пространстве имен xmlns:smev.

2.7. УНИФИЦИРОВАННЫЙ СЛУЖЕБНЫЙ БЛОК ПЕРЕДАЧИ СТРУКТУРИРОВАННЫХ СВЕДЕНИЙ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ПОСТАВЩИКА

Унифицированный служебный блок передачи структурированных сведений в соответствии с требованиями поставщика предназначен для структурированной передачи набора элементов, требования к составу и структуре которых определяет Поставщик сервиса.

СМЭВ не производит анализ сведений, переданных внутри данного блока.

Данный блок не предназначен для передачи вложений в электронных сообщениях (в случае возникновения такой необходимости следует использовать унифицированный служебный блок передачи вложений и правила, предъявляемые для передачи сведений в нем).

Если электронное сообщение при межведомственном информационном обмене не предполагает передачу вложений, то для удостоверения сведений передаваемых в этом блоке, может применяться блок электронной подписи субъекта взаимодействия - физического лица в формате XMLDsig. Правила формирования этого блока описываются в разделе 4 в пункте «Электронная подпись при межведомственном взаимодействии в сообщениях без вложений».

Для обозначения унифицированного служебного блока передачи сведений в соответствии с требованиями поставщика сервиса применяется элемент *smev:AppData* в пространстве имен *xmlns:smev.*

2.8. БЛОК ЭЛЕКТРОННОЙ ПОДПИСИ ФИЗИЧЕСКОГО ЛИЦА, СВЯЗАННОЙ С БЛОКОМ СТРУКТУРИРОВАННЫХ СВЕДЕНИЙ

При межведомственном взаимодействии допустимым является вариант информационного обмена, при котором не передаются вложения. В этом случае электронная подпись, соответствующая блоку структурированных сведений формируется в соответствии с форматом XMLDSig.

Правила и алгоритм формирования такой подписи представлены в разделе 4 «Электронные подписи субъектов взаимодействия – физических лиц».

2.9. УНИФИЦИРОВАННЫЙ СЛУЖЕБНЫЙ БЛОК ПЕРЕДАЧИ ВЛОЖЕНИЙ

Унифицированный служебный блок для передачи вложений предназначен для передачи вложений в виде архива, заключающего внутри себя набор файлов со сведениями и соответствующих им файлов электронной подписи субъекта взаимодействия – физического лица в формате PKCS#7 (detached).

Поддерживаются два формата передачи вложений:

– Вложение в виде бинарных данных в пределах самого блока передачи вложений;

– Вложение в виде ссылки, само вложение передается вне конверта электронного сообщения.

Для обозначения унифицированного служебного блока передачи вложений применяется элемент smev:AppDocument в пространстве имен xmlns:smev.

В случае электронных сообщений, подразумевающих передачу вложений, блок передачи структурированных сведений (*smev:AppData*) не удостоверяется электронной подписью субъекта взаимодействия - физического лица и предназначается для передачи технологических сведений, необходимых для обеспечения взаимодействия информационных систем.

В случае, когда вложение передается в виде бинарных данных, то архив вложений, содержащих заявление, вложения и соответствующие подписи, формируется с учетом требований, описанных в разделе 4 «Электронные подписи субъектов взаимодействия – физических лиц», и передается в формате Base64 в пределах данного элемента.

Если вложение передается в виде бинарных данных, то для передачи данных применяется элемент *smev:BinaryData* в пространстве имен *xmlns:smev.*

В случае если вложение передается в виде ссылки, то дочерними блоками элемента становятся идентификатор вложение и значение хеш-суммы от вложения, передаваемого вне конверта, для обеспечения возможности контроля неизменности передаваемого вложения.

Если вложение передается в виде ссылки, то для передачи данных применяются элементы *smev:Reference* и его дочерний элемент *xop:Include* (ссылка на вложение), а также элемент *smev:DigestValue* (в пространстве имен xmlns:smev).

Вложение в сообщении необходимо передавать только одно, в случае наличия необходимости передачи нескольких файлов (в том числе файла заявления), они группируются в одном архиве, который передается в качестве вложения.

2.10. ОГРАНИЧЕНИЕ РАЗМЕРА ЭЛЕКТРОННЫХ СООБЩЕНИЙ

При межведомственном обмене с использованием электронной подписи в электронных сообщениях, время, затрачиваемое на проверку и формирование электронной подписи субъектов взаимодействия – информационных систем, пропорционально размеру самих сообщений.

С учетом того, что участники в настоящее время применяют при взаимодействии через СМЭВ электронные сервисы, технически работающие в синхронном режиме, для электронных сообщений СМЭВ рекомендуется ограничить объем отдельных сообщений, отправляемых участниками друг другу.

Для обеспечения приемлемого времени отклика СМЭВ при обработке электронных сообщений в синхронном режиме рекомендуется ограничение в объеме 5 Мб на максимально допустимый размер отдельных сообщений, передаваемых в рамках одной сессии взаимодействия с использованием электронных сервисов.

Увеличение максимально допустимого размера сообщений будет производится по мере введения в промышленную эксплуатацию расширенного набора протоколов взаимодействия и модернизации аппаратного и программного обеспечения СМЭВ.

3. ЭЛЕКТРОННЫЕ ПОДПИСИ В ЭЛЕКТРОННЫХ СООБЩЕНИЯХ В СМЭВ

3.1. ВИДЫ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

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

- Электронная подпись, формируемая от имени пользователя Единого портала государственных услуг (функций), осуществляющего заказ услуг в электронном виде (далее – пользователя ЕПГУ, ЭП-П);
- Электронная подпись, формируемая от имени должностного лица органа власти, участвующего в межведомственном взаимодействии при оказании государственных услуг (далее – служебного пользования, ЭП-СП);
- Электронная подпись, формируемая от имени органа государственной власти и органа местного самоуправления (далее – органа власти, ЭП-ОВ), участвующего в межведомственном взаимодействии при оказании государственных услуг;
- Электронная подпись, формируемая федеральным или региональным узлом СМЭВ при обработке электронных сообщений, передаваемых через нее (далее – ЭП-СМЭВ и ЭП-РСМЭВ соответственно);
- Электронная подпись, формируемая ЕПГУ при формировании электронных сообщений, передаваемых в информационные системы органов власти (далее – ЭП-ПГУ).

До момента определения Правительством Российской Федерации в соответствии с п. 2 статьи 3 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» видов электронных подписей, используемых в органах власти, применяются положения статьи 19 Федерального закона от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи».

Форматы электронных подписей, применяемых в электронных сообщениях СМЭВ, подразделяются на две категории:

- Электронные подписи субъектов взаимодействия – физических лиц (к этой категории относятся электронная подпись пользователя ЕПГУ и электронная подпись должностного лица).

– Электронные подписи субъектов взаимодействия – информационных систем (к этой категории относятся электронная подпись органа власти, электронная подпись СМЭВ/РСМЭВ, электронная подпись ЕПГУ).

3.2. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ В СМЭВ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Технологический процесс организации информационного обмена через узел СМЭВ в рамках процесса заказа услуг и межведомственного электронного взаимодействия с применением электронных подписей включает в себя:

1. В процессе оказания государственной услуги (исполнения государственной функции) пользователь портала формирует в ЕПГУ или должностное лицо ОВ формирует в информационной системе ОВ запрос к информационному ресурсу другого ведомства и подписывает электронные документы, передаваемые в запросе, своей электронной подписью (аналог собственноручной подписи) (ЭП-П и ЭП-СП соответственно);

2. Сформированный и подписанный электронной подписью субъекта взаимодействия - физического лица электронный документ, размещается в конверте электронного сообщения, который подписывается ЭП информационной системы, формирующей конверт электронного сообщения (аналог гербовой печати ведомства) (ЭП-ОВ или ЭП-ЕПГУ).

Перед подписанием должна осуществляться проверка наличия у сотрудника ОВ соответствующих полномочий и действительности его сертификата. Формирование ЭП-ОВ аналогично в данном случае простановке печати организации на подписанном должностным лицом документе;

Данная операция обязательна как при интерактивном, так и при автоматическом подписании электронных документов с использованием электронной подписи для субъектов взаимодействия – информационных систем.

3. Подписанный ЭП-СП и ЭП-ОВ запрос поступает в СМЭВ;

4. СМЭВ автоматически осуществляет:

4.1. Идентификацию ИС отправителя по сертификату ЭП информационной системы;

4.2. Проверку сертификата ЭП информационной системы в реестре информационных систем, зарегистрированных в ЕСИА;

4.3. Проверку возможности обращения ИС отправителя к ИС адресата (получателя) электронного сообщения по реестру прав доступа (далее - единой матрице доступа) СМЭВ;

4.4. Подписание запроса собственной ЭП-СМЭВ соответствующего узла (технологическая ЭП) с простановкой метки времени;

4.5. Гарантированную доставку запроса до ИС адресата.

5. ИС адресата, получив из СМЭВ запрос, может:

5.1. Проверить сертификат и корректность формирования технологической ЭП СМЭВ на документе.

Успешность проверки гарантирует:

– поступление запроса именно от СМЭВ, как информационной системы, а не от другого источника (в принципе, это гарантируется архитектурой СМЭВ);

– поступление запроса от ИС отправителя в СМЭВ во время, указанное в штампе времени;

– право на обращение ИС отправителя к ИС получателя запроса.

5.2. Проверить сертификат и корректность формирования ЭП информационной системы отправителя (ЭП-ОВ или ЭП-ПГУ) в запросе.

Успешность проверки гарантирует:

– поступление запроса в СМЭВ именно от ИС отправителя;

– целостность (то, что запрос поступил к ИС получателя от ИС ОВ-отправителя в неизменном виде);

– формирование запроса должностным лицом ОВ-отправителя или пользователем на ЕПГУ;

– обладание должностным лицом ОВ-отправителя на момент подписания запроса ЭП-ОВ в ИС ОВ соответствующими полномочиями на обращение с запросом к информационному ресурсу ОВ-получателя.

5.3. Проверить сертификат и корректность формирования ЭП-СП должностным лицом ОВ-отправителя или ЭП-П пользователя ЕПГУ.

Успешность проверки гарантирует:

– формирование запроса конкретным физическим лицом: должностным лицом – сотрудником ОВ-отправителя или пользователем ЕПГУ;

– целостность переданного электронного документа.

6. Формирование и подписание электронными подписями ответов на запросы осуществляется аналогично.

Осуществление всех трех проверок сертификатов и подписей на поступивших документах не является обязательным – достаточно наличия и соответствующей успешной проверки только лишь подписей ЭП-СМЭВ и ЭП-ОВ, что в целом гарантирует:

– целостность документа отправителя и доставку его получателю в неискаженном виде;

– право отправителя на обращение к получателю;

– наличие соответствующих полномочий у должностного лица на формирование документа в ИС ОВ-отправителя.

По мнению Минкомсвязи РФ, указанных электронных подписей в составе электронного сообщения достаточно, чтобы информационная система-получатель сообщения отработала его и, в случае необходимости, направила ответ ОВ-отправителю.

В случае, наличия соответствующего нормативно закрепленного требования, поставщик может требовать обязательное заполнение в запросах ЭП-СП уполномоченных лиц. Соответствующее требование должно быть отражено в руководстве пользователя электронного сервиса.

3.3. МЕЖВЕДОМСТВЕННОЕ ВЗАИМОДЕЙСТВИЕ НА УРОВНЕ ОДНОГО УЗЛА СМЭВ

При взаимодействии на уровне регионального узла СМЭВ между региональными участниками, подключенными к данному узлу, предусматриваются такие же правила взаимодействия информационных систем участников с узлом РСМЭВ, как и для федерального узла СМЭВ:

- формирование ЭП-ОВ от имени ИС регионального участника осуществляется с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/smev";*
- региональный узел СМЭВ формирует ЭП-РСМЭВ с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/recipient" (*данный формат является локальным).

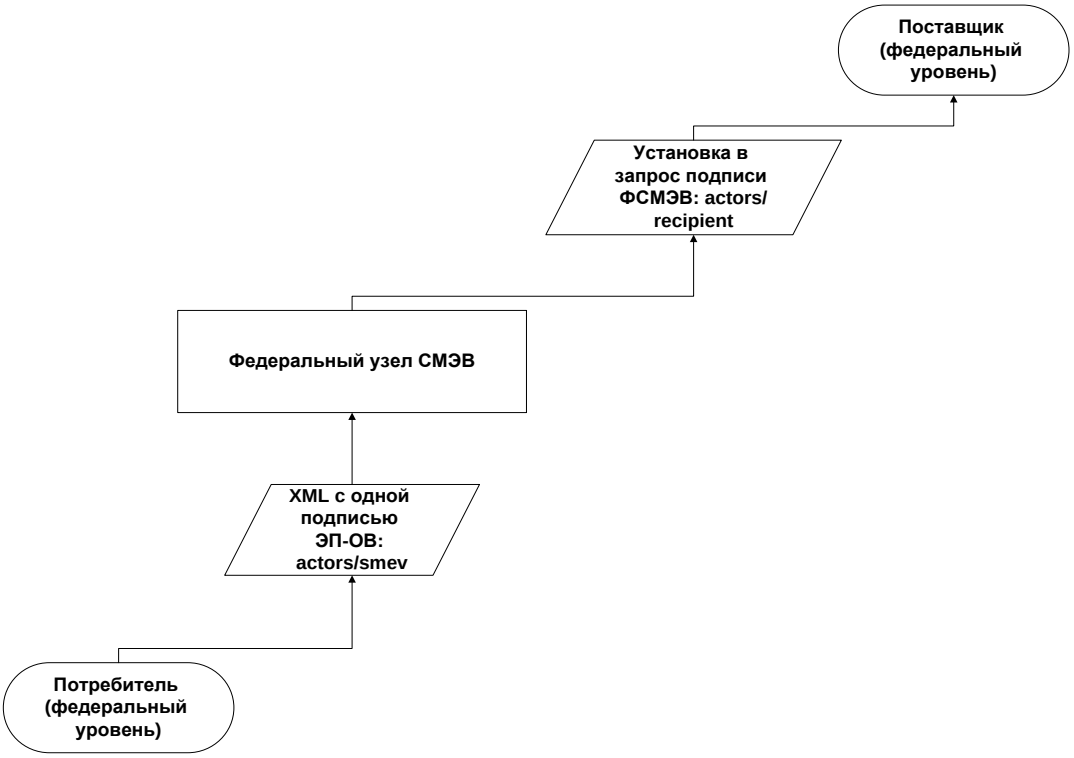


Рисунок 2 – Проставление атрибутов actor в ЭП информационных систем при взаимодействии на федеральном уровне

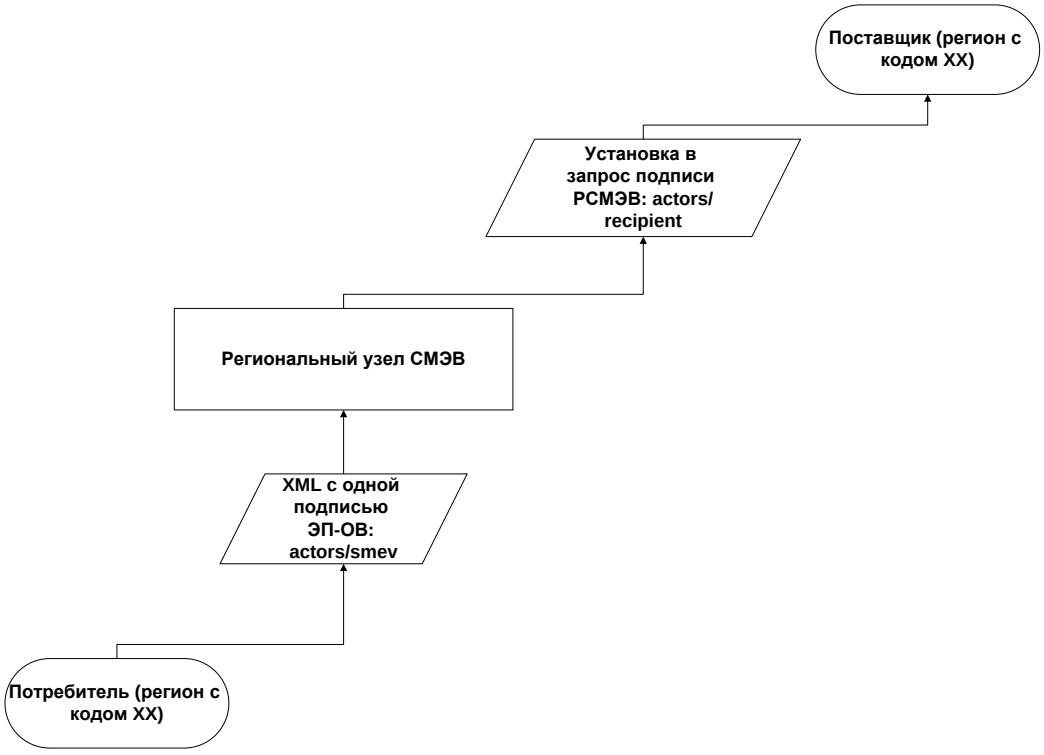


Рисунок 3 – Проставление атрибутов actor в ЭП информационных систем при взаимодействии на региональном уровне

3.4. МЕЖУРОВНЕВОЕ ВЗАИМОДЕЙСТВИЕ ЧЕРЕЗ РАЗЛИЧНЫЕ УЗЛЫ СМЭВ

При межуровневом взаимодействии через различные узлы СМЭВ для участников предусматриваются аналогичные правила использования атрибутов ЭП ИС, а также для ЭП-СМЭВ/ЭП-РСМЭВ для федерального и регионального узла:

1. потребитель при запросе формирует ЭП-ОВ для своей информационной системы с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/smev";*
2. узел СМЭВ, к которому подключена ИС потребителя, при запросе формирует ЭП-СМЭВ/ЭП-РСМЭВ с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/smevXX"* (где XX – соответствует коду узла, к которому будет осущетвляться обращение для доступа к системе поставщика);
3. узел СМЭВ, к которому подключена ИС поставщика, при запросе формирует ЭП-СМЭВ/ЭП-РСМЭВ с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/recipient";*
4. поставщик при ответе на запрос формирует ЭП-ОВ для своей информационной системы с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/smev";*
5. узел СМЭВ, к которому подключена ИС поставщика, при ответе на запрос формирует ЭП-СМЭВ/ЭП-РСМЭВ с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/smevYY"* (где YY – соответствует коду узла, к которому будет осущетвляться обращение для доступа к системе потребителя);
6. узел СМЭВ, к которому подключена ИС потребителя, при ответе на запрос формирует ЭП-СМЭВ/ЭП-РСМЭВ с использованием атрибута actor=*"http://smev.gosuslugi.ru/actors/recipient".*

Таким образом, можно видеть, что значения атрибута actor совпадают в шагах 1,3, 4 и 6 с теми значениями, которые используются при обмене на уровне одного узла.

Специфика, возникающая из-за того, что на самом деле сообщение проходит через несколько узлов СМЭВ для доставки сообщения от потребителя к поставщику, проявляется на шагах 2 и 5, что связано с тем, что в данном случае промежуточным получателем сообщения, отправляемого от «ближайшего» к отправителю узла, является узел, являющийся «ближайшим» к получателю.

Аналогичная логика используется при формировании унифицированных служебных заголовков узлов СМЭВ.

Данные особенности необходимо учитывать для проверки значений ЭП, формируемых от лица информационных систем, участниками межуровневого обмена.

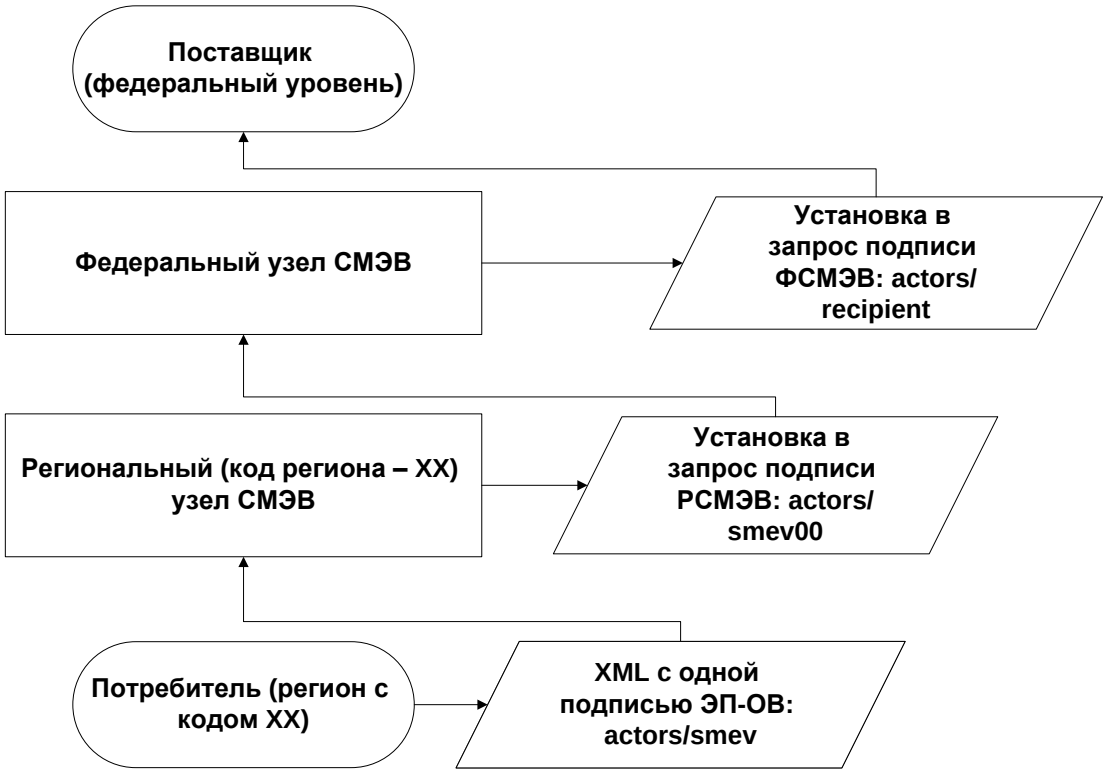


Рисунок 4 – Проставление атрибутов actor в ЭП информационных систем при межуровневом взаимодействии: вызов региональным потребителем федерального поставщика

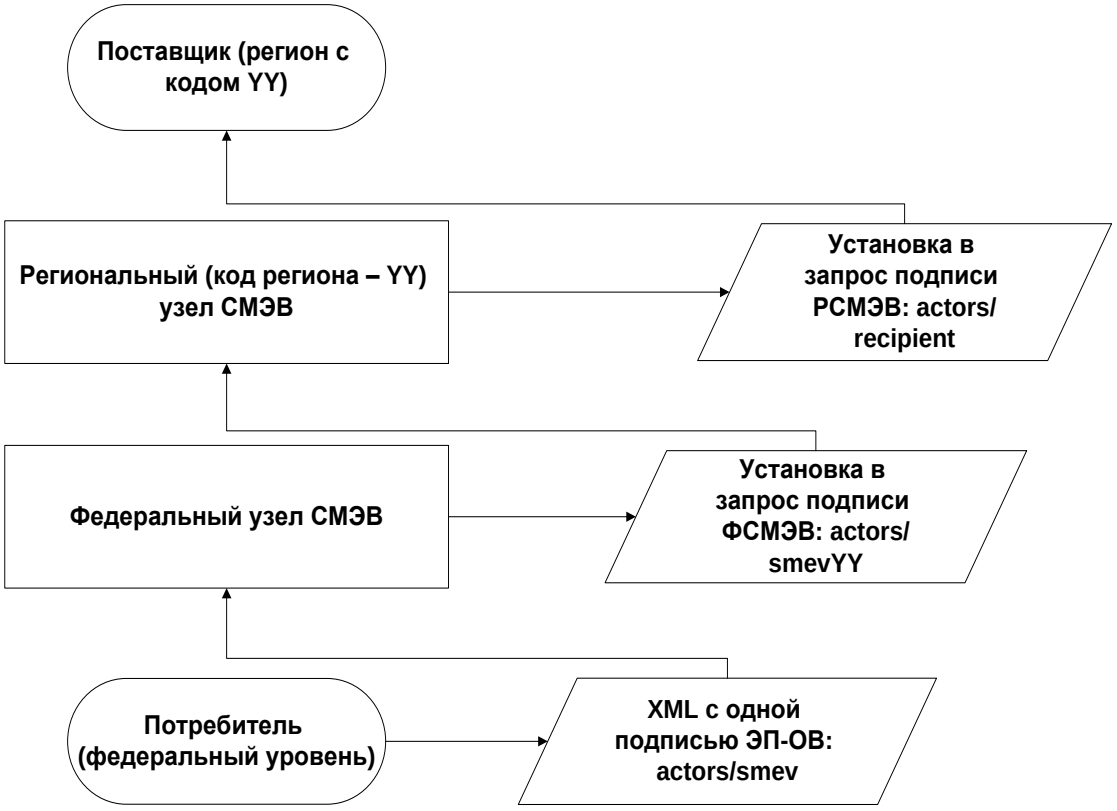


Рисунок 5 – Проставление атрибутов actor в ЭП информационных систем при межуровневом взаимодействии: вызов региональным потребителем федерального поставщика

3.5. ПРОВЕРКА СЕРТИФИКАТОВ И ПОДПИСЕЙ

Проверка сертификатов ключей электронной подписи и корректности формирования электронной подписи осуществляется:

– для электронной подписи субъектов взаимодействия - информационных систем (ЭП-СМЭВ, ЭП-ОВ, ЭП-ПГУ) – для проверки действительности сертификатов и значений электронной подписи - специализированным сервисом проверки (далее – СПЭП), зарегистрированным в СМЭВ. Проверка значений электронной подписи может также осуществляться без вызова специализированного сервиса проверки электронной подписи, средствами самой ИС;

– для электронной подписи субъектов взаимодействия – физических лиц (ЭП-П и ЭП-СП) – сервисом проверки сертификатов ЕПД, также зарегистрированным в СМЭВ.

3.5.1. Проверка электронной подписи ИС при межуровневом взаимодействии через СМЭВ

При обращении к узлу СМЭВ одной из проверок, осуществляемых для электронного сообщения, является проверка ЭП информационной системы – потребителя. Аналогичные проверки производятся и при обращении к федеральному и при обращении к региональным узлам СМЭВ. Установка подписи ЭП-СМЭВ/ЭП-РСМЭВ осуществляется, в случае успешного прохождения проверок на уровне соответствующего узла.

При обращении к региональному сервису с федерального уровня – региональная СМЭВ проверяет ЭП федерального узла СМЭВ, которая проставлятся, в случае успешного прохождения проверки подписи ЭП-ОВ на федеральному уровне.

При обращении к федеральному сервису с регионального уровня – федеральная СМЭВ проверяет ЭП регионального узла СМЭВ, которая проставляется, в случае успешного прохождения проверки подписи ЭП-ОВ на региональном уровне.

4. ЭЛЕКТРОННЫЕ ПОДПИСИ СУБЪЕКТОВ ВЗАИМОДЕЙСТВИЯ – ФИЗИЧЕСКИХ ЛИЦ

4.1. ОБЩИЕ ТРЕБОВАНИЯ К ЭЛЕКТРОННОЙ ПОДПИСИ, ФОРМИРУЕМОЙ ОТ ЛИЦА ПОЛЬЗОВАТЕЛЯ ЕПГУ ПРИ ЗАКАЗЕ УСЛУГ

Сертификаты и ключи электронной подписи (п. 3 ст. 14 Федерального закона № 63-ФЗ «Об электронной подписи») пользователя Единого портала государственных услуг (функций) выдаются на имя физического лица пользователя портала и применяются в информационных системах инфраструктуры электронного правительства при подписании сведений в запросах на оказание государственных и муниципальных услуг в электронном виде для формирования и (или) проверки электронных подписей.

Данные подписи аналогичны собственноручным подписям этих пользователей и подтверждают, в том числе, факт формирования электронного документа конкретным пользователем в ЕПГУ.

Ответственность за хранение и использование ключа подписи ЭП-П несет пользователь портала.

4.2. ОБЩИЕ ТРЕБОВАНИЯ К ЭЛЕКТРОННОЙ ПОДПИСИ, ФОРМИРУЕМОЙ ОТ ИМЕНИ ДОЛЖНОСТНЫХ ЛИЦ ОРГАНОВ ВЛАСТИ ПРИ МЕЖВЕДОМСТВЕННОМ ИНФОРМАЦИОННОМ ОБМЕНЕ

Сертификаты и ключи электронной подписи (п. 3 ст. 14 Федерального закона № 63-ФЗ «Об электронной подписи») должностного лица выдаются на имя физического лица представителя органа власти и применяются в информационных системах при оказании государственных и муниципальных услуг/исполнении государственных и муниципальных функций с использованием системы межведомственного электронного взаимодействия для формирования и (или) проверки электронных подписей.

Данные подписи 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 и 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 удостоверяющих центров,

входящих в единое пространство доверия ЭП, формируемое Минкомсвязью РФ (далее – ЕПД).

4.3. ЭЛЕКТРОННАЯ ПОДПИСЬ ПРИ ПОДАЧЕ ЗАЯВЛЕНИЙ С ЕПГУ ИЛИ ПРИ МЕЖВЕДОМСТВЕННОМ ВЗАИМОДЕЙСТВИИ ДЛЯ СООБЩЕНИЙ С ВЛОЖЕНИЯМИ

4.3.1. Правила формирования архива вложений и электронной подписи файлов для электронных сообщений, содержащих вложения

При подаче заявлений с ЕПГУ, а также при межведомственном взаимодействии, подразумевающем передачу вложений, файл заявления и файлы вложений передаются не по отдельности в электронных сообщениях, а сгруппированные в одном архиве (сформированном по алгоритму zip).

Архив (в формате Base64) или ссылки на него (в случае передачи вложения вне SOAP конверта) размещаются внутри подэлементов элемента smev:AppDocument.

Архив содержит следующие файлы:

- Заявление в информационную систему Поставщика в формате XML со ссылками на вложения.
- Электронную подпись физического лица, соответствующую файлу заявления на основе стандарта PKCS#7 (detached).
- Вложения в виде файлов форматов, согласованных с поставщиком сервиса;
- Электронные подписи физического лица, соответствующие каждому из файлов вложений, передаваемых в архиве, на основе стандарта PKCS#7 (detached).

  В случае подачи заявления с ЕПГУ электронная подпись к файлам вложений формируется с использованием сертификата ключа ЭП-ПГУ, если это не противоречит нормативно обоснованным требованиям участника-поставщика услуги.

  Имя файла заявления должно соответствовать определенной маске:

```
req_<GUID_заявления>.xml
```

где GUID_заявления - статистически уникальный 128-битный идентификатор (GUID) унифицированного вида (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx).

Имя архива должно соответствовать определенной маске:

```
req_<GUID_заявления>.zip
```

При формировании имени архива должен использоваться тот же GUID_заявления, что и при формировании файла заявления.

Электронные документы и их электронные подписи могут находиться на любом уровне вложенности в архиве, но пути должны быть прописаны в xml-файле заявления в соответствии с определенным форматом.

Файлы электронной подписи для заявлений и вложений в формате PKCS#7 (detached) имеют формализованное правило именования, при котором к имени исходного файла добавляется постфикс *.sig.

Пример именования файла подписи указан в таблице ниже.

Наименование файла	Наименование файла подписи
req_xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.xml	req_xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.xml.sig
attachment.txt	attachment.txt.sig

При описании вложений в файле заявления должны применяться следующие правила:

- Группа вложений описывается элементом AppliedDocuments.
- Каждое вложение описывается одним элементом AppliedDocument.
- Каждый элемент AppliedDocument должен содержать следующие элементы:

CodeDocument	Код документа.
Name	Имя файла документа.
Number	Номер документа.
URL	Относительный путь к файлу внутри архива.
Type	Тип контента (например: application/pdf или любой другой общепринятый MIME-тип)
DigestValue	Хеш-код вложения, рассчитываемый по

	ГОСТ Р 34.11-94.

В дополнение к перечисленным элементам поставщики могут использовать свои элементы при условии того, что они будут дочерними к тегу AppliedDocument.

Архив (в формате Base64) может передаваться как внутри SOAP-конверта электронного сообщения, так и вне его.

XSD описание структур данных, используемых для описания вложений внутри заявлений, приведено в приложении 4.

4.3.2. Порядок формирования архива вложений и электронной подписи

1. Генерация GUID по маске xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, где x описывается регулярным выражением [a-z0-9].
2. Формирование обращения на сервис ИС ОВ в формате XML с именем req_GUID.xml со ссылками на файлы-вложения.
3. Расчет хеш-кода каждого вложения и размещение полученных значений в структуру smev:AppliedDocuments в составе элемента smev:DigestValue.
4. Подпись каждого вложения по стандарту PKCS#7 и получение одноименных файлов. Пример: подпись attachment.pdf и получение attachment.pdf.sig.
5. Подпись XML-запроса по стандарту PKCS#7 и получение файла подписи req_GUID.xml.sig.
6. XML-заявление, его подпись, а также все вложения и их подписи архивируются в zip-файла наименованием req_GUID.zip.
7. Код заявления req_GUID проставляется в элемент smev:RequestCode.
8. Архив req_GUID.zip кодируется в Base64 и полученный код становится содержимым элемента smev:BinaryData в электронном сообщении СМЭВ (или передается вне сообщения как MTOM-attachment).

4.3.3. Передача архива вложений в блоке бинарных вложений

Пример передачи архива в виде бинарного вложения с использованием элемента smev:BinaryData.

```
<soapenv:Envelope …>
    . . . . .
   <soapenv:Body wsu:Id = …>
```

```
. . . . .
    <smev:MessageData>
      <smev:AppDocument>
. . . . .
        <smev:RequestCode>req_7d6476ac-a728-4863-804e-a5789d29c630</smev:RequestCode>

<smev:BinaryData>UEsDBAoAAAAAABBrAz/mb01kEgAAABIAAAAsAAAAcmVxXzk5NTM4MTAwLTliMjgtNDc4NC1iNDM3LTFmYjBkYTEzNzU5NS54bWw8ZGF0YT4KRGF0YTwvZGF0YT5QSwMECgAAAAAAE2sDP0lKW5b+BQAA/gUAADAAAAByZXFfOTk1MzgxMDAtOWIyOC00Nzg0LWI0MzctMWZiMGRhMTM3NTk1LnhtbC5zaWctLS0tLUJFR0lOIFBLQ1M3LS0tLS0KTUlJRVdnWU</smev:BinaryData>
      </smev:AppDocument>
    </smev:MessageData>
. . . . .
  </soapenv:Body>
</soapenv:Envelope>
```

4.3.4. Передача архива вложений вне конверта электронного сообщения

При передаче архива вложений вне SOAP-конверта электронного сообщения используются элементы smev:Reference и его дочерний элемент xop:Include (ссылка на вложение), а также элемент smev:DigestValue (в пространстве имен xmlns:smev).

Если архив с подписанными данными передается вне электронного сообщения (передается SOAP пакет: Multipart-сообщение, одна часть которого – это SOAP-сообщение, а другая – MTOM attachment), то необходимо заполнение следующих двух элементов:

- Хеш-код Base64 архива;
- Content-ID блока данных (attachment), передаваемого вне сообщения.

Хеш-код архива в Base64 должен быть рассчитан с помощью криптографической хеш-функции по стандарту ГОСТ Р 34.11-94. Полученное значение должно быть размещено внутри элемента smev:DigestValue.

Ссылка на attachment должна быть отражена в сообщении посредством тега xop:Include со значением атрибута href, равным Content-ID вложения, передаваемого вне электронного сообщения СМЭВ.

Атрибут start= может отсутствовать, тогда базовый SOAP запрос будет идентифицироваться по паре start-info="text/xml"; type="application/xop+xml"; и Content-Type: application/xop+xml;type="text/xml" соответственно.

```
MIME-Version: 1.0

Content-type: multipart/related;
start="<rootpart*c73c9ce8-6e02-40ce-9f68-064e18843428>";
start-info="text/xml";
type="application/xop+xml";
boundary="MIME_boundary";



--MIME_boundary

Content-Type: application/xop+xml;charset=utf-8;type="text/xml"
Content-Id: <rootpart*c73c9ce8-6e02-40ce-9f68-064e18843428>
Content-Transfer-Encoding: binary



<?xml version='1.0' ?>

<soapenv:Envelope …>

    . . . . .

   <soapenv:Body wsu:Id = …>

    . . . . .

         <smev:MessageData>

            <smev:AppDocument>

           <smev:RequestCode>req_7d6476ac-a728-4863-804e-a5789d29c630</smev:RequestCode>

      <smev:Reference>

      <xop:Include xmlns:xop="http://www.w3.org/2004/08/xop/include" href="cid:5aeaa450-17f0-4484-b845-
a8480c363444" />

      </smev:Reference>



<smev:DigestValue>Хеш кода архива</smev:DigestValue>

            </smev:AppDocument>

         </smev:MessageData>

    . . . . .

   </soapenv:Body>

</soapenv:Envelope>
```

```
--MIME_boundary
Content-Type: application/zip
Content-Transfer-Encoding: binary
Content-ID:5aeaa450-17f0-4484-b845-a8480c363444

...binary ZIP image...
--MIME_boundary--
```

4.4. ЭЛЕКТРОННАЯ ПОДПИСЬ ПРИ МЕЖВЕДОМСТВЕННОМ ВЗАИМОДЕЙСТВИИ В СООБЩЕНИЯХ БЕЗ ВЛОЖЕНИЙ

4.4.1. Правила формирования электронной подписи физического лица при межведомственном взаимодействии для сообщений без вложений

Для сообщений, не содержащих вложения, для удостоверения блока структурированных данных, используется электронная подпись, сформированная в соответствии с форматом XMLDSig (XMLDSIG-CORE «XML-Signature Syntax and Processing».
Опубликован в Интернете по адресу: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212).

Блок подписи размещается как дочерний для элемента smev:AppData, на одном уровне с прикладными данными.

Значение подписи должно рассчитываться для содержимого элемента smev:AppData и его составных элементов. При этом для привязки подписи к элементу smev:AppData используется атрибут Id.

```
<smev:AppData Id="AppData">...</smev:AppData>
```

В процессе создания электронной подписи информационной системы должны использоваться следующие алгоритмы для расчета хеш-сумм, формирования подписи и каноникализации:

	Наименование	URI
Расчет хеш-сумм	ГОСТ Р 34.11-94	http://www.w3.org/2001/04/xmldsig-more#gostr3411
Формирования	ГОСТ Р 34.10-2001	http://www.w3.org/2001/04/xmldsig-

подписи		more#gostr34102001-gostr3411
Каноникализация	Exclusive XML Canonicalization от 18 июля 2002	http://www.w3.org/2001/10/xml-exc-c14n#

Подписание электронного сообщения необходимо выполнять непосредственно перед отправкой, чтобы избежать искажений передаваемого XML при передаче через информационные системы с потерей соответствия между данными и подписью.

4.4.2. Порядок формирования электронной подписи физического лица при межведомственном взаимодействии для сообщений без вложений

Формирование блока электронной подписи, соответствующей блоку структурированных данных осуществляется в следующем порядке:

1. Формирование шаблона документа:

1.1. Создается элемент *Signature;*

1.2. К элементу *Signature* добавляется дочерний элемент *SignedInfo;*

1.3. К элементу *SignedInfo* добавляется дочерний элемент *CanonicalizationMethod;*

1.4. К элементу *SignedInfo* добавляется дочерний элемент *SignatureMethod;*

1.5. К элементу *SignedInfo* добавляется первый дочерний элемент *Reference;*

1.6. К элементу *Reference* добавляется дочерний элемент *Transforms;*

1.7. К элементу *Transforms* элемента *Reference* добавляется дочерний элемент *Transform (два элемента);*

1.8. К элементу *Reference* добавляется элемент *DigestMethod;*

1.9. К элементу *Reference* добавляется элемент *DigestValue;*

1.10. К элементу *Signature* добавляется дочерний элемент *SignatureValue;*

1.11. К элементу *Signature* добавляется дочерний элемент *KeyInfo;*

1.12. К элементу *KeyInfo* добавляется дочерний элемент *X509Data;*

1.13. К элементу *X509Data* добавляется дочерний элемент *X509Certificate.*

2. Установка предопределенных значений

2.1. Для элемента *CanonicalizationMethod* и для второго элемента *Transform* элемента *Reference* значения атрибута *Algorithm* устанавливается в «http://www.w3.org/2001/10/xml-exc-c14n#».

Для первого элемента *Transform* алгоритм выставляется значение "http://www.w3.org/2000/09/xmldsig#enveloped-signature".

2.2. Для элементов *DigestMethod* первого значения атрибута *Algorithm* устанавливается в "http://www.w3.org/2001/04/xmldsig-more#gostr3411".

2.3. Для элемента *SignatureMethod* значение атрибута *Algorithm* устанавливается в "http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411".

2.5. Атрибут *URI* элемента *Reference* заполняется выбранным значением (ссылка на атрибут id элемента smev:AppData.

3. Установка подписи

3.1. Открытый ключ подписи, закодированный по алгоритму «http://www.w3.org/2000/09/xmldsig#base64», после удаления символов не входящих в алфавит Base64, добавляется к элементу X509Certificate как дочерний текстовый узел.

3.2. Подписываются элементы документа, выбранные посредством XPATH выражения на основе значения атрибута URI элемента Reference.

Полученное значение кодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64» и добавляется как дочерний текстовый узел к элементу DigestValue первого элемента Reference.

3.3. Элемент SignedInfo трансформируется в соответствии с алгоритмом «http://www.w3.org/2001/10/xml-exc-c14n#». Затем на основании полученной строки и ключа подписи формируется значение ЭП в соответствии с алгоритмом «http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411». Полученное значение ЭП кодируется в соответствии с алгоритмом «http://www.w3.org/2000/09/xmldsig#base64», символы не входящие в алфавит Base64 удаляются и полученное значение добавляется как дочерний текстовый узел к элементу SignatureValue.

4.4.3. Пример формирования электронной подписи физического лица при межведомственном взаимодействии для сообщений без вложений

```
<soapenv:Envelope …>
   . . . . .
  <soapenv:Body wsu:Id = …>
   <smevSampleMsg:sampleRequest xmlns:smevSampleMsg="http://smev.gosuslugi.ru/SampleMessage">
```

```
      <smev:Message>...</smev:Message>
  <smev:MessageData>
            <smev:AppData Id="AppData">
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig">
            <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>
            <ds:Reference URI="#AppData">
            <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
            <ds:DigestValue>Значение хеша в Base64</ds:DigestValue>
            </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>Значение подписи в Base64</ds:SignatureValue>
            <ds:KeyInfo>
            <ds:X509Data>
            <ds:X509Certificate>Сертификат X.509 в Base64</ds:X509Certificate>
            </ds:X509Data>
            </ds:KeyInfo>
            </ds:Signature>
           </smev:AppData>
        </smev:MessageData>
    </smevSampleMsg:sampleRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

5. ЭЛЕКТРОННЫЕ ПОДПИСИ СУБЪЕКТОВ ВЗАИМОДЕЙСТВИЯ – ИНФОРМАЦИОННЫХ СИСТЕМ

5.1. ОБЩИЕ ТРЕБОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ, ФОРМИРУЕМОЙ ОТ ИМЕНИ ОРГАНА ВЛАСТИ ПРИ МЕЖВЕДОМСТВЕННОМ ИНФОРМАЦИОННОМ ОБМЕНЕ

Сертификаты и ключи электронной подписи (п. 3 ст. 14 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»), используемые для формирования электронных подписей органа власти выдаются на имя органа власти и применяются в информационных системах при оказании государственных и муниципальных услуг/исполнении государственных и муниципальных функций с использованием СМЭВ для формирования ЭП.

ЭП-ОВ аналогичны гербовой печати организации и подтверждают:

- факт формирования межведомственного запроса (проект Федерального закона «О внесении изменений в отдельные законодательные акты» (ранее проект федерального закона № 535056) 22.06.2011 одобренный Советом Федерации Федерального Собрания Российской Федерации) 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 СМЭВ 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).

По согласованию допускается несколько электронных подписей ЭП-ОВ для одного органа исполнительной власти.

Количество формируемых на ОВ сертификатов ЭП-ОВ не может быть меньше количества информационных систем данного ОВ, непосредственно подключенных к СМЭВ.

Ответственность за хранение и использование ключа подписи ЭП-ОВ обеспечивается организационно-техническими мероприятиями ведомства, на которое они выданы.

5.2. ОБЩИЕ ТРЕБОВАНИЯ К ЭЛЕКТРОННОЙ ПОДПИСИ, ФОРМИРУЕМОЙ УЗЛАМИ СМЭВ

Сертификаты и ключи электронной подписи (п. 3 ст. 14 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»), используемые для формирования электронных подписей в сообщениях, проходящих через федеральный и региональные узлы СМЭВ, выдаются на имя оператора соответствующей системы межведомственного электронного взаимодействия и применяются для формирования ЭП.

ЭП-СМЭВ/ЭП-РСМЭВ подтверждает:

- факт прохождения электронного сообщения через узел СМЭВ
- факт аутентификации и авторизации в соответствии с правилами, указанными в реестре прав доступа к электронным сервисам (матрице доступа)
- неизменность сведений, внесенных в электронное сообщение СМЭВ/РСМЭВ
- валидность сертификата СМЭВ на момент подписания сообщения подписью ЭП-СМЭВ/ЭП-РСМЭВ за счет проставления в ЭП-СМЭВ/ЭП-РСМЭВ метки времени

Сертификат ЭП-СМЭВ/ЭП-РСМЭВ выдается на каждый отдельный узел системы межведомственного электронного взаимодействия.

Ответственность за хранение и использование ключа подписи ЭП-СМЭВ/ЭП-РСМЭВ обеспечивается организационно-техническими мероприятиями оператора СМЭВ/оператора РСМЭВ.

5.2.1. Метка времени в электронной подписи, формируемой узлами СМЭВ

Метка времени – это подписанное электронной подписью сервера меток времени ИС ГУЦ CMS-сообщение, содержащее штамп времени, которым Главный Удостоверяющий Центр (ГУЦ) заверяет, что в указанный момент времени ему было предоставлено значение хеш-функции сообщения СМЭВ. Само значение хеш-функции также указывается в метке. Проставление меток времени в ходе асинхронного взаимодействия через СМЭВ позволяет:

- обеспечить юридическую значимость событий транспортного уровня (доставка сообщения Поставщику/Потребителю, получение ответа от Поставщика, получение статусного сообщения от Потребителя/Поставщика)
- зафиксировать строгую временную последовательность, в которой происходили события в ходе асинхронного взаимодействия через СМЭВ

Установка метки времени в электронное сообщение СМЭВ происходит сразу за шагом установки ЭП-СМЭВ, с использованием сервиса меток времени ИС ГУЦ, работающим по протоколу TSP (Time-Stamp Protocol, RFC3161) над HTTP. После установки узлом СМЭВ своей электронной подписи на сообщение, оно передается сервису установки метки времени, который, в свою очередь, извлекает его хеш, составляет TSP-запрос к сервису меток времени ИС ГУЦ, получает метку времени, проверяет её и возвращает в качестве результата исходное сообщение, включающее в себя метку времени.

Так как электронная подпись узла СМЭВ/РСМЭВ содержит метку времени, для её хранения в электронном сообщении используется расширение стандарта XMLDSIG - **XAdES-T.**

Стандарт вводит новый элемент ds:Object внутри блока ds:Signature. Блок ds:Object предназначен для хранения атрибутов электронной подписи, обеспечивающих её дополнительную защиту. Метка времени хранится в элементе EncapsulatedTimeStamp внутри блока ds:Object в коде Base64 (см. пример):

```
<wsse:Security env:actor="http://smev.gosuslugi.ru/actors/recipient" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">

  <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="CertId ">…</wsse:BinarySecurityToken>

      <ds:Signature Id="Signature-95751" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

        <ds:SignedInfo>

          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

          <ds:Reference URI="#ID-8df52b70-e4a3-43d9-b8c8-a627b3394dee">

            <ds:Transforms>

              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

            </ds:Transforms>

            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

            <ds:DigestValue>QOvzEDVAl9k00nG95gDBPz0/hdBcy5CpPasPEk1Rn+g=</ds:DigestValue>

          </ds:Reference>

          <ds:Reference URI="#id-95750">

            <ds:Transforms>
```

```
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
              <ds:DigestValue>8JclaFFiTTCokhPtXC/bHatjEvEUYEK5FHuBnUKDgNs=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>

<ds:SignatureValue>DDQ91uii+Rvtz2qqFCDzsXOULWuKIkwBh2ticarnI6C1OYe1uKf9IBqKoMUiDmSyhnzS259Twbm5
+se0pUlOMQ==</ds:SignatureValue>
          <ds:KeyInfo Id="KeyId-C7F269720BE6F58D941344862536377285845">
            <wsse:SecurityTokenReference wsu:Id="STRId-C7F269720BE6F58D941344862536377285846">
              <wsse:Reference URI="#CertId-C7F269720BE6F58D941344862536376285844"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
            </wsse:SecurityTokenReference>
          </ds:KeyInfo>

          <ds:Object>
            <xds:QualifyingProperties  xmlns:xds="http://uri.etsi.org/01903/v1.1.1#">
              <xds:UnsignedProperties>
                <xds:UnsignedSignatureProperties>
                  <xds:SignatureTimeStamp>
                    <xds:HashDataInfo uri="#signature-value-40ddb6ca-9ac1-4026-a049-76901f3aa5d8"/>
                    <xds:EncapsulatedTimeStamp>Метка времени в Base64</xds:EncapsulatedTimeStamp>
                  </xds:SignatureTimeStamp>
                  </xds:UnsignedSignatureProperties>
              </xds:UnsignedProperties>
            </xds:QualifyingProperties>
          </ds:Object>
        </ds:Signature>
      </wsse:Security>
```

5.3. ОБЩИЕ ТРЕБОВАНИЯ К ЭЛЕКТРОННОЙ ПОДПИСИ, ФОРМИРУЕМОЙ ЕПГУ

Сертификаты и ключи электронной подписи (п. 3 ст. 14 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»), используемые для формирования электронных подписей в сообщениях, формируемых в ЕПГУ, выдаются на имя оператора Единого портала государственных и муниципальных услуг (функций) и применяются для формирования ЭП.

ЭП-ПГУ подтверждает:

- факт формирования запроса на оказание услуг в электронном виде в информационной системе ЕПГУ;
- факт аутентификации и авторизации в личном кабинете ЕПГУ у лица, сформировавшего запрос в электронном виде на оказание услуг;
- неизменность переданных данных при передаче к ИС потребителя.

Сертификат ЭП-ПГУ выдается для каждого портала государственных услуг в инфраструктуре электронного правительства.

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

5.4. ПРАВИЛА ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Структура электронной подписи информационной системы должна соответствовать стандарту OASIS Standard 200401 (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf) с профилем X.509 Certificate Token Profile (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf).

В изложении используются следующие соответствия:

soapenv	http://schemas.xmlsoap.org/soap/envelope/
ds	http://www.w3.org/2000/09/xmldsig#
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd

В процессе создания электронной подписи информационной системы должны использоваться следующие алгоритмы для расчета хеш-сумм, формирования подписи и каноникализации:

	Наименование	URI
Расчет хеш-сумм	ГОСТ Р 34.11-94	http://www.w3.org/2001/04/xmldsig-more#gostr3411
Формирования подписи	ГОСТ Р 34.10-2001	http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411
Каноникализация	Exclusive XML Canonicalization от 18 июля 2002	http://www.w3.org/2001/10/xml-exc-c14n#

Для определения того, кому предназначается электронная подпись, используется атрибут actor блока Security.

Информационная система органа власти (потребителя) или ПГУ при формировании запроса к ИС поставщика, а также ИС Поставщика при формировании ответа должны проставлять в атрибуте actor значение, соответствующее СМЭВ как стороне проверяющей подпись:

```
soapenv:actor="http://smev.gosuslugi.ru/actors/smev"
```

При взаимодействии в пределах узла СМЭВ, для формирования электронной подписи в запросе и отправке его поставщику или отправке ответа к потребителю, проставляет в атрибуте actor значение:

```
soapenv:actor="http://smev.gosuslugi.ru/actors/recipient"
```

При межуровневом взаимодействии, для формирования электронной подписи ЭП-СМЭВ/ЭП-РСМЭВ в сообщениях применяется следующее правило использования атрибута actor для формирования подписи в транзитном формате:

soapenv:actor="*http://smev.gosuslugi.ru/actors/smevXX*"

где XX – состоящий из двух символов код региона узла СМЭВ, обращение к которому осуществляется для доставки электронного сообщения участнику взаимодействия.

Подписание электронного сообщения необходимо выполнять непосредственно перед отправкой, чтобы избежать искажений передаваемого XML при передаче через информационные системы с потерей соответствия между данными и подписью.

При подписании XML структур данных усовершенствованной электронной подписью рекомендуется использовать стандарт XML Advanced Electronic Signatures (XAdES) (http://www.w3.org/TR/XAdES/).

Для доказательства факта времени создания электронной подписи XML для структур данных рекомендуется использовать усовершенствованную подпись по стандарту XML Advanced Electronic Signatures with Time-Stamp (XAdES-T).

5.5. ПОРЯДОК ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

1. В сообщение добавляются объявления префиксов пространств имен. Префиксы можно определять по мере необходимости.

```
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
.....
</soapenv:Envelope>
```

2. Проставляется атрибут wsu:Id="body" элементу Body сообщения.

```
<soapenv:Envelope ...>
    ......
  <soapenv:Body wsu:Id="body">
    ........
</soapenv:Body>

</soapenv:Envelope>
```

3. Происходит подготовка структуры для сохранения результатов.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope .....>
  <soapenv:Header>
    <wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/smev">
        <wsse:BinarySecurityToken/>
        <ds:Signature>

        <ds:SignedInfo>
          <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <ds:SignatureMethod
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411" />
        </ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo/>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="body">
    .......
```

```
  </soapenv:Body>
</soapenv:Envelope>
```

Замечание: наличие атрибута Id для элементов ds:SignedInfo, ds:KeyInfo не является ошибкой, например <ds:KeyInfo Id=*"KeyId"*/> допустимое использование.

4. В <wsse:BinarySecurityToken/> добавляются атрибуты форматов и собственно сам сертификат и атрибут wsu:Id.

   Формат сертификата должен соответствовать спецификации X.509 и быть представленным в формате Base64.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope .....>
  <soapenv:Header>
    <wsse:Security soapenv:actor=".....">
      <wsse:BinarySecurityToken
            EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
            wsu:Id="CertId">MIIDjjCCAz2.....</wsse:BinarySecurityToken>
       <ds:Signature>

         <ds:SignedInfo>
           .........
         </ds:SignedInfo>
           .........
       </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
    .......
</soapenv:Envelope>
```

5. Добавляется ссылка на токен в раздел <ds:KeyInfo>.
   Значение атрибута URI элемента wsse:Reference должно соответствовать значению атрибута wsu:Id элемента wsse:BinarySecurityToken без лидирующего знака '#'.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope .....>
  <soapenv:Header>
    <wsse:Security soapenv:actor=".....">
      <wsse:BinarySecurityToken .....
            wsu:Id="CertId">....</wsse:BinarySecurityToken>
       <ds:Signature>

         <ds:SignedInfo>
           .........
         </ds:SignedInfo>
         <ds:SignatureValue>.....</ds:SignatureValue>

         <ds:KeyInfo>

           <wsse:SecurityTokenReference>
```

```
            <wsse:Reference URI="#CertId"

              ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"/>

            </wsse:SecurityTokenReference>

          </ds:KeyInfo>
        </ds:Signature>
      </wsse:Security>
    </soapenv:Header>
      .....
nv:Envelope>
```

Замечание: Наличие атрибута wsu:Id для элементов **wsse:SecurityTokenReference** не является ошибкой.

6. Добавляется ссылка на данные для подписи и параметры каноникализации.

   Значение атрибута URI элемента ds:Reference должно соответствовать значению атрибута wsu:Id элемента soapenv:Body без лидирующего знака '#'.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope .....>
  <soapenv:Header>
    <wsse:Security soapenv:actor="......">
      <wsse:BinarySecurityToken ......>....</wsse:BinarySecurityToken>
      <ds:Signature>

        <ds:SignedInfo>
          <ds:CanonicalizationMethod ...... />
          <ds:SignatureMethod ...../>
          <ds:Reference URI="#body">
            <ds:Transforms>
              <ds:Transform
                Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod
                Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
            <ds:DigestValue/>
          </ds:Reference>
          .........
        </ds:SignedInfo>
        <ds:SignatureValue>.....</ds:SignatureValue>
        <ds:KeyInfo>.........</ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="body">
    .......
  </soapenv:Body>
</soapenv:Envelope>
```

7. К элементу <soapenv:Body> и его потомкам, включая атрибуты, применяется каноникализация *http://www.w3.org/2001/10/xml-exc-c14n#*, на основе результата рассчитывается хеш по алгоритму ГОСТ Р 34.11-94 и заносится в <ds:DigestValue> в формате Base64.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope .....>
  <soapenv:Header>
    <wsse:Security soapenv:actor="......">
      <wsse:BinarySecurityToken ......>....</wsse:BinarySecurityToken>
      <ds:Signature>

        <ds:SignedInfo>
          <ds:CanonicalizationMethod ..... />
          <ds:SignatureMethod ...../>
          <ds:Reference URI="#body">
            <ds:Transforms>
              <ds:Transform .../>
            </ds:Transforms>
            <ds:DigestMethod..../>
            <ds:DigestValue>d7Q3878nvrGVpOI.....</ds:DigestValue>
          </ds:Reference>
          .........
        </ds:SignedInfo>
          ........
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="body">
    .......
  </soapenv:Body>
</soapenv:Envelope>
```

8. К элементу <ds:SignedInfo> и его потомкам, включая атрибуты, применяется каноникализация *http://www.w3.org/2001/10/xml-exc-c14n#*, на основе результата рассчитывается электронная подпись по алгоритму ГОСТ Р 34.11-2001 и заносится в <ds:SignatureValue> в формате Base64.

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope .....>
  <soapenv:Header>
    <wsse:Security soapenv:actor="......">
      <wsse:BinarySecurityToken ......>....</wsse:BinarySecurityToken>
       <ds:Signature>

        <ds:SignedInfo>.........</ds:SignedInfo>
        <ds:SignatureValue>ooXepzAw89CBIsbZ+g2oNFh.....</ds:SignatureValue>
        <ds:KeyInfo>.........</ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="body">
    .......
  </soapenv:Body>
</soapenv:Envelope>
```

5.6. ПРИМЕР ЭЛЕКТРОННОГО СООБЩЕНИЯ, СОДЕРЖАЩЕГО ТЕХНОЛОГИЧЕСКУЮ ПОДПИСЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНА ВЛАСТИ (ЭП-ОВ)

```
<?xml version="1.0" encoding="UTF-8"?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:smev="http://smev.gosuslugi.ru/ rev120315" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
```

wssecurity-utility-1.0.xsd">

<soapenv:Header><wsse:Security soapenv:actor=*"http://smev.gosuslugi.ru/actors/smev"*
xmlns:wsse=*"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"*><wsse:BinarySecurityToken EncodingType=*"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"* ValueType=*"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"* wsu:Id=*"CertId-1E42AC2E0B920AAF70131180067340425"*
xmlns:wsse=*"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"*
xmlns:wsu=*"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"*>MIIDjjCCAz2gAwIBAgIKEUWKtwAAAAAB8DAIBgYqhQMCAgMweTEXMBUGCSqGSIb3DQEJARYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoMG9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEUMBIGA1UEAxMLUlRLIFRlc3QgQ0EwHhcNMTEwNjI5MDczNzAwWhcNMTIwNjI5MDc0NjAwWjCBsDEbMBkGA1UEAx4SBCEEHAQtBBIAXwRCBDUEQQRCMQswCQYDVQQGEwJSVTEUMBIGA1UEBRMLMDAwMDAwMDAwMDExFTATBgNVBAgeDAQcBD4EQQQ6BDIEMDEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMS8wLQYDVQQKHiYEFwQQBB4AIAQtBDkEIgQ4ACAEGgQ+BD0EQQQwBDsEQgQ4BD0EMzEPMA0GA1UECx4GBCQEHwQUMGMwHAYGKoUDAgITMBIGByqFAwICJAAGByqFAwICHgEDQwAEQHRrw+NLa824XuNToKiQmd+YyMBIwpnit92qGgcPxzkr1k3kQxFEnR7HZR+r+LnyLXPHPp+4ekzLWrIGSHXNO7OjggFrMIIBZzALBgNVHQ8EBAMCBPAwJgYDVR0lBB8wHQYHKoUDAgIiBgYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBRl7yDW3eEdZr1WsspuQ4XBSy3QXjAfBgNVHSMEGDAWgBTcU2nSYtDb9vBavYJPU8DE1fA/VzBmBgNVHR8EXzBdMFugWaBXhlVodHRwOi8vZDAwcGd1Y2VydDAxLjAwLmVnb3YubG9jYWwvcmEvY2RwL2RjNTM2OWQyNjJkMGRiZjZmMDVhYmQ4MjRmNTNjMGM0ZDVmMDNmNTcuY3JsMFQGCCsGAQUFBwEBBEgwRjBEBggrBgEFBQcwAoY4aHR0cDovL2QwMHBndWNlcnQwMS4wMC5lZ292LmxvY2FsL3JhL2NkcC90ZXN0X2NhX3J0ay5jcnQwMgYJKwYBBAGCNxUKBCUwIzAJBgcqhQMCAiIGMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMAgGBiqFAwICAwNBAI3CL2fgGPLlZ5Vm6BwAfqHxCRJkmtLmFX4sD9iZ4jvp6BGIF+XkeAvWnedowJ8UurEGNoDwtfXf+xeHPT11Cm4=</wsse:BinarySecurityToken><ds:Signature Id=*"Signature-10"*
xmlns:ds=*"http://www.w3.org/2000/09/xmldsig#"*>

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm=*"http://www.w3.org/2001/10/xml-exc-c14n#"*/>

<ds:SignatureMethod Algorithm=*"http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"*/>

<ds:Reference URI=*"#sampleRequest"*>

<ds:Transforms>

<ds:Transform Algorithm=*"http://www.w3.org/2001/10/xml-exc-c14n#"*/>

</ds:Transforms>

<ds:DigestMethod Algorithm=*"http://www.w3.org/2001/04/xmldsig-more#gostr3411"*/>

<ds:DigestValue>5gIY+iLbtYhCJWjSo6QIMWhSR+zKFse3H98dyaWWUEo=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

aTUt+Ok2vt9qjMlVQt+wK4nxRXP9W2MRY1ZQGZpBb1fKeAyr8BtA2LJzPQZdwp4H0SIQ3GHsqrDp

```
7wIwtGOlWg==

</ds:SignatureValue>

<ds:KeyInfo Id="KeyId-1E42AC2E0B920AAF70131180067340426">

<wsse:SecurityTokenReference wsu:Id="STRId-1E42AC2E0B920AAF70131180067340427"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><wsse:Reference
URI="#CertId-1E42AC2E0B920AAF70131180067340425" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"/></wsse:SecurityTokenReference>

</ds:KeyInfo>

</ds:Signature></wsse:Security>

</soapenv:Header>



<soapenv:Body wsu:Id="sampleRequest">

        <smevSampleMsg:sampleRequest xmlns:smevSampleMsg="http://smev.gosuslugi.ru/SampleMessage">



                <smev:Message>

                        <smev:Sender/>

                        <smev:Recipient/>

                        <smev:Originator/>

                        <smev:TypeCode/>

                        <smev:Status/>

                        <smev:Date/>

                        <smev:ServiceCode/>

                        <smev:CaseNumber/>

                        <smev:ExchangeType/>

                        <smev:RequestIdRef/>

                        <smev:OriginRequestIdRef/>

                        . . . . .

                </smev:Message>

                <smev:MessageData>
```

```
                        <smev:AppData/>



                        <smev:AppDocument/>

                    </smev:MessageData>

            </smevSampleMsg:sampleRequest>

</soapenv:Body>

</soapenv:Envelope>
```

5.7. ПРИМЕР ЭЛЕКТРОННОГО СООБЩЕНИЯ, СОДЕРЖАЩЕГО ТЕХНОЛОГИЧЕСКУЮ ПОДПИСЬ ПГУ (ЭП-ПГУ)

Пример электронного сообщения, содержащего технологическую подпись ПГУ аналогичен по принципам формирования электронной подписи ЭП-ОВ с тем отличием, что подписание проводит не информационная система органа власти, а ИС ПГУ.

5.8. ПРИМЕР ЭЛЕКТРОННОГО СООБЩЕНИЯ, СОДЕРЖАЩЕГО ТЕХНОЛОГИЧЕСКУЮ ПОДПИСЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ (ЭП-ОВ) И СМЭВ (ЭП-СМЭВ)

```
<?xml version="1.0" encoding="UTF-8"?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:smev="http://smev.gosuslugi.ru/ rev120315" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd">

<soapenv:Header><wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/recipient"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"><wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" wsu:Id="CertId-1E42AC2E0B920AAF70131180088502428"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">MIIDjjCCAz2gAwIBAgIKEUWKtwAAAAAB8DAIBgYqhQMCAgMweTEXMBUGCSqGSIb3DQEJA
RYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoM
G9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEUMBIGA1UEAxMLUlRLIFRlc3QgQ0EwHhcNMTEwNjI
5MDczNzAwWhcNMTIwNjI5MDc0NjAwWjCBsDEbMBkGA1UEAx4SBCEEHAQtBBIAXwRCBDUEQQRCM
QswCQYDVQQGEwJSVTEUMBIGA1UEBRMLMDAwMDAwMDAwMDExFTATBgNVBAgeDAQcBD4EQQ
Q6BDIEMDEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMS8wLQYDVQQKHiYEFwQQBB4AIAQtBDkEIg
Q4ACAEGgQ+BD0EQQQwBDsEQgQ4BD0EMzEPMA0GA1UECx4GBCQEHwQUMGMwHAYGKoUDAgIT
MBIGByqFAwICJAAGByqFAwICHgEDQwAEQHRrw+NLa824XuNToKiQmd+YyMBIwpnit92qGgcPxzkr1k3k
QxFEnR7HZR+r+LnyLXPHPp+4ekzLWrIGSHXNO7OjggFrMIIBZzALBgNVHQ8EBAMCBPAwJgYDVR0lBB8
wHQYHKoUDAgIiBgYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBRl7yDW3eEdZr1WsspuQ
4XBSy3QXjAfBgNVHSMEGDAWgBTcU2nSYtDb9vBavYJPU8DE1fA/VzBmBgNVHR8EXzBdMFugWaBXhl
VodHRwOi8vZDAwcGd1Y2VydDAxLjAwLmVnb3YubG9jYWwvcmEvY2RwL2RjNTM2OWQyNjJkMGRiZjZ
mMDVhYmQ4MjRmNTNjMGM0ZDVmMDNmNTcuY3JsMFQGCCsGAQUFBwEBBEgwRjBEBggrBgEFBQc
wAoY4aHR0cDovL2QwMHBndWNlcnQwMS4wMC5lZ292LmxvY2FsL3JhL2NkcC90ZXN0X2NhX3J0ay5jcnQ
wMgYJKwYBBAGCNxUKBCUwIzAJBgcqhQMCAiIGMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMA
```

```
gGBiqFAwICAwNBAI3CL2fgGPLlZ5Vm6BwAfqHxCRJkmtLmFX4sD9iZ4jvp6BGIF+XkeAvWnedowJ8UurEG
NoDwtfXf+xeHPT11Cm4=</wsse:BinarySecurityToken><ds:Signature Id="Signature-11"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

<ds:Reference URI="#sampleRequest">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>5gIY+iLbtYhCJWjSo6QIMWhSR+zKFse3H98dyaWWUEo=</ds:DigestValue>

</ds:Reference>

<ds:Reference URI="#smevHeader">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>aGkYwJuM4pOEbQowUa73Bpo925Rx01LRLzauaie8u9I=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

pZvLihbYXaniH9J2QPcIOVXNhpxxaC02X1bPXuKOpzM7AUAF8GaONor07UBqNt22bm9myWQnNJGq

z8/Po8kIAA==

</ds:SignatureValue>

<ds:KeyInfo Id="KeyId-1E42AC2E0B920AAF70131180088502429">

<wsse:SecurityTokenReference wsu:Id="STRId-1E42AC2E0B920AAF70131180088502430"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><wsse:Reference
URI="#CertId-1E42AC2E0B920AAF70131180088502428" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"/></wsse:SecurityTokenReference>
```

```
</ds:KeyInfo>

<ds:Object>

   <xds:QualifyingProperties  xmlns:xds="http://uri.etsi.org/01903/v1.1.1#">

      <xds:UnsignedProperties>

         <xds:UnsignedSignatureProperties>

            <xds:SignatureTimeStamp>

               <xds:HashDataInfo uri="#signature-value-40ddb6ca-9ac1-4026-a049-76901f3aa5d8"/>

               <xds:EncapsulatedTimeStamp>Метка времени в Base64</xds:EncapsulatedTimeStamp>

            </xds:SignatureTimeStamp>

         </xds:UnsignedSignatureProperties>

      </xds:UnsignedProperties>

   </xds:QualifyingProperties>

</ds:Object>

</ds:Signature></wsse:Security><wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/smev"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"><wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" wsu:Id="CertId-1E42AC2E0B920AAF70131180067340425"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">MIIDjjCCAz2gAwIBAgIKEUWKtwAAAAAB8DAIBgYqhQMCAgMweTEXMBUGCSqGSIb3DQEJA
RYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoM
G9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEUMBIGA1UEAxMLUlRLIFRlc3QgQ0EwHhcNMTEwNjI
5MDczNzAwWhcNMTIwNjI5MDc0NjAwWjCBsDEbMBkGA1UEAx4SBCEEHAQtBBIAXwRCBDUEQQRCM
QswCQYDVQQGEwJSVTEUMBIGA1UEBRMLMDAwMDAwMDAwMDExFTATBgNVBAgeDAQcBD4EQQ
Q6BDIEMDEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMS8wLQYDVQQKHiYEFwQQBB4AIAQtBDkEIg
Q4ACAEGgQ+BD0EQQQwBDsEQgQ4BD0EMzEPMA0GA1UECx4GBCQEHwQUMGMwHAYGKoUDAgIT
MBIGByqFAwICJAAGByqFAwICHgEDQwAEQHRrw+NLa824XuNToKiQmd+YyMBIwpnit92qGgcPxzkr1k3k
QxFEnR7HZR+r+LnyLXPHPp+4ekzLWrIGSHXNO7OjggFrMIIBZzALBgNVHQ8EBAMCBPAwJgYDVR0lBB8
wHQYHKoUDAgIiBgYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBRl7yDW3eEdZr1WsspuQ
4XBSy3QXjAfBgNVHSMEGDAWgBTcU2nSYtDb9vBavYJPU8DE1fA/VzBmBgNVHR8EXzBdMFugWaBXhl
VodHRwOi8vZDAwcGd1Y2VydDAxLjAwLmVnb3YubG9jYWwvcmEvY2RwL2RjNTM2OWQyNjJkMGRiZjZ
mMDVhYmQ4MjRmNTNjMGM0ZDVmMDNmNTcuY3JsMFQGCCsGAQUFBwEBBEgwRjBEBggrBgEFBQc
wAoY4aHR0cDovL2QwMHBndWNlcnQwMS4wMC5lZ292LmxvY2FsL3JhL2NkcC90ZXN0X2NhX3J0ay5jcnQ
wMgYJKwYBBAGCNxUKBCUwIzAJBgcqhQMCAiIGMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMA
gGBiqFAwICAwNBAI3CL2fgGPLlZ5Vm6BwAfqHxCRJkmtLmFX4sD9iZ4jvp6BGIF+XkeAvWnedowJ8UurEG
NoDwtfXf+xeHPT11Cm4=</wsse:BinarySecurityToken><ds:Signature Id="Signature-10"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

<ds:Reference URI="#sampleRequest">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>5gIY+iLbtYhCJWjSo6QIMWhSR+zKFse3H98dyaWWUEo=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

aTUt+Ok2vt9qjMlVQt+wK4nxRXP9W2MRY1ZQGZpBb1fKeAyr8BtA2LJzPQZdwp4H0SIQ3GHsqrDp

7wIwtGOlWg==

</ds:SignatureValue>

<ds:KeyInfo Id="KeyId-1E42AC2E0B920AAF70131180067340426">

<wsse:SecurityTokenReference wsu:Id="STRId-1E42AC2E0B920AAF70131180067340427"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><wsse:Reference
URI="#CertId-1E42AC2E0B920AAF70131180067340425" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"/></wsse:SecurityTokenReference>

</ds:KeyInfo>

</ds:Signature></wsse:Security>

        <smev:Header wsu:Id="smevHeader">

                <smev:NodeId>Уникальный идентификатор узла СМЭВ</smev:NodeId>

                <smev:MessageId>Уникальный код сообщения в СМЭВ</smev:MessageId>

                <smev:TimeStamp>Дата получения сообщения СМЭВ</smev:TimeStamp>

                <smev:MessageClass>Идентификатор класса сообщения</smev:MessageClass>

        </smev:Header>

</soapenv:Header>


<soapenv:Body wsu:Id="sampleRequest">
```

```
        <smevSampleMsg:sampleRequest xmlns:smevSampleMsg="http://smev.gosuslugi.ru/SampleMessage">


                <smev:Message>

                        <smev:Sender/>

                        <smev:Recipient/>

                        <smev:Originator/>

                        <smev:TypeCode/>

                        <smev:Status/>

                        <smev:Date/>

                        <smev:ServiceCode/>

                       <smev:CaseNumber/><smev:ExchangeType/>

                        <smev:RequestIdRef/>

                        <smev:OriginRequestIdRef/>

                       . . . . .

                </smev:Message>


                <smev:MessageData>


                        <smev:AppData/>


                        <smev:AppDocument/>

                </smev:MessageData>

        </smevSampleMsg:sampleRequest>

</soapenv:Body>

</soapenv:Envelope>
```

5.9. ПРИМЕР ЭЛЕКТРОННОГО СООБЩЕНИЯ, СОДЕРЖАЩЕГО ТЕХНОЛОГИЧЕСКУЮ ПОДПИСЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ (ЭП-ОВ) И НЕСКОЛЬКИХ УЗЛОВ СМЭВ (ЭП-СМЭВ/ЭП-РСМЭВ)

```
<?xml version="1.0" encoding="UTF-8"?><soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:smev="http://smev.gosuslugi.ru/ rev120315" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
```

200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

<soapenv:Header><wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/recipient" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"><wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="CertId-1E42AC2E0B920AAF70131180088502428" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">MIIDjjCCAz2gAwIBAgIKEUWKtwAAAAAB8DAIBgYqhQMCAgMweTEXMBUGCSqGSIb3DQEJARYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoMG9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEUMBIGA1UEAxMLUlRLIFRlc3QgQ0EwHhcNMTEwNjI5MDczNzAwWhcNMTIwNjI5MDc0NjAwWjCBsDEbMBkGA1UEAx4SBCEEHAQtBBIAXwRCBDUEQQRCMQswCQYDVQQGEwJSVTEUMBIGA1UEBRMLMDAwMDAwMDAwMDExFTATBgNVBAgeDAQcBD4EQQQ6BDIEMDEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMS8wLQYDVQQKHiYEFwQQBB4AIAQtBDkEIgQ4ACAEGgQ+BD0EQQQwBDsEQgQ4BD0EMzEPMA0GA1UECx4GBCQEHwQUMGMwHAYGKoUDAgITMBIGByqFAwICJAAGByqFAwICHgEDQwAEQHRrw+NLa824XuNToKiQmd+YyMBIwpnit92qGgcPxzkr1k3kQxFEnR7HZR+r+LnyLXPHPp+4ekzLWrIGSHXNO7OjggFrMIIBZzALBgNVHQ8EBAMCBPAwJgYDVR0lBB8wHQYHKoUDAgIiBgYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBRl7yDW3eEdZr1WsspuQ4XBSy3QXjAfBgNVHSMEGDAWgBTcU2nSYtDb9vBavYJPU8DE1fA/VzBmBgNVHR8EXzBdMFugWaBXhlVodHRwOi8vZDAwcGd1Y2VydDAxLjAwLmVnb3YubG9jYWwvcmEvY2RwL2RjNTM2OWQyNjJkMGRiZjZmMDVhYmQ4MjRmNTNjMGM0ZDVmMDNmNTcuY3JsMFQGCCsGAQUFBwEBBEgwRjBEBggrBgEFBQcwAoY4aHR0cDovL2QwMHBndWNlcnQwMS4wMC5lZ292LmxvY2FsL3JhL2NkcC90ZXN0X2NhX3J0ay5jcnQwMgYJKwYBBAGCNxUKBCUwIzAJBgcqhQMCAiIGMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMAgGBiqFAwICAwNBAI3CL2fgGPLlZ5Vm6BwAfqHxCRJkmtLmFX4sD9iZ4jvp6BGIF+XkeAvWnedowJ8UurEGNoDwtfXf+xeHPT11Cm4=</wsse:BinarySecurityToken><ds:Signature Id="Signature-11" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

<ds:Reference URI="#sampleRequest">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>5gIY+iLbtYhCJWjSo6QIMWhSR+zKFse3H98dyaWWUEo=</ds:DigestValue>

</ds:Reference>

<ds:Reference URI="#GUID2">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

```
</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>aGkYwJuM4pOEbQowUa73Bpo925Rx01LRLzauaie8u9I=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

pZvLihbYXaniH9J2QPcIOVXNhpxxaC02X1bPXuKOpzM7AUAF8GaONor07UBqNt22bm9myWQnNJGq

z8/Po8kIAA==

</ds:SignatureValue>

<ds:KeyInfo Id="KeyId-1E42AC2E0B920AAF70131180088502429">

<wsse:SecurityTokenReference wsu:Id="STRId-1E42AC2E0B920AAF70131180088502430"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><wsse:Reference URI="#CertId-1E42AC2E0B920AAF70131180088502428"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"/></wsse:SecurityTokenReference>

</ds:KeyInfo>

<ds:Object>

   <xds:QualifyingProperties  xmlns:xds="http://uri.etsi.org/01903/v1.1.1#">

      <xds:UnsignedProperties>

         <xds:UnsignedSignatureProperties>

            <xds:SignatureTimeStamp>

               <xds:HashDataInfo uri="#signature-value-40ddb6ca-9ac1-4026-a049-76901f3aa5d8"/>

               <xds:EncapsulatedTimeStamp>Метка времени в Base64</xds:EncapsulatedTimeStamp>

            </xds:SignatureTimeStamp>

         </xds:UnsignedSignatureProperties>

      </xds:UnsignedProperties>

   </xds:QualifyingProperties>

</ds:Object>

</ds:Signature></wsse:Security>

<wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/smev00" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"><wsse:BinarySecurityToken
```

EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" wsu:Id="CertId-1E42AC2E0B920AAF70131180088502428" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">MIIDjjCCAz2gAwIBAgIKEUWKtwAAAAAB8DAIBgYqhQMCAgMweTEXMBUGCSqGSIb3DQEJARYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoMG9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEUMBIGA1UEAxMLUlRLIFRlc3QgQ0EwHhcNMTEwNjI5MDczNzAwWhcNMTIwNjI5MDc0NjAwWjCBsDEbMBkGA1UEAx4SBCEEHAQtBBIAXwRCBDUEQQRCMQswCQYDVQQGEwJSVTEUMBIGA1UEBRMLMDAwMDAwMDAwMDExFTATBgNVBAgeDAQcBD4EQQQ6BDIEMDEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMS8wLQYDVQQKHiYEFwQQBB4AIAQtBDkEIgQ4ACAEGgQ+BD0EQQQwBDsEQgQ4BD0EMzEPMA0GA1UECx4GBCQEHwQUMGMwHAYGKoUDAgITMBIGByqFAwICJAAGByqFAwICHgEDQwAEQHRrw+NLa824XuNToKiQmd+YyMBIwpnit92qGgcPxzkr1k3kQxFEnR7HZR+r+LnyLXPHPp+4ekzLWrIGSHXNO7OjggFrMIIBZzALBgNVHQ8EBAMCBPAwJgYDVR0lBB8wHQYHKoUDAgIiBgYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBRl7yDW3eEdZr1WsspuQ4XBSy3QXjAfBgNVHSMEGDAWgBTcU2nSYtDb9vBavYJPU8DE1fA/VzBmBgNVHR8EXzBdMFugWaBXhlVodHRwOi8vZDAwcGd1Y2VydDAxLjAwLmVnb3YubG9jYWwvcmEvY2RwL2RjNTM2OWQyNjJkMGRiZjZmMDVhYmQ4MjRmNTNjMGM0ZDVmMDNmNTcuY3JsMFQGCCsGAQUFBwEBBEgwRjBEBggrBgEFBQcwAoY4aHR0cDovL2QwMHBndWNlcnQwMS4wMC5lZ292LmxvY2FsL3JhL2NkcC90ZXN0X2NhX3J0ay5jcnQwMgYJKwYBBAGCNxUKBCUwIzAJBgcqhQMCAiIGMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMAgGBiqFAwICAwNBAI3CL2fgGPLlZ5Vm6BwAfqHxCRJkmtLmFX4sD9iZ4jvp6BGIF+XkeAvWnedowJ8UurEGNoDwtfXf+xeHPT11Cm4=</wsse:BinarySecurityToken><ds:Signature Id="Signature-11" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

<ds:Reference URI="#sampleRequest">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>5gIY+iLbtYhCJWjSo6QIMWhSR+zKFse3H98dyaWWUEo=</ds:DigestValue>

</ds:Reference>

<ds:Reference URI="#GUID1">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>aGkYwJuM4pOEbQowUa73Bpo925Rx01LRLzauaie8u9I=</ds:DigestValue>

```
</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

pZvLihbYXaniH9J2QPcIOVXNhpxxaC02X1bPXuKOpzM7AUAF8GaONor07UBqNt22bm9myWQnNJGq

z8/Po8kIAA==

</ds:SignatureValue>

<ds:KeyInfo Id="KeyId-1E42AC2E0B920AAF70131180088502429">

<wsse:SecurityTokenReference wsu:Id="STRId-1E42AC2E0B920AAF70131180088502430"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><wsse:Reference URI="#CertId-1E42AC2E0B920AAF70131180088502428"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"/></wsse:SecurityTokenReference>

</ds:KeyInfo>

<ds:Object>

   <xds:QualifyingProperties  xmlns:xds="http://uri.etsi.org/01903/v1.1.1#">

      <xds:UnsignedProperties>

         <xds:UnsignedSignatureProperties>

            <xds:SignatureTimeStamp>

               <xds:HashDataInfo uri="..."/>

               <xds:EncapsulatedTimeStamp>Метка времени в Base64</xds:EncapsulatedTimeStamp>

            </xds:SignatureTimeStamp>

         </xds:UnsignedSignatureProperties>

      </xds:UnsignedProperties>

   </xds:QualifyingProperties>

</ds:Object>

</ds:Signature></wsse:Security><wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/smev"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"><wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
x509-token-profile-1.0#X509v3" wsu:Id="CertId-1E42AC2E0B920AAF70131180067340425"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">MIIDjjCCAz2gAwIBAgIKEUWKtwAAAAAB8DAIBgYqhQMCAgMweTEXMBUGCSqGSIb3DQEJA
RYIY2FAcnQucnUxCzAJBgNVBAYTAlJVMRUwEwYDVQQHDAzQnNC+0YHQutCy0LAxJDAiBgNVBAoM
```

G9Ce0JDQniDQoNC+0YHRgtC10LvQtdC60L7QvDEUMBIGA1UEAxMLUlRLIFRlc3QgQ0EwHhcNMTEwNjI
5MDczNzAwWhcNMTIwNjI5MDc0NjAwWjCBsDEbMBkGA1UEAx4SBCEEHAQtBBIAXwRCBDUEQQRCM
QswCQYDVQQGEwJSVTEUMBIGA1UEBRMLMDAwMDAwMDAwMDExFTATBgNVBAgeDAQcBD4EQQ
Q6BDIEMDEVMBMGA1UEBx4MBBwEPgRBBDoEMgQwMS8wLQYDVQQKHiYEFwQQBB4AIAQtBDkEIg
Q4ACAEGgQ+BD0EQQQwBDsEQgQ4BD0EMzEPMA0GA1UECx4GBCQEHwQUMGMwHAYGKoUDAgIT
MBIGByqFAwICJAAGByqFAwICHgEDQwAEQHRrw+NLa824XuNToKiQmd+YyMBIwpnit92qGgcPxzkr1k3k
QxFEnR7HZR+r+LnyLXPHPp+4ekzLWrIGSHXNO7OjggFrMIIBZzALBgNVHQ8EBAMCBPAwJgYDVR0lBB8
wHQYHKoUDAgIiBgYIKwYBBQUHAwIGCCsGAQUFBwMEMB0GA1UdDgQWBBRl7yDW3eEdZr1WsspuQ
4XBSy3QXjAfBgNVHSMEGDAWgBTcU2nSYtDb9vBavYJPU8DE1fA/VzBmBgNVHR8EXzBdMFugWaBXhl
VodHRwOi8vZDAwcGd1Y2VydDAxLjAwLmVnb3YubG9jYWwvcmEvY2RwL2RjNTM2OWQyNjJkMGRiZjZ
mMDVhYmQ4MjRmNTNjMGM0ZDVmMDNmNTcuY3JsMFQGCCsGAQUFBwEBBEgwRjBEBggrBgEFBQc
wAoY4aHR0cDovL2QwMHBndWNlcnQwMS4wMC5lZ292LmxvY2FsL3JhL2NkcC90ZXN0X2NhX3J0ay5jcnQ
wMgYJKwYBBAGCNxUKBCUwIzAJBgcqhQMCAiIGMAoGCCsGAQUFBwMCMAoGCCsGAQUFBwMEMA
gGBiqFAwICAwNBAI3CL2fgGPLlZ5Vm6BwAfqHxCRJkmtLmFX4sD9iZ4jvp6BGIF+XkeAvWnedowJ8UurEG
NoDwtfXf+xeHPT11Cm4=</wsse:BinarySecurityToken><ds:Signature Id="Signature-10"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>

<ds:Reference URI="#sampleRequest">

<ds:Transforms>

<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>

<ds:DigestValue>5gIY+iLbtYhCJWjSo6QIMWhSR+zKFse3H98dyaWWUEo=</ds:DigestValue>

</ds:Reference>

</ds:SignedInfo>

<ds:SignatureValue>

aTUt+Ok2vt9qjMlVQt+wK4nxRXP9W2MRY1ZQGZpBb1fKeAyr8BtA2LJzPQZdwp4H0SIQ3GHsqrDp

7wIwtGOlWg==

</ds:SignatureValue>

<ds:KeyInfo Id="KeyId-1E42AC2E0B920AAF70131180067340426">

<wsse:SecurityTokenReference wsu:Id="STRId-1E42AC2E0B920AAF70131180067340427"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><wsse:Reference URI="#CertId-1E42AC2E0B920AAF70131180067340425"
ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-

```
1.0.xsd"/></wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature></wsse:Security>
        <smev:Header wsu:Id="GUID2" actor="http://smev.gosuslugi.ru/actors/recipient">
                <smev:NodeId>Уникальный идентификатор узла СМЭВ</smev:NodeId>
                <smev:MessageId>Уникальный код сообщения в СМЭВ</smev:MessageId>
                <smev:TimeStamp>Дата получения сообщения СМЭВ</smev:TimeStamp>
                <smev:MessageClass>Идентификатор класса сообщения</smev:MessageClass>
        </smev:Header>
        <smev:Header wsu:Id="GUID1" actor="http://smev.gosuslugi.ru/actors/smev00">
                <smev:NodeId>Уникальный идентификатор узла СМЭВ</smev:NodeId>
                <smev:MessageId>Уникальный код сообщения в СМЭВ</smev:MessageId>
                <smev:TimeStamp>Дата получения сообщения СМЭВ</smev:TimeStamp>
                <smev:MessageClass>Идентификатор класса сообщения</smev:MessageClass>
        </smev:Header>

</soapenv:Header>

<soapenv:Body wsu:Id="sampleRequest">
        <smevSampleMsg:sampleRequest xmlns:smevSampleMsg="http://smev.gosuslugi.ru/SampleMessage">

                <smev:Message>
                        <smev:Sender/>
                        <smev:Recipient/>
                        <smev:Originator/>
                        <smev:TypeCode/>
                        <smev:Status/>
                        <smev:Date/>
        <smev:ServiceCode/>
```

```
        <smev:CaseNumber/>
                        <smev:ExchangeType/>
                        <smev:RequestIdRef/>
                        <smev:OriginRequestIdRef/>
        . . . . .
                    </smev:Message>

                    <smev:MessageData>

                        <smev:AppData/>

                        <smev:AppDocument/>
                    </smev:MessageData>
          </smevSampleMsg:sampleRequest>
</soapenv:Body>
</soapenv:Envelope>
```

6. РЕЖИМЫ ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ЧЕРЕЗ СМЭВ

При информационном обмене ИС через СМЭВ можно выделить два режима взаимодействия: синхронный и асинхронный.

6.1. МОДЕЛЬ СИНХРОННОГО ВЗАИМОДЕЙСТВИЯ

Синхронное взаимодействие возникает в случаях, когда в ответ на запрос информационной системы потребителя информационная система поставщика посылает электронное сообщение с терминальным статусом и содержащее результат, являющийся целью исходного запроса потребителя, в течение короткого периода времени. Синхронное взаимодействие характерно для тех случаев, когда ответ на стороне потребителя формируется автоматически без необходимости участия в операциях субъекта взаимодействия - физического лица.

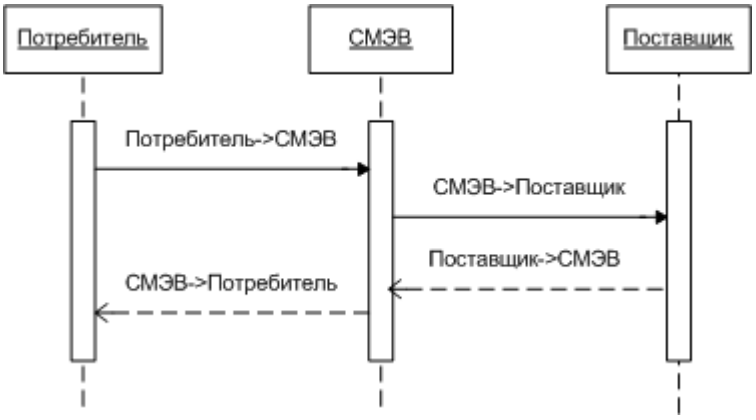


Рисунок 6 - Модель синхронного информационного обмена

6.2. МОДЕЛИ АСИНХРОННОГО ВЗАИМОДЕЙСТВИЯ

Асинхронное взаимодействие возникает в случаях, когда обработка запроса на стороне информационной системы поставщика требует больше времени, чем период ожидания ответа со стороны СМЭВ и информационной системы потребителя. В таком случае асинхронное взаимодействие реализуется через два синхронных вызова электронных сервисов, осуществляемых через СМЭВ.

Рекомендуемым является применение двух моделей асинхронного взаимодействия с участием СМЭВ:

- Модель асинхронного взаимодействия с повторным опросом (для межведомственных запросов);
- Модель асинхронного взаимодействия с обратным вызовом (для подачи заявлений с ЕПГУ).

6.3. МОДЕЛЬ АСИНХРОННОГО ВЗАИМОДЕЙСТВИЯ С ПОВТОРНЫМ ОПРОСОМ

Рекомендуемая модель ***асинхронного взаимодействия с повторным опросом*** заключается в разработке на стороне поставщика электронного сервиса, реализующего функции приема заявлений на обработку запросов и возврата статусов и результатов обработки в асинхронном режиме. При этом различные функции реализуются в виде операций (методов) единого электронного сервиса.

Допустимой является модификация модели, при которой на стороне поставщика реализуются два раздельных электронных сервиса: один для приема заявлений и другой для возврата статусов и результатов.

Функция приема заявления должна быть реализована на стороне поставщика и предусматривать синхронный возврат ответа-квитанции потребителю, свидетельствующей о приеме в обработку заявления.

В случае, когда при приеме заявления информационная система поставщика синхронно может сформировать мотивированный отказ в обработке, или возникновении каких-либо ошибок, препятствующих обработке запроса, асинхронное взаимодействие прекращается до отправки повторного запроса со стороны потребителя.

Для предоставления сведений о статусе обработки запроса или его результатов поставщик должен реализовать функцию соответствующую единую функцию для всех потребителей на стороне своей информационной системы.

Потребитель для получения статусов и/или результатов должен реализовать в своей информационной системе функцию периодического вызова сервиса возврата статусов и результатов на стороне информационной системы поставщика.

Периодичность вызова информационной системы поставщика со стороны потребителя регулируется договоренностями между потребителем и поставщиком. Регламентированная периодичность вызова информационной системы поставщика со стороны различных потребителей, указывается в паспорте электронного сервиса поставщика.

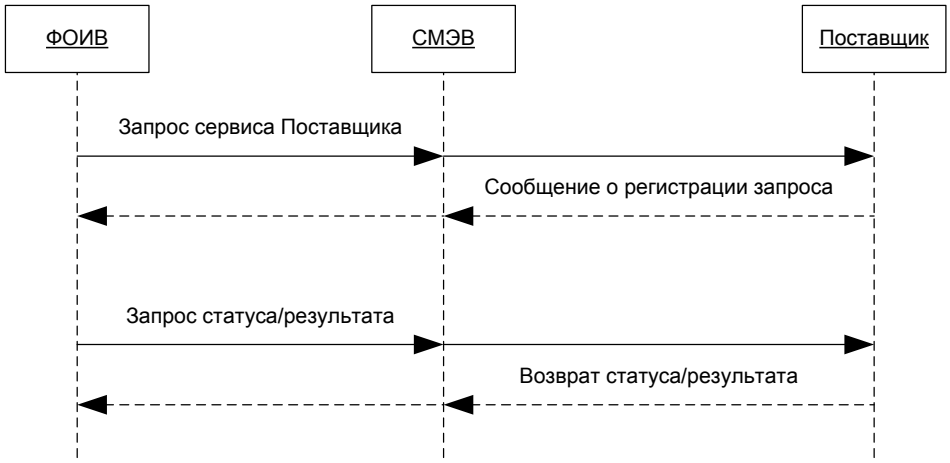


Рисунок 7 - Модель асинхронного информационного обмена при межведомственном взаимодействии

Наиболее часто ***модель асинхронного взаимодействия с повторным опросом*** рекомендована к применению для межведомственного взаимодействия органов власти с использованием СМЭВ.

6.4. МОДЕЛЬ АСИНХРОННОГО ВЗАИМОДЕЙСТВИЯ С ОБРАТНЫМ ВЫЗОВОМ

Рекомендуемая модель ***асинхронного взаимодействия с обратным вызовом*** заключается в разработке на стороне поставщика электронного сервиса, реализующего функции приема заявлений на обработку запросов. Электронный сервис для приема статусов и результатов реализуется на стороне инициатора взаимодействия.

Модель асинхронного взаимодействия с повторным опросом должна применяться для процессов обмена сообщений между ЕПГУ и участниками, ответственными за оказание государственных услуг в электронном виде.

Функция приема заявления должна быть реализована на стороне поставщика, ответственного за оказание услуги в электронном виде, и предусматривать синхронный возврат ответа-квитанции потребителю (ЕПГУ), свидетельствующей о приеме в обработку заявления.

В случае, когда при приеме заявления информационная система поставщика синхронно может сформировать мотивированный отказ в обработке, или возникновении каких-либо ошибок, препятствующих обработке запроса, асинхронное взаимодействие прекращается до отправки повторного запроса со стороны потребителя (ЕПГУ).

По результатам обработки запроса информационная система поставщика, ответственного за оказание услуг в электронном виде, вызывает электронный сервис приема статусов и результатов, реализованный на стороне потребителя (ЕПГУ).

В случае возникновения сбоев на стороне потребителя (ЕПГУ) при приеме результатов и статусов, информационная система поставщика, ответственного за оказание услуг в электронном виде, осуществляет повторную доставку этих сведений посредством вызова электронного сервиса приема статусов и результатов.

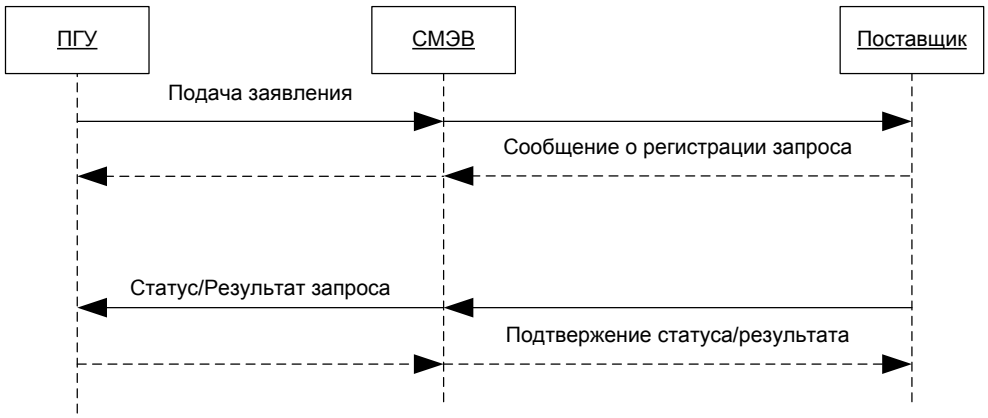


Рисунок 8 - Модель асинхронного информационного обмена при межведомственном взаимодействии

6.5. МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ С ПЕРЕДАЧЕЙ ПАКЕТОВ СООБЩЕНИЙ

Межведомственный обмен с использованием пакетов сообщений означает передачу нескольких прикладных сообщений в одном электронном сообщении СМЭВ.

Обмен с использованием пакетов сообщений может использоваться в следующих случаях:

- связанные сообщения - участнику взаимодействия необходимо передать другому участнику несколько связанных друг с другом сообщений, при этом сообщения не имеют смысла друг без друга;
- детерминированный порядок сообщений - участникам взаимодействия очень важно соблюсти порядок сообщений, и в ИС участников взаимодействий нет возможности организовать буферизацию сообщений;
- оптимизация обмена - участникам взаимодействия необходимо обменяться большим количеством маленьких сообщений (отношение длины прикладных данных сообщения к длине заголовка меньше единицы).

В других случаях целесообразна отправка самостоятельных сообщений без объединения в пакеты. Пакетный режим функционирования сервиса может быть выбран на усмотрение поставщика в случае наличия соответствующего корректно задокументированного описания интерфейсов в руководстве пользователя.

Схемы обмена пакетными сообщениями при синхронном взаимодействии приведены на рис. 9.

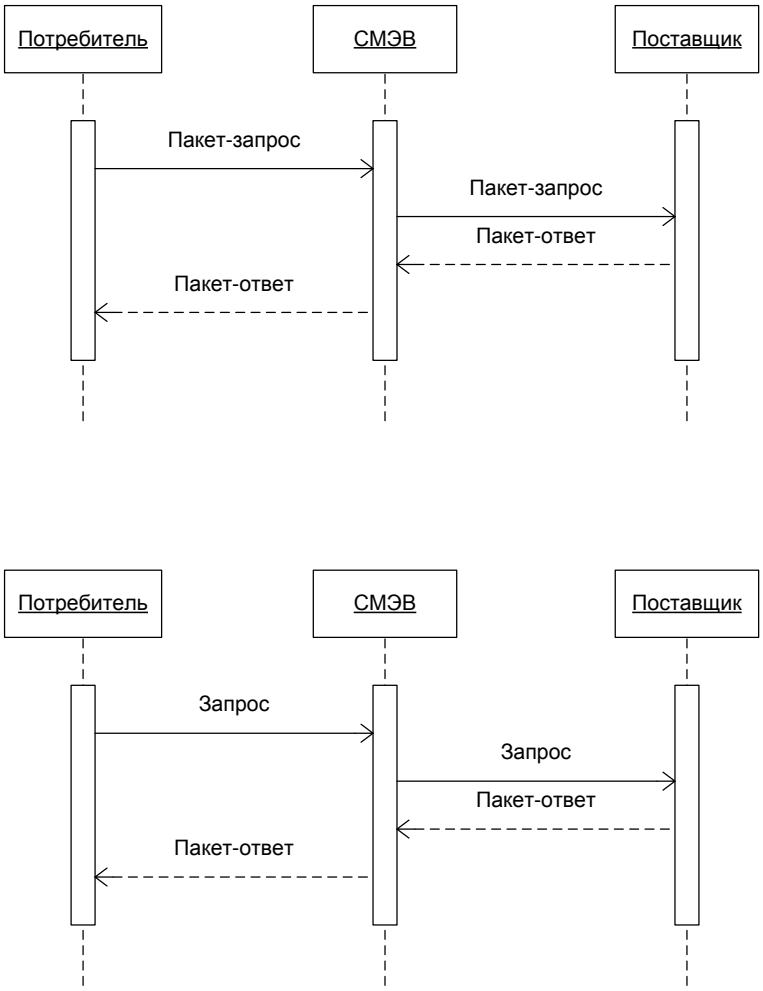


Рисунок 9 - Модель синхронного взаимодействия с использованием пакетов

При асинхронном взаимодействии сценарии взаимодействия аналогичны, с тем отличием, что пакет-ответ будет возвращаться в рамках другой сессии синхронного взаимодействия.

Допускается при ответе в асинхронном режиме выделять отдельные сообщения, перегруппировывать сообщения в несколько пакетов, передавать сообщения другим участникам обмена с указанием значений элементов smev:Originator, smev:OriginRequestIdRef и smev:RequestIdRef исходных сообщений. То есть, после того, как пакет принят и по нему отправлен ответ, свидетельствующий о приеме запроса в обработку, отдельные запросы внутри пакета далее могут обрабатываться индивидуально.

При обмене пакетами сообщений СМЭВ накладывает следующие ограничения:

- поставщик, отправитель и инициатор цепочки сообщений - единые для всего пакета;
- принимающий сервис поставщика - единый для всего пакета сообщений;

- данные о вызываемом сервисе - единые на весь пакет сообщений;
- класс сообщения - единый для всего пакета;
- тип сообщения - единый для всего пакета;
- категория взаимодействия - единая для всего пакета;
- признак тестового взаимодействия - единый для всего пакета;
- все сообщения в пакете доставляются (или не доставляются) одновременно (при асинхронном взаимодействии целевая ИС принимает и подтверждает квитанцией сразу весь пакет).

  При этом дальнейшая обработка и отправка ответа в асинхронном режиме по каждому сообщению может производиться индивидуально или с объединением в группы сообщений. Для каждого сообщения в пакете может проставляться индивидуальный статус, характеризующий взаимомодействие по конкретному запросу.

Размер пакета сообщений не должен превышать размера, допустимого для электронного сообщения СМЭВ.

Присвоение идентификаторов сообщений

Присвоение идентификатора пакету сообщений выполняется СМЭВ-ом в обычном режиме.

Присвоение идентификаторов сообщениям в пакете выполняется СМЭВ-ом на основе номеров отдельных сообщений в пакете, присвоенных отправляющей стороной. Отправитель сообщения обязан проставлять уникальные номера сообщений внутри пакета.

СМЭВ для входящих сообщений контролирует наличие уникальных номеров сообщений внутри пакета в поле *smev:SubRequestNumber*. Номера сообщений внутри пакета - числа, начиная с 1. Возрастающий порядок номеров также определяет последовательность сообщений в пакете.

СМЭВ присваивает уникальный идентификатор каждому сообщению, и в заголовке сообщения *smev:Header* устанавливает соответствие присвоенных идентификаторов сообщений в пакете и номеров, присвоенных пользователями. Таким образом, для пакетов сообщений применяется особый формат унифицированного служебного заголовка электронных сообщений СМЭВ.

Данное соответствие устанавливается в дополнительном элементе внутри *smev:Header*. Требования к формированию унифицированного служебного заголовка для пакетного режима обмена описываются в разделе «Унифицированные служебные заголовки федерального и региональных узлов».

Классификатор "Мнемоники статусов сообщений" расширяется новым значением:

- PACKET - означает, что статусы сообщений устанавливаются индивидуально для каждого сообщения в пакете. Данное значение используется, как для сообщений-запросов так и для сообщений-ответов.

Статус сообщения в заголовке выставляется в значение PACKET, а индивидуальные статусы сообщений указываются в детализации сообщений.

Для пакетного режима взаимодействия элемент smev:Message расширяется дополнительным необязательным полем smev:SubMessages. Правила заполнения данного элемента представлены в разделе «Унифицированные служебные заголовки федерального и регионального узлов СМЭВ».

К содержимому тегов AppData и AppDocument специальных требований при передаче пакетов не предъявляется, чтобы не инициировать дополнительные доработки в ИС участников.

Поставщики при разработке протокола взаимодействия могут произвольным образом определять правила формирования ссылок на номера сообщений внутри тега <smev:SubMessages> для привязки к параметрам сообщений.

7. ПРАВИЛА ЗАПОЛНЕНИЯ СЛУЖЕБНЫХ ЭЛЕМЕНТОВ ЭЛЕКТРОННЫХ СООБЩЕНИЙ В СМЭВ

Унифицированный служебный блок атрибутов сообщения играет ключевую роль в сборе статистики прохождения электронных запросов через СМЭВ и формировании целостных отчетов о межведомственном обмене.

7.1. ПРАВИЛА ЗАПОЛНЕНИЯ ЭЛЕМЕНТОВ ДЛЯ ИДЕНТИФИКАЦИИ СУБЪЕКТОВ МЕЖВЕДОМСТВЕННОГО ВЗАИМОДЕЙСТВИЯ

Элементы smev:Sender, smev:Recipient и smev:Originator используются для передачи сведений о субъектах межведомственного взаимодействия. Для каждого субъекта взаимодействия достаточно передачи его наименования и кода (мнемоники) точки подключения информационной системы.

В случае цепочки обменов между участниками, в структуре smev:Originator всегда указываются сведения о субъекте, инициировавшем цепочку, а не потребителя, отправившего последнее сообщение поставщику.

Участники должны корректно заполнять сведения об инициаторе цепочки сообщений при различных сценариях взаимодействия. Инициатором взаимодействия в рамках оказания государственной услуги в электронном виде выступает ЕПГУ, а в рамках исполнения государственной функции – один из органов исполнительной власти.

Каждый из этих элементов содержит дочерние элементы, описанные ниже:

Код (мнемоника) точки подключения ИС	smev:Code	Код информационной системы по унифицированному справочнику мнемоник точек подключения информационных систем.
Наименование участника	smev:Name	Текстовое наименование участника межведомственного обмена, являющегося владельцем информационной системы.

Правила кодификации мнемоник точек подключения информационных систем представлены в разделе 7.7.7.

Для каждой информационной системы требуется использование отдельных сертификатов электронной подписи в независимости от количества точек подключения.

Мнемоника точки подключения предоставляется участнику взаимодействия в процессе регистрации информационной системы.

7.2. ПРАВИЛА ЗАПОЛНЕНИЯ ЭЛЕМЕНТОВ ДЛЯ ВЗАИМОСВЯЗИ ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Корректное заполнение элементов smev:OriginRequestIdRef и smev:RequestIdRef, применяемых для взаимосвязи различных электронных сообщений в рамках одного процесса, является основополагающим для формирования целостных отчетов об истории взаимодействий через СМЭВ в рамках одного процесса.

При обработке электронного сообщения, для которого корректно осуществляются проверки в подсистеме регламентации доступа СМЭВ осуществляется добавление перед отправкой поставщику универсального служебного заголовка СМЭВ, содержащего метку времени (smev:TimeStamp), а также идентификатор сообщения (smev:MessageId).

Идентификатор сообщения всегда является GUID унифицированной структуры (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx).

Для связи различных электронных сообщений между собой участники взаимодействия должны сохранять идентификаторы сообщений в СМЭВ, и использовать их в качестве корреляционных для отражения взаимосвязи сообщений в рамках процесса информационного обмена.

Правила заполнения элементов smev:OriginRequestIdRef и smev:RequestIdRef описываются ниже для различных сценариев взаимодействия.

7.2.1. Синхронный режим взаимодействия

Синхронный режим взаимодействия описан в разделе 6 данного документа.

При заполнении служебных элементов smev:OriginRequestIdRef и smev:RequestIdRef отправляющая сторона (потребитель) должна выполнять следующие последовательности операций:

1. Потребитель отправляет через СМЭВ запрос к Поставщику.

   В связи с тем, что на этом этапе потребитель не знает идентификатор сообщения в СМЭВ, то унифицированный служебный блок атрибутов запроса не должен содержать элементы smev:OriginRequestIdRef и smev:RequestIdRef.

2. СМЭВ, получив запрос и убедившись в корректности значений подписи и валидности сертификата ключа ЭП отправителя, устанавливает свою подпись и добавляет в заголовок электронного сообщения (в soap:Header) универсальный служебный заголовок, содержащий элемент smev:MessageId, содержащий идентификатор сообщения в СМЭВ.

   Далее СМЭВ передает сообщение Поставщику.

3. Поставщик производит обработку сообщения-запроса и подготовку сообщения-ответа.

   При этом поставщик указывает значение элемента smev:MessageId электронного сообщения-запроса в smev:OriginRequestIdRef и smev:RequestIdRef электронного сообщения-ответа.

4. СМЭВ осуществляет проверку подписи поставщика в электронном сообщении-ответе, после чего добавляет в него универсальный служебный заголовок СМЭВ, содержащий элемент smev:MessageId с идентификатором сообщения-ответа.

5. Потребитель сохраняет у себя номер электронного сообщения-запроса и электронного сообщения-ответа: номер сообщения-запроса из элемента smev:RequestIdRef и номер сообщения-ответа из элемента smev:MessageId.

   Сохранение значений smev:RequestIdRef и smev:OriginRequestIdRef на стороне потребителя необходимо для возможности разбора конфликтных ситуаций с использованием номера сообщения СМЭВ.

Таким образом, потребитель:

- При синхронном взаимодействии не должен заполнять элементы smev:OriginRequestIdRef и smev:RequestIdRef в своих запросах;
- Должен сохранять номера сообщений СМЭВ сообщения-запроса и сообщения-ответа на основании сведений из ответа от поставщика в рамках сессии взаимодействия.

Таким образом, поставщик:

- При синхронном взаимодействии должен записать в элемент smev:RequestIdRef и smev:OriginRequestIdRef ответа значение элемента smev:MessageId сообщения-запроса;
- Должен сохранить на своей стороне номер сообщения запроса к нему;
- Не может сохранить номер сообщения ответа от себя, этот номер будет известен только потребителю, которому будет доставлен ответ через СМЭВ.

Примерная диаграмма заполнения служебных элементов для синхронного взаимодействия представлена на рисунке ниже:

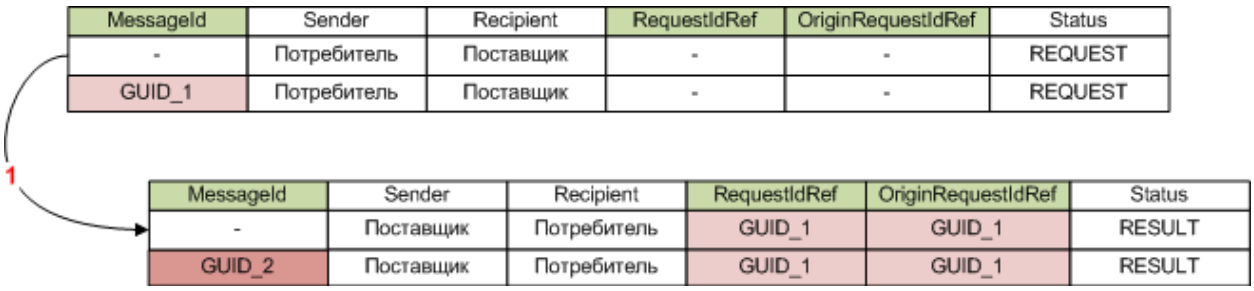


Рисунок 10 - Заполнение служебных элементов при синхронном взаимодействии

Первый блок отражает заполнение полей при формировании электронного сообщения на стороне Потребителя и обработке сообщения при прохождении через СМЭВ.

Второй блок отражает заполнение полей при формировании ответа на стороне Поставщика и обработке сообщения при его прохождении через СМЭВ.

7.2.2. Асинхронный режим взаимодействия

Под асинхронным взаимодействием подразумевается многоэтапный (более чем одна пара запрос-ответ) обмен электронными сообщениями через СМЭВ.

1. Потребитель отправляет через СМЭВ запрос к Поставщику.

Унифицированный служебный блок атрибутов запроса не должен содержать элементы smev:OriginRequestIdRef и smev:RequestIdRef.

2. СМЭВ, получив запрос и убедившись в валидности подписи, устанавливает свою подпись и добавляет в сообщение (в soapenv:Header) универсальный служебный заголовок, содержащий элемент smev:MessageId сообщения запроса.

Далее СМЭВ передает сообщение Поставщику.

3. Поставщик записывает значение элемента smev:MessageId первого запроса в элементы smev:RequestIdRef и smev:OriginRequestIdRef.

Далее поставщик передает сообщение-квитанцию, свидетельствующее о начале асинхронной обработки, в СМЭВ. Формат сообщения-квитанции определяется в соответствии с требованиями поставщика сервиса.

4. СМЭВ, получив ответ-квитанцию и убедившись в валидности подписи, устанавливает свою подпись и добавляет в сообщение (в soapenv:Header) универсальный служебный заголовок, содержащий элемент smev:MessageId (идентификатор сообщения-квитанции).

Далее СМЭВ отправляет сообщение-квитанцию Потребителю.

5. Потребитель получает ответ в виде сообщения-квитанции.

Через определенное регламентом взаимодействия время потребитель осуществляет запрос на получение статуса/результата (или повторные запросы) через СМЭВ к сервису поставщика.

При отправлении запроса на получение статуса/результата потребитель должен указать значение элемента smev:OriginRequestIdRef, соответствующее номеру запроса, инициировавшему цепочку асинхронного взаимодействия (смотри шаг 2).

При отправлении запроса на получение статуса/результата потребитель должен указать значение элемента smev:RequestIdRef, соответствующее номеру последнего ответа сервиса поставщика - предыдущего сообщения цепочки, составляющей асинхронное взаимодействие (смотри шаг 2).

В случае если асинхронное взаимодействие предусматривает обмен более, чем между двумя участниками, то потребитель должен сохранять неизменный smev:OriginRequestIdRef, но при заполнении smev:RequestIdRef – указывать номер последнего ответного сообщения поставщика в рамках данного асинхронного взаимодействия (например, содержащего квиток).

Примерная диаграмма заполнения служебных элементов для асинхронного взаимодействия, реализуемого в виде нескольких синхронных вызовов, представлена на рисунке ниже:

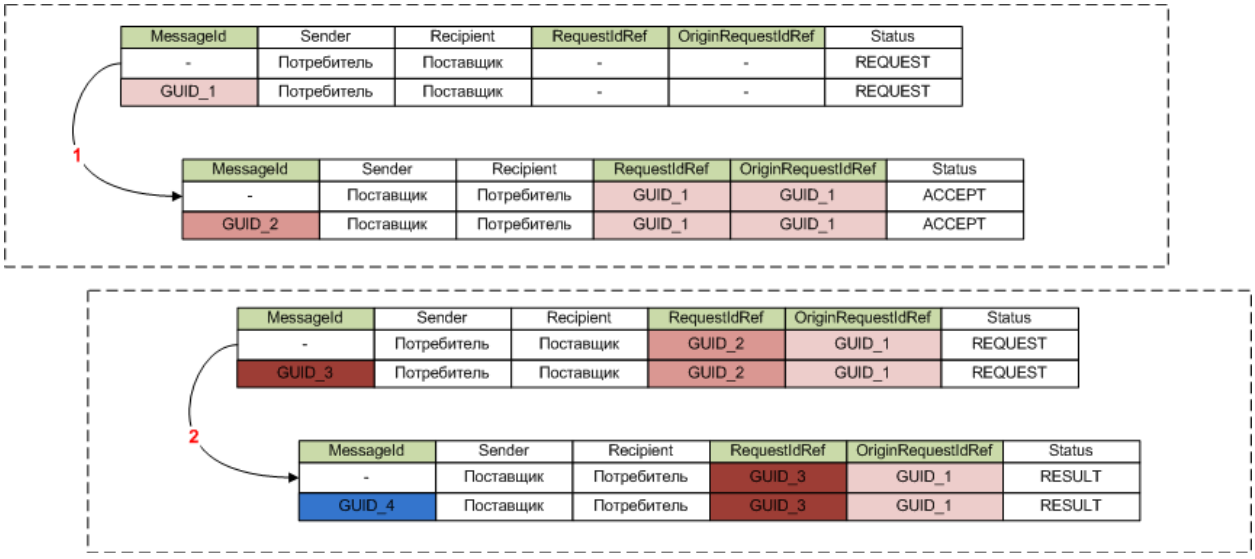


Рисунок 11 - Заполнение служебных элементов при асинхронном взаимодействии (межведомственное взаимодействие)

1 - первый запрос к Поставщику в рамках асинхронного взаимодействия (подача заявления). Поставщик его принимает, отвечая сообщением со статусом ACCEPT

2 - второй запрос к Поставщику для получения результата. Поставщик передает результат - отвечает сообщением со статусом RESULT.

При асинхронном взаимодействии с ЕПГУ реализуется схема, при которой Поставщик возвращает результат Потребителю самостоятельно:

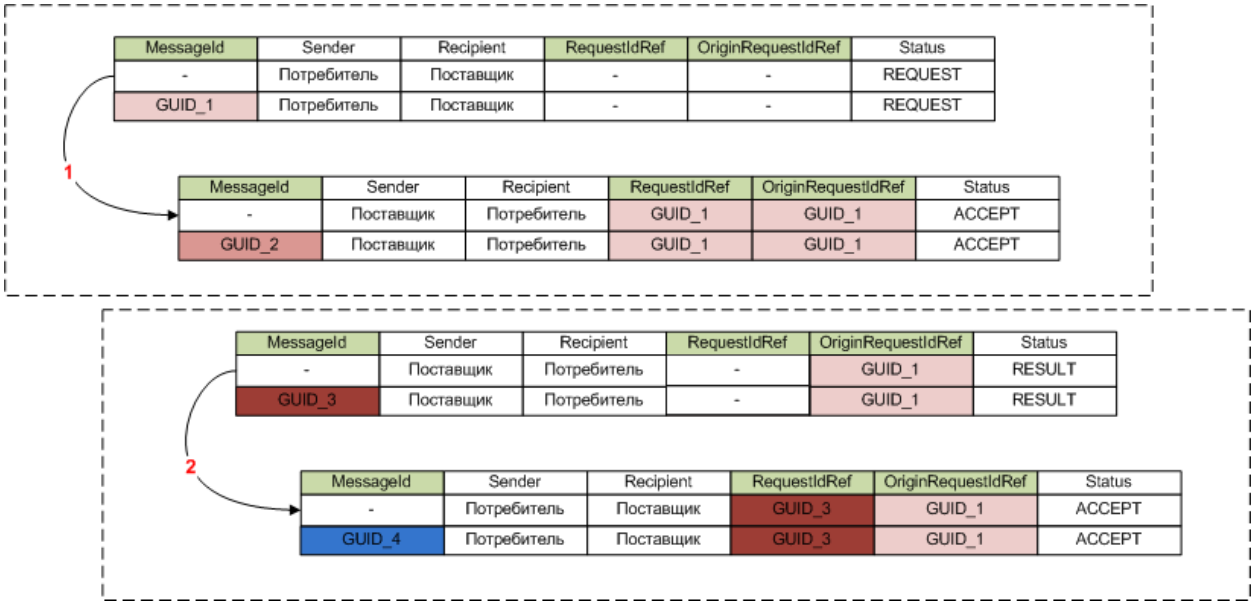


Рисунок 12 - Заполнение служебных элементов при асинхронном взаимодействии (подача заявлений с ЕПГУ)

1 - первый запрос к Поставщику в рамках асинхронного взаимодействия (подача заявления). Поставщик его принимает, отвечая сообщением со статусом ACCEPT.

2 - Поставщик возвращает Потребителю результат (сообщение со статусом RESULT). Потребитель принимает результат - отвечает сообщением со статусом ACCEPT.

7.3. ПРАВИЛА ЗАПОЛНЕНИЯ ЭЛЕМЕНТА ДЛЯ ПРИКЛАДНЫХ СТАТУСОВ СООБЩЕНИЙ

Элемент smev:Status предназначен для передачи прикладного статуса сообщения, который характеризует операцию, относящуюся к информационному обмену между Потребителем и Поставщиком.

Использование статусов при обмене сообщениями между Потребителем и Поставщиком представлено на рисунке ниже:

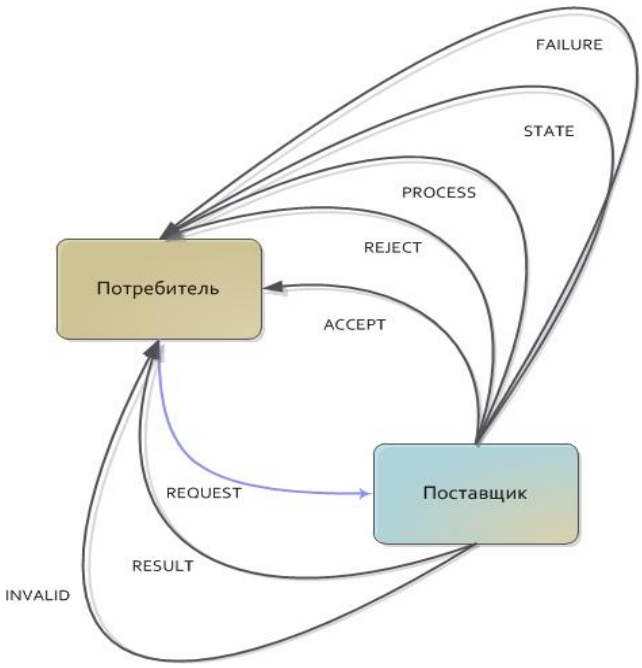


Рисунок 13 - Использование статусов электронных сообщений

7.3.1. Синхронное взаимодействие

При инициации нового запроса на оказание государственной услуги или запроса от одного ОИВ к другому в рамках оказания государственной услуги или выполнения государственной функции используется значение статуса REQUEST.

При синхронном ответе на такой запрос (при возможности сразу выполнить запрос в автоматическом режиме) ОИВ отвечает сообщением с выставлением статуса RESULT.

Если запрос не проходит ФЛК или проверку ЭП, то в ответе проставляется статус INVALID.

Если один ОИВ отправляет другому ОИВ или ПГУ мотивированный отказ, то в ответе проставляется статус REJECT.

Если ОИВ или ПГУ не может принять сообщение (например, находится в профилактическом режиме), то он отвечает статусом FAILURE. Данный статус не проставляется в случае критического сбоя на стороне ИС поставщика, но может применяться в случае, если эксплуатация системы допускает регламентированные прерывания сервиса.

7.3.2. Асинхронное взаимодействие

В случае если участник после обработки запроса должен в асинхронном режиме возвратить ответ на запрос другого ОИВ, он посылает сообщение со статусом RESULT, получатель сообщения подтверждает прием ответным сообщением со статусом ACCEPT. Подобная схема применяется при модели обмена с ЕПГУ.

При запросе от одного ОИВ к другому и асинхронном исполнении запроса, ОИВ потребитель может периодически запрашивать состояние исполнения запроса сообщением со статусом PING.

Если запрос на стороне поставщика еще находится в обработке, Поставщик отвечает сообщением со статусом PROCESS, если запрос выполнен – со статусами RESULT, REJECT или INVALID.

Использование статусов REJECT и INVALID аналогично синхронному взаимодействию.

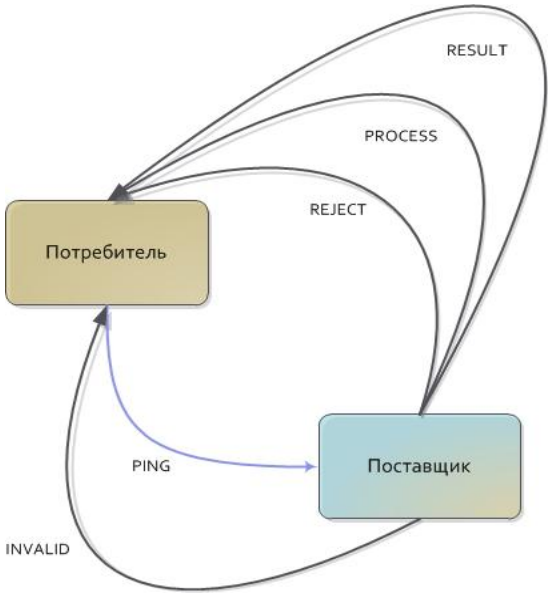


Рисунок 14 - Использование статусов сообщений при асинхронном взаимодействии

В ответах на повторные запросы статуса/результата, формируемых при асинхронном взаимодействии статус REJECT может применяться в различных прикладных ситуациях, таких как:

запрашиваемые сведения в учете отсутствуют;

запрос с указанным номером отправила иная система;

запрос с соответствующим номером не зарегистрирован в системе поставщика.

В ответах на повторные запросы статуса/результата, формируемых при асинхронном взаимодействии, статус FAILURE может применяться в случае, если во время обработки запроса произошла системная ошибка, которая была корректно обработана ИС поставщика.

7.3.3. Взаимодействие для уведомления поставщика об ошибках в данных

Для подачи сообщений, содержащих уведомления об ошибках в данных, на стороне поставщика может разрабатываться специализированная операция электронного сервиса. Данный тип запроса используется только при асинхронном взаимодействии.

Если ОИВ или ПГУ хочет уведомить другой ОИВ об ошибке в его данных, он посылает сообщение со статусом NOTIFY.

Ответом на данное сообщение может быть сообщение со статусами ACCEPT, REJECT, INVALID.

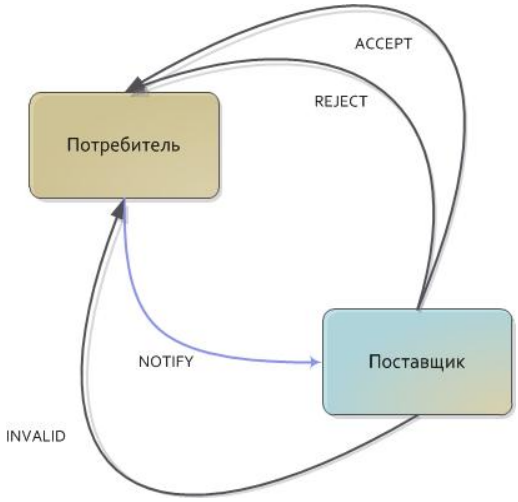


Рисунок 15 - Использование статусов сообщений при уведомлении об ошибке в данных

7.3.4. Взаимодействие для уведомления поставщика об отмене запроса

Для подачи сообщений, инициирующих отзыв поданного ранее запроса, на стороне поставщика сервиса может разрабатываться специализированная операция электронного сервиса. Данный тип запросов используется только при асинхронном взаимодействии.

При необходимости отозвать ранее инициированную обработку запроса, ОИВ или ПГУ посылает сообщение со статусом CANCEL.

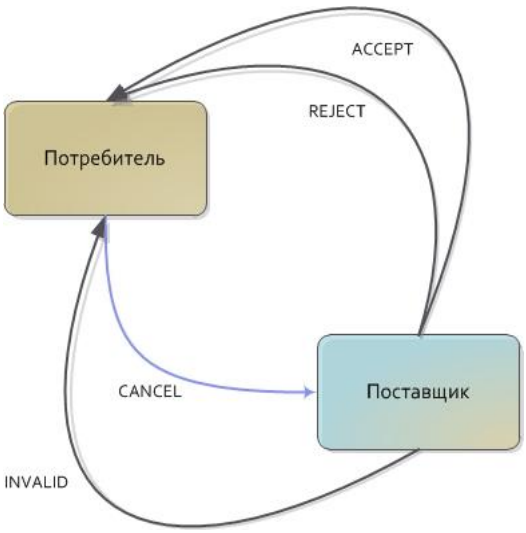


Рисунок 16 - Использование статусов сообщений при отмене ранее отправленного запроса

7.3.5. Взаимодействие в пакетном режиме

Для передачи электронных сообщений в пакетном режиме, содержащих несколько прикладных сообщений, участники должны применять статус PACKET как при запросе, так и при ответе.

Принципы проставления статусов для отдельных прикладных сообщений внутри пакета применяются такие же, как и для электронных сообщений, передаваемых не в пакетном режиме.

7.4. ПРАВИЛА ЗАПОЛНЕНИЯ ЭЛЕМЕНТА ДЛЯ ПЕРЕДАЧИ СВЕДЕНИЙ О ГОСУДАРСТВЕННОЙ УСЛУГЕ

Элемент smev:ServiceCode предназначен для передачи сведений о государственной услуге, в рамках исполнения которой производится взаимодействие субъектов.

Код государственной услуги указывается на основании Сводного реестра государственных услуг (функций).

7.5. ПРАВИЛА ЗАПОЛНЕНИЯ ЭЛЕМЕНТА ДЛЯ ПЕРЕДАЧИ НОМЕРА ДЕЛА

Элемент smev:CaseNumber является вспомогательным элементом, помогающим при разборе конфликтных ситуаций, возникающих при обмене сообщениями между поставщиком и потребителем. Данный элемент содержит номер дела в информационной системе Поставщика или Потребителя, в рамках которого ведется электронный обмен сообщениями. Данное поле позволяет связать номера дел в информационных системах Поставщика и Потребителя.

Сценарий взаимодействия с использованием данного поля:

а) Потребитель отправляет сообщение поставщику, указывая номер дела в своей информационной системе;

б) Поставщик отправляет ответное сообщение, указывая номер дела в своей информационной системе;

Таким образом, в обеих системах, появляется возможность связать соответствующие номера дел.

7.6. ПРИНЦИПЫ РАСЧЕТА СТАТИСТИКИ ОБМЕНА В РАМКАХ МЕЖВЕДОМСТВЕННОГО ВЗАИМОДЕЙСТВИЯ

1. Отчет формируется оператором СМЭВ, путем подсчета обращений к электронным сервисам, имеющим операции, предназначенные для межведомственного обмена, что означает:

Для корректного расчета статистики по межведомственному взаимодействию участники при формировании электронных сообщений должны в унифицированном служебном блоке атрибутов сообщения заполнять элемент smev:ExchangeType с указанием класса сообщений со значением 2 – Межведомственное взаимодействие (смотри классификатор в приложении 2).

2. В отчете отражаются только данные по межведомственному взаимодействию, в том числе:

- в отчет не включаются обращения с единого портала государственных услуг (функций), что означает исключение из расчета электронных сообщений с классом 1 – Взаимодействие с Порталом государственных услуг;
- обращения ведомств к собственным сервисам, что означает исключение из расчета электронных сообщений с классом 3 – Внутриведомственное взаимодействие;
- контрольные примеры, что означает исключение сообщений с элементом-признаком smev:TestMsg в унифицированном служебном блоке атрибутов;
- другие обращения, не связанные с межведомственным обменом при оказании государственных услуг и исполнении государственных функций, что означает включение в статистику только сообщений, у которых элемент smev:TypeCode принимает значения GSRV (взаимодействие в рамках оказания госуслуг) или GFNC (взаимодействие в рамках исполнения госфункций);
- в статистике отображаются только сообщения, которые имеют статусы smev:Status из списка:
    - REQUEST – подача заявления;
    - RESULT – возврат результата;
    - REJECT – мотивированный отказ;
    - NOTIFY – уведомление об ошибке в данных;

- CANCEL – запрос на отзыв заявления;
- STATE – возврат сообщения о статусе.

- для пакетных сообщений каждое логическое сообщение в пакете учитывается в статистике как отдельное сообщение при условии соблюдения требований к заполнению полей сообщения также и в структурах *smev:SubMessage*. Статус обработки пакета определяется статусами обработки содержащихся в не отдельных сообщений.

7.7. ПРАВИЛА КОДИФИКАЦИИ ОБЪЕКТОВ

7.7.1. Правила формирования мнемоник федеральных участников

Мнемоника федерального участника представляет собой четырехсимвольный код:

XXXX, где XXXX – мнемоника участника из четырех английских символов или цифр.

Например, мнемониками федеральных участников могут быть:

FMS0 – Федеральная миграционная служба России;

PFRF – Пенсионный фонд России.

Полный список мнемоник федеральных участников приведен в приложении 5.

7.7.2. Правила формирования мнемоник региональных участников

Мнемоника регионального участника представляет собой цифровой код:

YYYY, где YYYY – последовательность из четырех цифр или английских символов.

Регистрационные номера уникальным региональным участникам будут присваиваться в порядке регистрации их информационных систем в реестре информационных систем ЕСИА.

7.7.3. Правила формирования мнемоник информационных систем федерального уровня

Мнемоника информационной системы федерального уровня формируется по правилу:

XXXXNN – мнемоника федеральной информационной системы, где XXXX – мнемоника федерального участника;

NN – двухзначный цифровой номер информационной системы ведомства.

Например, **FMS001**, **FMS002** – для первой и второй информационной системы Федеральной миграционной службы России.

Мнемоники информационных систем при необходимости, могут вноситься в поле CN сертификата ЭП-ОВ наименования информационной системы, использующей данный сертификат.

Мнемоника присваивается информационной системе в ходе её регистрации в СМЭВ.

7.7.4. Правила формирования мнемоник информационных систем регионального уровня

Мнемоника информационной системы регионального уровня формируется по правилу:

YYYYNN – мнемоника федеральной информационной системы,

где YYYY – мнемоника регионального участника;

NN – двухзначный цифровой номер информационной системы ведомства.

Мнемоники информационных систем при необходимости, могут вноситься в поле CN сертификата ЭП-ОВ наименования информационной системы, использующей данный сертификат.

Мнемоника присваивается информационной системе в ходе её регистрации в СМЭВ.

7.7.5. Правила формирования мнемоник информационных систем, входящих в инфраструктуру электронного правительства

Для информационных систем, входящих в инфраструктуру электронного правительства, несмотря на то, что они принадлежат единому участнику взаимодействия – Минкомсвязи РФ, рекомендуется использовать более наглядные мнемоники информационных систем.

Список приведен в приложении 5.

Мнемоники ИС ИЭП формируются по правилу:

IEEENN – мнемоника информационной системы ИЭП,

где I – признак, характеризующий отношение к инфраструктуре электронного правительства;

EEE – трехсимвольный цифровой код: английские символы верхнего и нижнего регистра [A-Za-z] и цифры [0-9];

NN – двухзначный цифровой номер информационной системы участника.

7.7.6. Правила формирования мнемоник информационных систем участников, являющихся негосударственными поставщиками начислений или кредитными организациями

Для информационных систем участников, являющихся негосударственными поставщиками начислений или кредитными организациями, рекомендуется использовать более наглядные мнемоники информационных систем.

Список приведен в приложении 5.

Мнемоники ИС поставщиков начислений или кредитных организаций формируются по правилу:

KEEENN – мнемоника информационной системы ИЭП,

где K – признак, характеризующий отношение к негосударственным поставщикам начислений или кредитным организациям;

EEE – трехсимвольный цифровой код: английские символы верхнего и нижнего регистра [A-Za-z] и цифры [0-9];

NN – двухзначный цифровой номер информационной системы участника.

7.7.7. Правила определения кодов регионов

При кодификации региона рекомендуется использовать двухсимвольный цифровой код по классификатору КЛАДР.

Список кодов регионов, применяемых при взаимодействии через СМЭВ, приведен в приложении 5.

В случае, если информационные системы, применяемые в территориальных подразделениях, обслуживают нужды нескольких регионов, то такая ИС должна обеспечивать проставление корректного кода в электронных сообщениях для каждого региона.

7.7.8. Правила формирования мнемоник электронных сервисов

Мнемоника электронного сервиса формируется на базе мнемоники участника обмена и текстового описания сервиса, облегчающего распознавание на уровне мнемоники прикладной сущности сервиса:

Для электронных сервисов федеральных поставщиков мнемоника будет иметь вид:

XXXXzzzzzzzzzzzzzzzzzzzzzzzzzz,

где XXXX – мнемоника федерального участника;

zzzzzzzzzzzzzzzzzzzzzzzzzz - наименование сервиса (не более 26 символов): английские символы верхнего и нижнего регистра [A-Za-z] и цифры [0-9].

Для электронных сервисов региональных поставщиков мнемоника будет иметь вид:

YYYYzzzzzzzzzzzzzzzzzzzzzzzzzz,

где YYYY – мнемоника регионального участника;

zzzzzzzzzzzzzzzzzzzzzzzzzz - наименование сервиса (не более вооо26 символов): английские символы [A-Za-z] и цифры [0-9].

Наименование сервиса может быть выбрано поставщиком сервиса на основании описанных выше правил формирования.

7.7.9. Правила формирования мнемоник точек подключения

Мнемоники точек подключения информационных систем формируются по следующему шаблону:

XXXXNNRRM – для федеральных участников,

YYYYNNRRM – для региональных участников,

где XXXX/YYYY – мнемоника участника из четырех символов;

NN – двухзначный цифровой номер информационной системы ведомства;

RR – двузначный цифровой код региона, к которому относится точка подключения;

M – однозначный цифровой номер экземпляра точки подключения в регионе.

Например, если у Федеральной миграционной службы РФ используется 2 информационные системы для взаимодействия через СМЭВ, подключенные к федеральному узлу СМЭВ, то мнемоники точек подключения для них будут:

FMS001001 – первая информационная система (Сервисный концентратор), подключенная к федеральному СМЭВ (где 00 – соответствует федеральному узлу).

FMS002001 – вторая информационная система (ПАК ГИСМУ Интеграция), подключенная к федеральному СМЭВ.

8. ПРАВИЛА РАЗРАБОТКИ МУНИЦИПАЛЬНЫХ СЕРВИСОВ ПО ПРЕДОСТАВЛЕНИЮ ТИПОВЫХ СВЕДЕНИЙ

8.1 ПРОТОКОЛ ВЗАИМОДЕЙСТВИЯ С МУНИЦИПАЛЬНЫМИ СЕРВИСАМИ ПО ПРЕДОСТАВЛЕНИЮ ТИПОВЫХ СВЕДЕНИЙ

Федеральный закон №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» определяет перечень сведений, предоставляемых всеми муниципальными образованиями. Требования данного раздела предназначены для обеспечения единообразного вызова таких сервисов, чтобы Потребителю не пришлось интегрироваться с каждым ОМСУ (Поставщиками сервисов) по отдельному протоколу.

Процесс взаимодействия Потребителя (ФОИВ) и Поставщиков сервисов (ОМСУ) является в данном случае асинхронным, однако строится он на синхронных вызовах.

При взаимодействии используется модель ***асинхронного взаимодействия с повторным опросом,*** которая заключается в разработке на стороне поставщика электронного сервиса, реализующего функции приема заявлений на обработку запросов и возврата статусов и результатов обработки в асинхронном режиме. При этом различные функции реализуются в виде одной операции (метода) единого электронного сервиса.

Функция приема заявления должна быть реализована на стороне поставщика и предусматривать синхронный возврат ответа-квитанции потребителю, свидетельствующей о приеме в обработку заявления.

В случае, когда при приеме заявления информационная система поставщика синхронно может сформировать мотивированный отказ в обработке, или возникновении каких-либо ошибок, препятствующих обработке запроса, асинхронное взаимодействие прекращается до отправки повторного запроса со стороны потребителя.

Предоставление сведений о статусе обработки запроса или его результатов должно осуществляться через ту же самую функцию, что и отправка заявления.

Требуемое действие Потребитель сервиса указывается в поле smev:Status заголовка smev:Message:

REQUEST	Отправка заявления
PING	Запрос статуса заявления
CANCEL	Отзыв заявления

Поставщик сервиса указывает в поле smev:Status заголовка smev:Message результат выполнения операции:

ACCEPT	Заявление принято
PROCESS	Идет обработка заявления
RESULT	Ответное сообщение представляет собой результат обработки заявления
REJECT	Мотивированный отказ
FAILURE	Технический сбой

Потребитель для получения статусов и/или результатов должен реализовать в своей информационной системе функцию периодического вызова сервиса возврата статусов и результатов на стороне информационной системы поставщика.

Периодичность вызова информационной системы поставщика со стороны потребителя регулируется договоренностями между потребителем и поставщиком. Регламентированная периодичность вызова информационной системы поставщика со стороны различных потребителей, указывается в паспорте электронного сервиса поставщика.

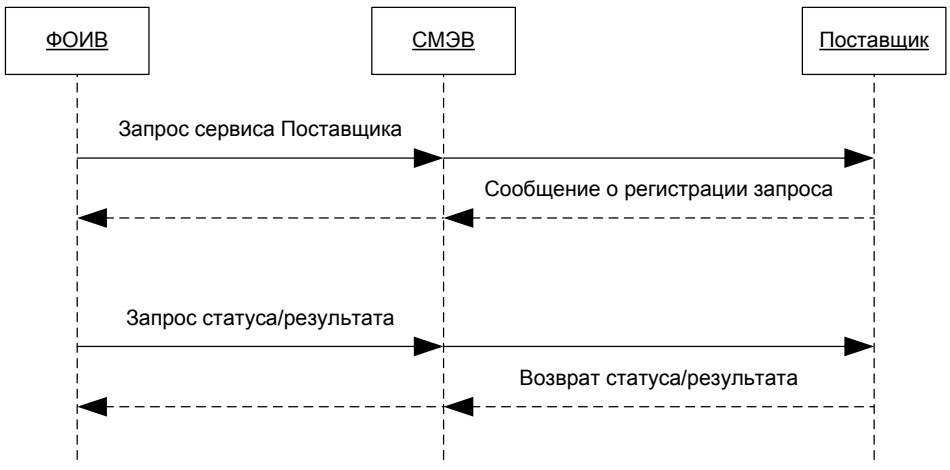


Рисунок 17 - Модель асинхронного информационного обмена при межведомственном взаимодействии с ОМСУ

Таким образом, для каждого типа сведений реализуется один сервис, содержащий один метод, обрабатывающий все типы запросов (заявление, проверка статуса, возврат

результата). Прикладная часть формата сервиса определяется ФОИВ-ом, ответственным за данный сервис и обязательна для точной реализации на стороне Поставщика сервиса.

При вызове сервиса Потребитель обязательно указывает в заголовке smev:Message поле ОКТМО, на основе которого СМЭВ производит маршрутизацию в нужный регион и соответствующему Поставщику сервиса.

В ходе предоставления региональных типовых сведений по запросу ФОИВ в поле smev:Recipient/smev:Code Потребитель (федеральный) указывает мнемонику ИС маршрутизатора ФСМЭВ (ISMV01001), т.к. получателем сообщения является сервис-маршрутизатор, располагающийся на федеральном узле СМЭВ. В поле smev:Recipient/smev:Name Потребитель указывает значение "Маршрутизатор типовых сведений единой системы межведомственного электронного взаимодействия".

В ходе предоставления федеральных типовых сведений по запросу РОИВ (ОМСУ) в поле smev:Recipient/smev:Code Потребитель (региональный) указывает мнемонику ИС федерального Поставщика, предоставляющего запрашиваемое типовое сведение.

9. ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1. ОБЩАЯ СТРУКТУРА ЭЛЕКТРОННОГО СООБЩЕНИЯ СМЭВ

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:smev="http://smev.gosuslugi.ru/rev120315" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
<!-- Заголовок электронного сообщения -->
<soapenv:Header>
        <!— ЭП-ПГУ или ЭП-ОВ информационной системы, отправляющей электронное сообщение. Проверяется в СМЭВ -->
        <wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/smev">
                <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
messagesecurity-
                1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"
                wsu:Id="SenderCertificate"><!-- Токен безопасности в Base64 --></wsse:BinarySecurityToken>
                <ds:Signature Id="sender-wssec">
                        <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-
                                gostr3411"/>
```

```
                                        <ds:Reference URI="#sampleRequest">
                                                <ds:Transforms>
                                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                                </ds:Transforms>
                                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
                                                <ds:DigestValue><!-- Значение хеша в Base64 --></ds:DigestValue>
                                        </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue><!-- Значение подписи в Base64 --></ds:SignatureValue>
                                <ds:KeyInfo>
                                        <wsse:SecurityTokenReference>
                                        <wsse:Reference URI="#SenderCertificate" ValueType="http://docs.oasisopen.
                                        org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
                                        </wsse:SecurityTokenReference>
                                </ds:KeyInfo>
                        </ds:Signature>
                </wsse:Security>
                <!-- ЭП-СМЭВ. Проверяется в информационной системе, получающей электронное сообщение. -->
                <wsse:Security soapenv:actor="http://smev.gosuslugi.ru/actors/recipient">
                        <wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
messagesecurity-
                        1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3"
                        wsu:Id="SMEVCertificate"><!-- Токен безопасности в Base64 --></wsse:BinarySecurityToken>
                        <ds:Signature Id="smev-wssec">
                                <ds:SignedInfo>
                                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-
                                        gostr3411"/>
                                        <ds:Reference URI="#sampleRequest">
                                                <ds:Transforms>
                                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                                </ds:Transforms>
                                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
```

```
                                    <ds:DigestValue><!-- Значение хеша в Base64 --></ds:DigestValue>
                                    </ds:Reference>
                                    <ds:Reference URI="#smevHeader">
                                        <ds:Transforms>
                                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
                                    <ds:DigestValue><!-- Значение хеша в Base64 --></ds:DigestValue>
                                    </ds:Reference>
                            </ds:SignedInfo>
                            <ds:SignatureValue><!-- Значение подписи в Base64 --></ds:SignatureValue>
                            <ds:KeyInfo>
                                    <wsse:SecurityTokenReference>
                                        <wsse:Reference URI="#SMEVCertificate" ValueType="http://docs.oasisopen.
                                        org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
                                    </wsse:SecurityTokenReference>
                            </ds:KeyInfo>
                <!-- Метка времени внутри ЭП-СМЭВ. -->
                    <ds:Object>
                    <xds:QualifyingProperties  xmlns:xds="http://uri.etsi.org/01903/v1.1.1#">
                    <xds:UnsignedProperties>
                    <xds:UnsignedSignatureProperties>
                    <xds:SignatureTimeStamp>
                    <xds:HashDataInfo uri="#signature-value-40ddb6ca-9ac1-4026-a049-76901f3aa5d8"/>
                    <xds:EncapsulatedTimeStamp>Метка времени в Base64</xds:EncapsulatedTimeStamp>
                    </xds:SignatureTimeStamp>
                    </xds:UnsignedSignatureProperties>
                    </xds:UnsignedProperties>
                    </xds:QualifyingProperties>
                    </ds:Object>
                    </ds:Signature>
            </wsse:Security>
            <!-- Унифицированный служебный заголовок СМЭВ. Подписывается ЭП СМЭВ. -->
```

```
        <smev:Header wsu:Id="smevHeader">
                <smev:NodeId>Уникальный идентификатор узла СМЭВ</smev:NodeId>
                <smev:MessageId>Уникальный код сообщения в СМЭВ</smev:MessageId>
                <smev:TimeStamp>Дата получения сообщения СМЭВ</smev:TimeStamp>
                <smev:MessageClass>REQUEST</smev:MessageClass>
        </smev:Header>
</soapenv:Header>
<!-- Тело электронного сообщения -->
<soapenv:Body wsu:Id="sampleRequest">
        <smevSampleMsg:sampleRequest xmlns:smevSampleMsg="http://smev.gosuslugi.ru/SampleMessage">
                <!-- Унифицированный служебный блок атрибутов сообщения СМЭВ. Подписывается ЭП ОВ информационной
                системы, отправляющей электронное сообщение -->
                <smev:Message>
                        <smev:Sender><!--Данные о системе-инициаторе взаимодействия (Потребителе) --></smev:Sender>
                        <smev:Recipient><!--Данные о системе-получателе сообщения (Поставщике) --></smev:Recipient>
                        <smev:Originator><!--Данные о системе, инициировавашей цепочку из нескольких запросов-ответов,
                        объединенных единым процессом в рамках взаимодействия --></smev:Originator>
                        <smev:Service>
                          <smev:Mnemonic><!-Мнемоника сервиса--></smev:Mnemonic>
                          <smev:Version><!-Версия сервиса--></smev:Version>
                        </smev:Service>
                        <smev:TypeCode><!--Тип сообщения по классификатору сообщений в СМЭВ --></smev:TypeCode>
                        <smev:Status><!-- Статусе электронного сообщения по классификатору статусов  --></smev:Status>
                        <smev:Date><!--Дата создания сообщения--></smev:Date>
                        <smev:RequestIdRef><!--Идентификатор сообщения-запроса, инициировавшего взаимодействие --
></smev:RequestIdRef>
                        <smev:OriginRequestIdRef><!--Идентификатор сообщения-запроса, инициировавшего цепочку из
                        нескольких запросов-ответов, объединенных единым процессом в рамках взаимодействия --
></smev:OriginRequestIdRef>
                        <smev:ServiceCode>< !--Код государственной услуги указывается в соответствии с правилами
кодификации, установленными в ИС Сводного реестра государственных услуг --></smev:ServiceCode>
                        <smev:CaseNumber>< !--Номер дела указывается в соответствии с правилами, установленными в
информационной системы-отправителя. --></smev:CaseNumber>
                        <smev:ExchangeType>< !-- Признак принадлежности электронного сообщения различным категориям
взаимодействия. Указывается в соответствие с классификатором категорий взаимодействия--></smev:ExchangeType>
                        <smev:TestMsg>< !--Признак тестового электронного сообщения: запроса или ответа. Не указывается
```

```
при продуктивном взаимодействии. --></smev:TestMsg>
                        <smev:OKTMO><!-- Код ОКТМО . --></smev:OKTMO>
                    </smev:Message>
                    <!-- Унифицированный служебный блок-обертка передаваемых данных сообщения СМЭВ. Данные электронного
                    сообщения -->
                    <smev:MessageData>
                        <!-- Унифицированный блок-обертка для передачи информации в соответствии с требованиями
                        поставщика -->
                        <smev:AppData><!-- Данные из ОИВ --></smev:AppData>
                        <!-- Унифицированный блок передачи прикладных данных -->
                        <smev:AppDocument><!-- Передаваемый ZIP-архив в Base64 --></smev:AppDocument>
                    </smev:MessageData>
            </smevSampleMsg:sampleRequest>
</soapenv:Body>
</soapenv:Envelope>
```

ПРИЛОЖЕНИЕ 2. КЛАССИФИКАТОРЫ ДЛЯ СЛУЖЕБНЫХ ЭЛЕМЕНТОВ ЭЛЕКТРОННЫХ СООБЩЕНИЙ СМЭВ

Классификатор «Класс сообщения»

Идентификатор	Значение
REQUEST	Электронное сообщение - запрос
RESPONSE	Электронное сообщение - ответ

Классификатор «Тип сообщения»

Идентификатор	Значение
GSRV	Взаимодействие в рамках оказания государственных услуг
GFNC	Взаимодействие в рамках исполнения государственных функций
OTHR	Взаимодействие в иных целях, предусмотренных законодательством

Классификатор «Мнемоники статусов сообщения»

Мнемоника	Наименование	Описание	Допустимость для класса сообщения
ACCEPT	Сообщение-квиток о приеме	Служебное сообщение, свидетельствует о приеме электронного сообщения на стороне поставщика электронного сервиса.	Ответ
CANCEL	Отзыв заявления	Запрос на отмену обработки электронного заявления на стороне поставщика, инициированного предшествующим запросом.	Запрос
FAILURE	Технический сбой	Обработанное прерывание на стороне поставщика электронного сервиса, свидетельствующее об ошибке обработки электронного сообщения запроса.	Ответ
INVALID	Ошибка при ФЛК	Ошибка, возникающая при выполнении формально-логического контроля входящего сообщения.	Ответ (синхронный режим)/Запрос (асинхронный режим)
NOTIFY	Уведомление об ошибке	Сообщение, отправляемое поставщику сервиса с уведомлением об ошибке в сведениях, предоставленных его электронным сервисом.	Запрос
PACKET	Пакетный режим обмена	Электронное сообщение содержит пакет прикладных сообщений.	Запрос/Ответ
PING	Запрос данных/результатов	Запрос результата у поставщика в асинхронном режиме взаимодействия.	Запрос
PROCESS	В обработке	Ответ на запрос данных/результатов, отправляемый поставщиком сервиса в случае, если результат еще может быть предоставлен по причине того, что обработка не завершена.	Ответ
REJECT	Мотивированный отказ	Отрицательный ответ прикладного уровня на запрос	Ответ (синхронный режим)/Запрос (асинхронный режим)

REQUEST	Запрос	Электронное сообщение, которое инициирует одну сессию взаимодействия между потребителем и поставщиком.	Запрос
RESULT	Результат	Ответ на запрос, который содержит сведения, ради которых инициировался обмен данными.	Ответ (синхронный режим)/Запрос (асинхронный режим)
STATE	Возврат состояния	Ответ на запрос, который содержит сведения о состоянии обработки электронного заявления.	Ответ (синхронный режим)/Запрос (асинхронный режим)

Классификатор «Категория взаимодействия»

Идентификатор категории	Наименование категории	Участники взаимодействия	Описание категории
0	**Неопределенная категория**		В случае отсутствия в классификаторе допускается использовать данную категорию до тех пор, пока со стороны Оператора СМЭВ не будут обозначены рекомендации по использованию другой категории.
1	**Взаимодействие с порталами государственных услуг**	ПГУ-ОИВ ОИВ-ПГУ	Передача данных из заполненной формы заказа услуги на Едином портале государственных услуг (функций) в информационную систему участника взаимодействия, ответственного за оказание услуги в электронном виде или возврат статуса/результата оказания услуги в электронном виде.
2	**Межведомственное взаимодействие**	ОИВ1-ОИВ2	Взаимодействие между различными органами исполнительной власти в рамках оказания государственных услуг или исполнения государственных функций.
3	**Внутриведомственное взаимодействие через СМЭВ**	ОИВ-ОИВ	Взаимодействие между различными информационными системами одного органа исполнительной власти через СМЭВ.
4	**Взаимодействие с поставщиками начислений**	ИПШ - поставщики начислений	Взаимодействие информационно-платежного шлюза с поставщиками начислений для оплаты услуг в электронном виде.
5	**Взаимодействие ИПШ с ФК**	ИПШ-ФК	Взаимодействие ИПШ с системой УНИФО ФК для

			получения начислений и фактов оплаты для пользователей ПГУ
6	**Взаимодействие ОИВ с ФК**	ОИВ-ФК	Взаимодействие ОИВ с системой УНИФО ФК для передачи начислений и получения фактов оплаты

ПРИЛОЖЕНИЕ 3. СХЕМА ДАННЫХ СЛУЖЕБНЫХ ЭЛЕМЕНТОВ В ЭЛЕКТРОННЫХ СООБЩЕНИЯХ СМЭВ

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"

        xmlns:smev="http://smev.gosuslugi.ru/rev120315"
xmlns:xop="http://www.w3.org/2004/08/xop/include"

        targetNamespace="http://smev.gosuslugi.ru/rev120315"

        elementFormDefault="qualified" attributeFormDefault="unqualified"

        version="2.5.3">

        <xs:import namespace="http://www.w3.org/2004/08/xop/include"

                schemaLocation="http://www.w3.org/2004/08/xop/include" />

        <xs:element name="Header" type="smev:HeaderType">

                <xs:annotation>

                        <xs:documentation>Служебный загловок СМЭВ</xs:documentation>

                </xs:annotation>

        </xs:element>

        <xs:element name="BaseMessage" type="smev:BaseMessageType">

                <xs:annotation>

                        <xs:documentation>Базовый тип, описывающий сообщение в целом

                        </xs:documentation>

                </xs:annotation>

        </xs:element>

        <xs:element name="Message" type="smev:MessageType">

                <xs:annotation>

                        <xs:documentation>Служебный блок атрибутов СМЭВ

                        </xs:documentation>

                </xs:annotation>

        </xs:element>
```

```
<xs:element name="SubMessage" type="smev:SubMessageType">
	<xs:annotation>
		<xs:documentation>Описание заявки пакета
		</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="SubMessages" type="smev:SubMessagesType">
	<xs:annotation>
		<xs:documentation>Набор описей заявок пакета
		</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="MessageData" type="smev:MessageDataType">
	<xs:annotation>
		<xs:documentation>Блок-обертка данных СМЭВ</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="AppData" type="smev:AppDataType">
	<xs:annotation>
		<xs:documentation>Блок структурированных сведений</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="AppDocument" type="smev:AppDocumentType">
	<xs:annotation>
		<xs:documentation>Блок вложений</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="SubRequestNumber" type="xs:string">
```

```
                <xs:annotation>
                        <xs:documentation>Уникальный идентификатор сообщения внутри пакета
назначается инициатором взаимодействия
                        </xs:documentation>
                </xs:annotation>
        </xs:element>
        <xs:element name="Sender" type="smev:orgExternalType">
                <xs:annotation>
                        <xs:documentation>Данные о системе-инициаторе взаимодействия
                                (Потребителе) (валидируется СМЭВ на соответствие сертификату)
                        </xs:documentation>
                </xs:annotation>
        </xs:element>
        <xs:element name="Recipient" type="smev:orgExternalType">
                <xs:annotation>
                        <xs:documentation>Данные о системе-получателе сообщения (Поставщике)
                                (валидируется СМЭВ по реестру поставщиков)
                        </xs:documentation>
                </xs:annotation>
        </xs:element>
        <xs:element name="Originator" type="smev:orgExternalType">
                <xs:annotation>
                        <xs:documentation>Данные о системе, инициировавашей цепочку из
                                нескольких запросов-ответов, объединенных единым процессом в рамках
                                взаимодействия
                        </xs:documentation>
                </xs:annotation>
        </xs:element>
        <xs:element name="Service" type="smev:ServiceType">
```

```
            <xs:annotation>
                <xs:documentation>
                    Целевой сервис
                </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="TypeCode" type="smev:TypeCodeType">
            <xs:annotation>
                <xs:documentation>Тип сообщения</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="Date" type="xs:dateTime">
            <xs:annotation>
                <xs:documentation>Дата создания запроса</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="RequestIdRef" type="smev:idType">
            <xs:annotation>
                <xs:documentation>Идентификатор сообщения-запроса, инициировавшего
                    взаимодействие
                </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="OriginRequestIdRef" type="smev:idType">
            <xs:annotation>
                <xs:documentation>Идентификатор сообщения-запроса, инициировавшего
                    цепочку из нескольких запросов-ответов, объединенных единым
                    процессом в рамках взаимодействия
```

```
                </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="ServiceCode" type="xs:string">
            <xs:annotation>
                <xs:documentation>Код услуги</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="CaseNumber" type="xs:string">
            <xs:annotation>
                <xs:documentation>Номер заявки в информационной системе-отправителе
                </xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="ServiceName" type="xs:string">
            <xs:annotation>
                <xs:documentation>Мнемоника электронного сервиса</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="OKTMO" type="xs:string">
            <xs:annotation>
                <xs:documentation>Код  ОКТМО</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="MessageId" type="smev:idType">
            <xs:annotation>
                <xs:documentation>Идентификатор сообщения</xs:documentation>
            </xs:annotation>
```

```
</xs:element>
<xs:element name="TimeStamp" type="xs:dateTime">
        <xs:annotation>
                <xs:documentation>Метка времени получения запроса СМЭВ.ом
                </xs:documentation>
        </xs:annotation>
</xs:element>
<xs:element name="NodeId" type="xs:string">
        <xs:annotation>
                <xs:documentation>Уникальный идентификатор узла</xs:documentation>
        </xs:annotation>
</xs:element>
<xs:element name="MessageClass" type="smev:MessageClassType">
        <xs:annotation>
                <xs:documentation>Идентификатор класса сообщения</xs:documentation>
        </xs:annotation>
</xs:element>
<xs:element name="Status" type="smev:StatusType">
        <xs:annotation>
                <xs:documentation>Статус сообщения</xs:documentation>
        </xs:annotation>
</xs:element>
<xs:element name="ExchangeType" type="xs:string">
        <xs:annotation>
                <xs:documentation>Категория взаимодействия</xs:documentation>
        </xs:annotation>
</xs:element>
<xs:element name="BinaryData" type="xs:base64Binary">
```

```
            <xs:annotation>
                <xs:documentation>Контент вложения</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="Reference" type="smev:ReferenceType">
            <xs:annotation>
                <xs:documentation>Ссылка на вложение</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="DigestValue" type="xs:base64Binary">
            <xs:annotation>
                <xs:documentation>Хеш-код вложения</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="TestMsg" type="xs:string">
            <xs:annotation>
                <xs:documentation>Идентификатор тестового запроса</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="RequestCode" type="xs:string">
            <xs:annotation>
                <xs:documentation>Код заявления</xs:documentation>
            </xs:annotation>
        </xs:element>
        <xs:element name="Id" type="smev:PacketIdType">
            <xs:annotation>
                <xs:documentation>Идентификатор заявки пакета</xs:documentation>
            </xs:annotation>
```

```
	</xs:element>
	<xs:element name="PacketIds" type="smev:PacketIdsType">
		<xs:annotation>
			<xs:documentation>Блок идентификаторов заявок пакета</xs:documentation>
		</xs:annotation>
	</xs:element>

	<xs:complexType name="HeaderType">
		<xs:sequence>
			<xs:element ref="smev:NodeId" />
			<xs:element ref="smev:MessageId" />
			<xs:element ref="smev:TimeStamp" />
			<xs:element ref="smev:MessageClass" />
			<xs:element ref="smev:PacketIds" minOccurs="0" />
		</xs:sequence>
		<xs:attribute name="actor" type="xs:string" />
		<xs:anyAttribute namespace="##any" processContents="lax" />
	</xs:complexType>
	<xs:complexType name="BaseMessageType">
		<xs:sequence>
			<xs:element ref="smev:Message" />
			<xs:element ref="smev:MessageData" />
		</xs:sequence>
	</xs:complexType>
	<xs:complexType name="SubMessageType">
		<xs:sequence>
			<xs:element ref="smev:SubRequestNumber" />
			<xs:element ref="smev:Status" />
```

```
                <xs:element ref="smev:Originator" minOccurs="0" />
                <xs:element ref="smev:Date" />
                <xs:element ref="smev:RequestIdRef" minOccurs="0" />
                <xs:element ref="smev:OriginRequestIdRef" minOccurs="0" />
                <xs:element ref="smev:ServiceCode" minOccurs="0" />
                <xs:element ref="smev:CaseNumber" minOccurs="0" />
        </xs:sequence>
</xs:complexType>
<xs:complexType name="SubMessagesType">
        <xs:sequence>
                <xs:element ref="smev:SubMessage" minOccurs="1" maxOccurs="unbounded"/>
        </xs:sequence>
</xs:complexType>
<xs:complexType name="MessageType">
        <xs:sequence>
                <xs:element ref="smev:Sender" />
                <xs:element ref="smev:Recipient" />
                <xs:element ref="smev:Originator" minOccurs="0" />
                <xs:choice>
                        <xs:element ref="smev:ServiceName" />
                        <xs:element ref="smev:Service"/>
                </xs:choice>                        <xs:element ref="smev:TypeCode" />
                <xs:element ref="smev:Status" />
                <xs:element ref="smev:Date" />
                <xs:element ref="smev:ExchangeType" />
                <xs:element ref="smev:RequestIdRef" minOccurs="0" />
                <xs:element ref="smev:OriginRequestIdRef" minOccurs="0" />
                <xs:element ref="smev:ServiceCode" minOccurs="0" />
```

```
                <xs:element ref="smev:CaseNumber" minOccurs="0" />
                <xs:element ref="smev:SubMessages" minOccurs="0" maxOccurs="1"/>
                <xs:element ref="smev:TestMsg" minOccurs="0" />
                <xs:element ref="smev:OKTMO" minOccurs="0" />
        </xs:sequence>
</xs:complexType>
<xs:complexType name="MessageDataType">
        <xs:sequence>
                <xs:element ref="smev:AppData" minOccurs="0" />
                <xs:element ref="smev:AppDocument" minOccurs="0" />
        </xs:sequence>
</xs:complexType>
<xs:complexType name="PacketIdType">
        <xs:sequence>
                <xs:element ref="smev:MessageId" />
                <xs:element ref="smev:SubRequestNumber" />
        </xs:sequence>
</xs:complexType>
<xs:complexType name="PacketIdsType">
        <xs:sequence>
                <xs:element ref="smev:Id" maxOccurs="unbounded" />
        </xs:sequence>
</xs:complexType>
<xs:complexType name="AppDataType">
        <xs:sequence>
                <xs:any namespace="##any" processContents="lax" minOccurs="0"
                        maxOccurs="unbounded" />
        </xs:sequence>
```

```
        <xs:anyAttribute namespace="##any" processContents="lax" />
    </xs:complexType>
    <xs:complexType name="AppDocumentType">
        <xs:sequence>
            <xs:element ref="smev:RequestCode" />
            <xs:choice>
                <xs:element ref="smev:BinaryData" />
                <xs:sequence>
                    <xs:element ref="smev:Reference" />
                    <xs:element ref="smev:DigestValue" />
                </xs:sequence>
            </xs:choice>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ReferenceType" mixed="true">
        <xs:sequence>
            <xs:element ref="xop:Include" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="orgExternalType">
        <xs:annotation>
            <xs:documentation>Сведения об информационной системе
            </xs:documentation>
        </xs:annotation>
        <xs:sequence>                    <xs:element name="Code" type="smev:MnemonicType">
            <xs:annotation>
<xs:documentation>Идентификатор системы</xs:documentation>
</xs:annotation>                    </xs:element>
            <xs:element name="Name" type="xs:string">
```

```
                                        <xs:annotation>
                                                <xs:documentation>Наименование системы</xs:documentation>
                                        </xs:annotation>
                                </xs:element>                </xs:sequence>
        </xs:complexType>
        <xs:simpleType name="TypeCodeType">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="GSRV">
                                <xs:annotation>
                                        <xs:documentation>Взаимодействие в рамках оказания
государственных
                                                услуг
                                        </xs:documentation>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="GFNC">
                                <xs:annotation>
                                        <xs:documentation>Взаимодействие в рамках исполнения
государственных функций
                                        </xs:documentation>
                                </xs:annotation>
                        </xs:enumeration>
                        <xs:enumeration value="OTHR">
                                <xs:annotation>
                                        <xs:documentation>
                                                Взаимодействие в иных целях, предусмотренных
законодательством Российской Федерации
                                        </xs:documentation>
                                </xs:annotation>
```

```
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="MessageClassType">
            <xs:restriction base="xs:string">
                <xs:enumeration value="REQUEST">
                    <xs:annotation>
                        <xs:documentation>Запрос от потребителя к поставщику
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="RESPONSE">
                    <xs:annotation>
                        <xs:documentation>Ответ поставщика
потребителю</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="StatusType">
            <xs:restriction base="xs:string">
                <xs:enumeration value="REQUEST">
                    <xs:annotation>
                        <xs:documentation>Запрос</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="RESULT">
                    <xs:annotation>
                        <xs:documentation>Результат</xs:documentation>
```

```
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="REJECT">
                    <xs:annotation>
                        <xs:documentation>Мотивированный отказ</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="INVALID">
                    <xs:annotation>
                        <xs:documentation>Ошибка при ФЛК</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="ACCEPT">
                    <xs:annotation>
                        <xs:documentation>Сообщение-квиток о
приеме</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="PING">
                    <xs:annotation>
                        <xs:documentation>Запрос данных/результатов</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="PROCESS">
                    <xs:annotation>
                        <xs:documentation>В обработке</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="NOTIFY">
```

```
                                        <xs:annotation>
                                                <xs:documentation>Уведомление об ошибке</xs:documentation>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="FAILURE">
                                        <xs:annotation>
                                                <xs:documentation>Технический сбой</xs:documentation>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="CANCEL">
                                        <xs:annotation>
                                                <xs:documentation>Отзыв заявления</xs:documentation>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="STATE">
                                        <xs:annotation>
                                                <xs:documentation>Возврат состояния</xs:documentation>
                                        </xs:annotation>
                                </xs:enumeration>
                                <xs:enumeration value="PACKET">
                                        <xs:annotation>
                                                <xs:documentation>Передача пакетного
сообщения</xs:documentation>
                                        </xs:annotation>
                                </xs:enumeration>
                        </xs:restriction>
                </xs:simpleType>
                <xs:simpleType name="idType">
                        <xs:restriction base="xs:string" />
```

```
	</xs:simpleType>
	<xs:simpleType name="MnemonicType">
		<xs:annotation>
			<xs:documentation>Формат мнемоники</xs:documentation>
		</xs:annotation>
		<xs:restriction base="xs:string">
			<xs:minLength value="9" />
			<xs:maxLength value="9" />
			<xs:pattern value="[A-Z0-9]{4}\d{5}" />
			<xs:whiteSpace value="collapse" />
		</xs:restriction>
	</xs:simpleType>
	<xs:complexType name="ServiceType">
		<xs:annotation>
			<xs:documentation>Информация о целевом сервисе</xs:documentation>
		</xs:annotation>
		<xs:sequence>
			<xs:element name="Mnemonic" type="xs:string">
				<xs:annotation>
					<xs:documentation>Мнемоника сервиса</xs:documentation>
				</xs:annotation>
			</xs:element>
			<xs:element name="Version" type="smev:VersionType">
				<xs:annotation>
					<xs:documentation>Версия сервиса</xs:documentation>
				</xs:annotation>
			</xs:element>
		</xs:sequence>
```

```
        </xs:complexType>


        <xs:simpleType name="VersionType">
                <xs:annotation>
                        <xs:documentation>
                                Формат версии
                        </xs:documentation>
                </xs:annotation>
                <xs:restriction base="xs:string">
                        <xs:pattern value="\d{1,2}\.\d{2}"></xs:pattern>
                </xs:restriction>
        </xs:simpleType>
</xs:schema>
```

ПРИЛОЖЕНИЕ 4. СХЕМА ДАННЫХ, ИСПОЛЬЗУЕМЫХ ДЛЯ ОПИСАНИЯ ВЛОЖЕНИЙ ВНУТРИ ЗАЯВЛЕНИЙ

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
	xmlns:smev-request="http://smev.gosuslugi.ru/request/rev111111"
	targetNamespace="http://smev.gosuslugi.ru/request/rev111111"
	elementFormDefault="qualified" attributeFormDefault="unqualified"
	version="2.4.4">
	<xs:element name="AppliedDocuments" type="smev-request:AppliedDocumentsType">
		<xs:annotation>
			<xs:documentation>Группа вложений</xs:documentation>
		</xs:annotation>
	</xs:element>
	<xs:element name="AppliedDocument" type="smev-request:AppliedDocumentType">
		<xs:annotation>
			<xs:documentation>Вложение</xs:documentation>
		</xs:annotation>
	</xs:element>
	<xs:element name="CodeDocument" type="xs:string">
		<xs:annotation>
			<xs:documentation>Код документа</xs:documentation>
		</xs:annotation>
	</xs:element>
	<xs:element name="Name" type="xs:string">
		<xs:annotation>
			<xs:documentation>Имя файла документа</xs:documentation>
		</xs:annotation>
	</xs:element>
```

```
<xs:element name="Number" type="xs:string">
	<xs:annotation>
		<xs:documentation>Номер документа</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="URL" type="xs:string">
	<xs:annotation>
		<xs:documentation>Относительный путь к файлу внутри архива
		</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="Type" type="xs:string">
	<xs:annotation>
		<xs:documentation>MIME-тип контента</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:element name="DigestValue" type="xs:base64Binary">
	<xs:annotation>
		<xs:documentation>Хеш-код вложения</xs:documentation>
	</xs:annotation>
</xs:element>
<xs:complexType name="AppliedDocumentsType">
	<xs:sequence>
		<xs:element ref="smev-request:AppliedDocument" maxOccurs="unbounded"
			minOccurs="0" />
	</xs:sequence>
</xs:complexType>
<xs:complexType name="AppliedDocumentType">
	<xs:sequence>
		<xs:element ref="smev-request:CodeDocument" minOccurs="0" />
```

```
                        <xs:element ref="smev-request:Name" />
                        <xs:element ref="smev-request:Number" minOccurs="0" />
                        <xs:element ref="smev-request:URL" />
                        <xs:element ref="smev-request:Type" />
                        <xs:element ref="smev-request:DigestValue" minOccurs="0" />
                </xs:sequence>
                <xs:attribute ref="smev-request:ID" use="optional" />
        </xs:complexType>

        <xs:attribute name="ID">
                <xs:annotation>
                        <xs:documentation>Уникальный идентификатор вложения
                        </xs:documentation>
                </xs:annotation>
                <xs:simpleType>
                        <xs:restriction base="xs:ID" />
                </xs:simpleType>
        </xs:attribute>
</xs:schema>
```

Классификатор «Федеральные участники»

Мнемоника участника	Федеральные органы исполнительной власти
ARCH	Росархив
CUST	ФТС России
ECON	Минэкономразвития России
FADM	Росмолодежь
FAPM	Роспечать
FASR	ФАС России
FAVT	Росавиация
FFMS	ФСФР России
FGRP	ФБУ ГРП при Минюсте России
FINN	Росфиннадзор
FIPS	Роспатент
FISH	Росрыболовство
FLOT	Росморречфлот
FMBA	ФМБА России
FMS0	ФМС России
FNSR	ФНС России
FOMS	ФОМС
FRAR	Росалкогольрегулирование
FSBR	ФСБ России
FSFM	Росфинмониторинг
FSIN	ФСИН России
FSKN	ФСКН России
FSOR	ФСО России
FSOZ	Рособоронзаказ
FSPC	Роскосмос
FSSP	ФССП России
FSSR	ФСС России
FSTC	ФСТЭК России
FSVP	Россельхознадзор
FSVT	ФСВТС России
FTRF	ФСТ России
GFSR	ГФС России
GGER	Главгосэкспертиза
GKSR	Росстат
GOST	Росстандарт
GUSP	ГУСП

Мнемоника участника	Федеральные органы исполнительной власти
MCHS	МЧС России
MCXR	Минсельхоз России
MFIN	Минфин России
MIDR	МИД России
MINO	Минобороны России
MKRF	Минкультуры России
MNJT	Минюст России
MNPR	Минприроды России
MNPT	Минпромторг России
MNRG	Минэнерго России
MNSV	Минкомсвязь России
MONR	Минобрнауки России
MREG	Минрегион России
MSTM	Минспорттуризм России
MTRF	Росгидромет
MTRS	Минтранс России
MVDR	МВД России
OBRN	Рособрнадзор
PFRF	Пенсионный фонд РФ
RAVT	Росавтодор
RBRN	Рособоронпоставка
RGRN	Росграница
RKZN	Казначейство России
RLHZ	Рослесхоз
RNDR	Роснедра
RPRN	Росприроднадзор
RPTN	Роспатент
RPTR	Роспотребнадзор
RRRV	Росрезерв
RRTR	Росреестр
RSIM	Росимущество
RSOC	Роскомнадзор
RSSR	Россотрудничество
RSVZ	Россвязь
RTNZ	Ростехнадзор
RTRD	Роструд
RTRN	Ространснадзор
RZDN	Росздравнадзор
SPAL	Счетная палата Российской Федерации
SPTR	Спецстрой России

Мнемоника участника	Федеральные органы исполнительной власти
SVRR	СВР России
TOUR	Ростуризм
UDPR	Управление делами Президента Российской Федерации (федеральное агентство)
VODA	Росводресурсы
ZDSC	Минздравсоцразвития России
ZLDR	Росжелдор

Классификатор «Информационные системы инфраструкты электронного правительства»

Мнемоника ИС	Информационная система ИЭП
IPGU01	Единый портал государственных услуг (epgu.gosuslugi.ru)
IPGU02	Единый портал государственных услуг (gosuslugi.ru)
ICTO01	Экспертная система центров телефонного обслуживания
IZGS01	Электронный ЗАГС
ISMV00	Единая система межведомственного электронного взаимодействия
ISMV01	Маршрутизатор типовых сведений единой системы межведомственного электронного взаимодействия
ISMU01	Система обеспечения взаимодействия мобильных устройств с инфраструктурой электронного правительства
ISKM01	Система контроля и мониторинга
IPRK01	Система контроля реализации поручений Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления
ISIA01	Единая система идентификации и аутентификации
IPGP01	Портал госпродаж
IPGZ01	Независимый регистратор (Портал госзакупок)
IPSH01	Информационно-платёжный шлюз
IEPD01	Информационная система удостоверяющих центров ЕПД Электронного правительства
INSI01	Единая система нормативно-справочной информации
IGPS01	Государственная электронная почтовая система

Классификатор «Информационные системы участников, являющихся негосударственными поставщиками начислений или кредитными организациями»

Мнемоника ИС	Информационная система ИЭП

KUNI01	Юнителлер
KQWI01	Qiwi
KBMS01	Банк Москвы
KKA301	А3
KOCB01	Океан Банк
KGZP01	Газпромбанк
KPLB01	Банк Платина
KSBR01	СберБанк

Классификатор «Коды регионов»

Код региона	Регион
01	Республика Адыгея
02	Республика Башкортостан
03	Республика Бурятия
04	Республика Алтай
05	Республика Дагестан
06	Республика Ингушетия
07	Кабардино-Балкарская Республика
08	Республика Калмыкия
09	Карачаево-Черкесская Республика
10	Республика Карелия
11	Республика Коми
12	Республика Марий Эл
13	Республика Мордовия
14	Республика Саха
15	Республика Северная Осетия
16	Республика Татарстан
17	Республика Тыва
18	Удмуртская Республика
19	Республика Хакасия
20	Чеченская Республика
21	Чувашская Республика-Чувашия
22	Алтайский край
23	Краснодарский край
24	Красноярский край
25	Приморский край
26	Ставропольский край
27	Хабаровский край
28	Амурская область
29	Архангельская область
30	Астраханская область

31	Белгородская область
32	Брянская область
33	Владимирская область
34	Волгоградская область
35	Вологодская область
36	Воронежская область
37	Ивановская область
38	Иркутская область
39	Калининградская область
40	Калужская область
41	Камчатская область
42	Кемеровская область
43	Кировская область
44	Костромская область
45	Курганская область
46	Курская область
47	Ленинградская область
48	Липецкая область
49	Магаданская область
50	Московская область
51	Мурманская область
52	Нижегородская область
53	Новгородская область
54	Новосибирская область
55	Омская область
56	Оренбургская область
57	Орловская область
58	Пензенская область
59	Пермский край
60	Псковская область
61	Ростовская область
62	Рязанская область
63	Самарская область
64	Саратовская область
65	Сахалинская область
66	Свердловская область
67	Смоленская область
68	Тамбовская область
69	Тверская область
70	Томская область
71	Тульская область
72	Тюменская область
73	Ульяновская область
74	Челябинская область

75	Читинская область
76	Ярославская область
77	Город Москва
78	Город Санкт-Петербург
79	Еврейская автономная область
80	Агинский Бурятский автономный округ
82	Корякский автономный округ
83	Ненецкий автономный округ
84	Таймырский автономный округ
85	Усть-Ордынский Бурятский автономный округ
86	Ханты-Мансийский автономный округ
87	Чукотский автономный округ
88	Эвенкийский автономный округ
89	Ямало-Ненецкий автономный округ

ПРИЛОЖЕНИЕ 6. СПРАВОЧНИК ОШИБОК СМЭВ

Ошибки обработки запроса		
Код ошибки	**Сообщение об ошибке**	**Категория**
SMEV-100001	Внутренняя ошибка сервиса	Проверка подписи
SMEV-100002	Ошибка разбора XML сообщения [{0}]	Системная
SMEV-100003	Неверная ЭП сообщения	Проверка подписи
SMEV-100004	Не найден сертификат	Проверка подписи
SMEV-100005	Сертификат просрочен	Проверка подписи
SMEV-100006	Найдено более одного сертификата	Проверка подписи
SMEV-100007	Сертификат отозван УЦ	Проверка подписи
SMEV-100008	Не найдена подпись документа	Проверка подписи
SMEV-100009	Должно быть подписано Body сообщения	Проверка подписи
SMEV-100010	Неправильная конфигурация	ФЛК
SMEV-100011	Недоверенный сертификат	Проверка подписи
SMEV-100012	Нет прав доступа	Ограничение доступа
SMEV-100013	Неверный формат сертификата	Проверка подписи
SMEV-100014	Неизвестный тип токена	Проверка подписи

SMEV-100015	Неизвестный алгоритм	Проверка подписи
SMEV-100016	Неверный формат раздела Security	Проверка подписи
SMEV-100017	Ошибка в токене	Ограничение доступа
SMEV-100018	Токен не найден	Ограничение доступа
SMEV-100019	Сообщение просрочено	Проверка блока WSSecurity
SMEV-100020	Не могу связаться с сервисом проверки сертификата	Проверка подписи
SMEV-100021	Ошибка вызова внешнего сервиса проверки сертификата	Проверка подписи
SMEV-100022	Невозможно определить целевой регион	Конфигурация сервиса
SMEV-100100	Невозможно определить конечную точку маршрута сообщения	Динамическая маршрутизация
SMEV-102000	Сообщение не прошло ФЛК [имя проверки]. Найдены ошибки.	ФЛК
SMEV-104000	Ошибка обращения к серверу по протоколу HTTP	Установка метки времени
SMEV-104200	Ошибка валидации данных TSP	Установка метки времени
SMEV-104201	Ошибка при инициализации протокола TSP	Установка метки времени
Ошибки обработки ответа		
Код ошибки	**Сообщение об ошибке**	**Категория**
SMEV-200001	Внутренняя ошибка сервиса	Проверка подписи
SMEV-200002	Ошибка разбора XML сообщения [{0}]	Системная
SMEV-200003	Неверная ЭП сообщения	Проверка подписи
SMEV-200004	Не найден сертификат	Проверка подписи
SMEV-200005	Сертификат просрочен	Проверка подписи
SMEV-200006	Найдено более одного сертификата	Проверка подписи
SMEV-200007	Сертификат отозван УЦ	Проверка подписи

SMEV-200008	Не найдена подпись документа	Проверка подписи
SMEV-200009	Должно быть подписано Body сообщения	Проверка подписи
SMEV-200010	Неправильная конфигурация	ФЛК
SMEV-200011	Недоверенный сертификат	Проверка подписи
SMEV-200012	Нет прав доступа	Ограничение доступа
SMEV-200013	Неверный формат сертификата	Проверка подписи
SMEV-200014	Неизвестный тип токена	Проверка подписи
SMEV-200015	Неизвестный алгоритм	Проверка подписи
SMEV-200016	Неверный формат раздела Security	Проверка подписи
SMEV-200017	Ошибка в токене	Ограничение доступа
SMEV-200018	Токен не найден	Ограничение доступа
SMEV-200019	Сообщение просрочено	Проверка блока WSSecurity
SMEV-200020	Не могу связаться с сервисом проверки сертификата	Проверка подписи
SMEV-200021	Ошибка вызова внешнего сервиса проверки сертификата	Проверка подписи
SMEV-200022	Невозможно определить целевой регион	Конфигурация сервиса
SMEV-200100	Невозможно определить конечную точку маршрута сообщения	Динамическая маршрутизация
SMEV-202000	Сообщение не прошло ФЛК [имя проверки]. Найдены ошибки.	ФЛК
SMEV-204000	Ошибка обращения к серверу по протоколу HTTP	Установка метки времени
SMEV-204200	Ошибка валидации данных TSP	Установка метки времени
SMEV-204201	Ошибка при инициализации протокола TSP	Установка метки времени