Разработано

Генеральный директор
ЗАО «АСТ»

Руководитель (должность, наименование предприятия - разработчика АС)

_____ *А.А.Хмелинин*

Личная подпись Расшифровка подписи

«___» _____ 2012 г.

Согласовано

Директор
государственного казенного учреждения
«Региональный центр управления
государственными и муниципальными
информационными системами и ресурсами
Самарской области»

Руководитель (должность, наименование предприятия - заказчика АС)

_____ *Д.П.Шевченко*

Личная подпись Расшифровка подписи

«___» _____ 2012 г.

Выполнение работ по развитию государственной информационной системы Самарской области «Система межведомственного электронного взаимодействия»

СПЕЦИФИКАЦИЯ ТРЕБОВАНИЙ К МЕХАНИЗМАМ ПОСТАНОВКИ И ПРОВЕРКИ ЭП

Государственный контракт № ГК-2012-10/38

от 07.11.2012

ЛИСТОВ 24

Самара 2012 г.

Содержание

1. Введение

Полное наименование – государственная информационная система Самарской области «Система межведомственного электронного взаимодействия». Далее в тексте используются сокращенные наименования – Система, СМЭВ СО.

Данный документ описывает основные требования, предъявляемые к постановке электронной подписи (далее – ЭП) на сообщения и проверке ЭП сообщений, используемых в рамках межведомственного электронного взаимодействия посредством СМЭВ СО.

При постановке и проверке ЭП также следует руководствоваться требованиями документа «Методические рекомендации по использованию электронной подписи при межведомственном электронном взаимодействии» (версия 4.3) Министерства связи и массовых коммуникаций Российской Федерации.

2. Общие требования

В электронных сообщениях, передаваемых через СМЭВ СО, применяются следующие виды электронной подписи:

- электронная подпись, формируемая от имени пользователя РПГУ/ЕПГУ, осуществляющего заказ услуг в электронном виде (электронная подпись пользователя, далее – ЭП-П);
- электронная подпись, формируемая от имени должностного лица ОИВ/ОМСУ, участвующего в межведомственном взаимодействии при оказании государственных услуг (электронная подпись служебного пользования, далее – ЭП-СП);
- электронная подпись, формируемая от имени ОИВ/ОМСУ (электронная подпись органа власти или информационной системы органа власти, далее – ЭП-ОВ), участвующего в межведомственном

взаимодействии при оказании государственных услуг;

- электронная подпись, формируемая СМЭВ СО при обработке электронных сообщений, передаваемых через нее (далее – ЭП-СМЭВСО);
- электронная подпись, формируемая РПГУ/ЕПГУ при формировании электронных сообщений, передаваемых в информационные системы органов власти (далее – ЭП-ПГУ).

Форматы электронных подписей, применяемых в электронных сообщениях при межведомственном взаимодействии в электронном виде посредством СМЭВ СО, подразделяются на две категории:

- электронные подписи физических лиц (к этой категории относятся ЭП-П и ЭП-СП);
- электронные подписи органов власти (к этой категории относятся ЭП-ОВ, ЭП-СМЭВСО и ЭП-ПГУ).

Электронные подписи, используемые сотрудниками и информационными системами ОИВ и ОМСУ Самарской области, формируются на основе цифровых сертификатов электронной подписи, выдаваемых РУЦ СО. Порядок получения цифровых сертификатов определяется в соответствии с распоряжением Правительства Самарской области от 08.06.2011 № 175-р «О региональном удостоверяющем центре Самарской области».

Процесс информационного взаимодействия в электронном виде через СМЭВ СО с использованием электронных подписей включает в себя:

1. В процессе оказания государственной услуги (исполнения государственной функции) пользователь портала формирует в РПГУ/ЕПГУ или должностное лицо ОИВ/ОМСУ формирует в информационной системе ОИВ/ОМСУ 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 (блок ЭП для блока структурированных сведений), который подписывается ЭП информационной системы ОИВ/ОМСУ (ЭП-ОВ или ЭП-ПГУ) и размещается в блоке ЭП ИС отправителя, формирующей конверт электронного сообщения (аналог гербовой печати ведомства).

   - Перед подписанием на стороне ОИВ/ОМСУ должна осуществляться проверка наличия у сотрудника ОИВ/ОМСУ соответствующих полномочий и действительности его сертификата. Проверка полномочий осуществляется на стороне ОИВ/ОМСУ средствами информационной системы, используемой ОИВ/ОМСУ. Формирование ЭП-ОВ в данном случае аналогично 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 СО;

4. СМЭВ СО в автоматическом режиме производит:

   - идентификацию ИС отправителя по сертификату ЭП-ОВ;
   - проверку сертификата ЭП-ОВ в списке отозванных сертификатов;
   - проверку возможности обращения ИС отправителя к ИС адресата (получателя) электронного сообщения по матрице доступа СМЭВ СО;

- подписание запроса собственной ЭП-СМЭВСО (ЭП размещается в блоке ЭП СМЭВ СО);
- гарантированную доставку запроса до ИС адресата.

5. ИС адресата, получив из СМЭВ СО запрос осуществляет:
   - проверку сертификата и корректность формирования ЭП-СМЭВСО;
   - проверку сертификата и корректность формирования ЭП-ОВ или ЭП ПГУ;
   - проверку сертификата и корректность формирования ЭП-П или ЭП-СП.
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-СМЭВСО 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.

При взаимодействии региональных информационных систем между собой посредством СМЭВ СО используются следующие правила:

- формирование ЭП-ОВ от имени ИС регионального участника осуществляется с использованием атрибута actor="http://smev.samregion.ru/actors/smev";

- СМЭВ СО формирует ЭП-СМЭВСО с использованием атрибута actor="http://smev.samregion.ru/actors/recipient".

При межуровневом взаимодействии для участников предусматриваются аналогичные правила использования атрибутов ЭП-ОВ и ЭП-СМЭВСО:

- Потребитель при запросе формирует ЭП-ОВ для своей информационной системы с использованием атрибута actor="http://smev.samregion.ru/actors/smev";
- СМЭВ СО при запросе формирует ЭП-СМЭВСО с использованием атрибута actor="http://smev.samregion.ru/actors/smevXX" (где XX – соответствует коду узла, к которому будет осуществляться обращение для доступа к системе Поставщика);
- узел СМЭВ, к которому подключена ИС Поставщика, при запросе формирует ЭП-РСМЭВ с использованием атрибута actor="http://smev.gosuslugi.ru/actors/recipient";
- Поставщик при ответе на запрос формирует ЭП-ОВ для своей информационной системы с использованием атрибута actor="http://smev.gosuslugi.ru/actors/smev";
- 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 осуществляться обращение для доступа к системе Потребителя);
- СМЭВ СО при ответе на запрос формирует ЭП-СМЭВСО с использованием атрибута actor="http://smev.samregion.ru/actors/recipient".

3. Электронные подписи физических лиц

Сертификаты и ключи электронной подписи пользователя РПГУ/ЕПГУ (ЭП-П) 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 РПГУ/ЕПГУ.

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

Сертификаты и ключи 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 ОИВ/ОМСУ в ИС ОВ.

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

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

При подаче заявлений с РПГУ/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 с 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 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 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.

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:

Наименование элемента	**Описание элемента**
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.

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 ОИВ/ОМСУ в формате XML с именем req_GUID.xml со ссылками на файлы-вложения.
3. Расчет хэш-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-файле 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 СО (или передается вне сообщения как MTOM-attachment).

3.3. 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» http://www.w3.org/TR/2002/REC-xmldsig-core-20020212).

Блок подписи размещается как дочерний для элемента smev:AppData, на одном уровне с бизнес-содержимым.

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.

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

Алгоритм	Наименование	URI
Расчет хэш-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 July 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.

3.4. 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:

   - Создается элемент Signature;
   - К элементу Signature добавляется дочерний элемент SignedInfo;
   - К элементу SignedInfo добавляется дочерний элемент

CanonicalizationMethod;

- К элементу SignedInfo добавляется дочерний элемент SignatureMethod;
- К элементу SignedInfo добавляется первый дочерний элемент Reference;
- К элементу Reference добавляется дочерний элемент Transforms;
- К элементу Transforms элемента Reference добавляется дочерний элемент Transform (два элемента);
- К элементу Reference добавляется элемент DigestMethod;
- К элементу Reference добавляется элемент DigestValue;
- К элементу Signature добавляется дочерний элемент SignatureValue;
- К элементу Signature добавляется дочерний элемент KeyInfo;
- К элементу KeyInfo добавляется дочерний элемент X509Data;
- К элементу X509Data добавляется дочерний элемент X509Certificate.

2. Установка предопределенных значений

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

more#gostr34102001-gostr3411".

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

3. Установка подписи

- 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.
- 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.
- 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. Электронные подписи органов власти

Сертификаты и ключи электронной подписи, используемые для формирования электронных подписей ОИВ/ОМСУ выдаются на имя органа власти и применяются в информационных системах при оказании государственных и муниципальных услуг/исполнении государственных и муниципальных функций с использованием СМЭВ СО для формирования ЭП.

ЭП-ОВ аналогичны гербовой печати организации и подтверждают:

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

Орган власти, отправляющий электронный документ с использованием СМЭВ СО 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.

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

Сертификаты и ключи электронной подписи, используемые для формирования электронных подписей в сообщениях СМЭВ СО, выдаются на имя оператора системы межведомственного электронного взаимодействия Самарской области и применяются в СМЭВ СО для формирования ЭП.

ЭП-СМЭВСО подтверждает:

- факт прохождения электронного сообщения через СМЭВ СО;
- 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 СО.

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

4.1. 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 хэш-сумм, формирования подписи и каноникализации:

Алгоритм	Наименование	URI
Расчет хэш-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	http://www.w3.org/2001/10/xml-exc-c14n#

	Canonicalization от 18 July 2002	

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

Информационная система органа власти Потребителя или РПГУ/ЕПГУ/РАИС МФЦ при формировании запроса к ИС Поставщика, а также ИС Поставщика при формировании ответа должны проставлять в атрибуте actor значение, соответствующее СМЭВ СО, как стороне, проверяющей подпись.

СМЭВ СО при формировании электронной подписи в запросе при отправке его Поставщику или при отправке ответа к Потребителю проставляет в атрибуте actor значение, соответствующее получателю.

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).

4.2. Порядок формирования электронной подписи информационной системы

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

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

3. Происходит подготовка структуры для сохранения результатов (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.

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 '#' (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 '#'.

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 хэш по алгоритму ГОСТ Р 34.11-94 и заносится в <ds:DigestValue> в формате Base64.

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.

5. Описание логики работы сервиса подписи СМЭВ СО

В состав СМЭВ СО входит реализация служебного сервиса подписи, предназначенного для выполнения следующих операций:

- проверка сертификата на предмет действительности (отсутствие в списке отозванных сертификатов – CRL);
- создание подписи XML-сообщения;
- проверка подписи XML-сообщения.

5.1. Проверка сертификата

Данная операция выполняется в момент создания или проверки подписи XML-сообщения. В связи с функционированием компонентов ЭП СО в рамках защищенных сетей с ограниченным доступом, сервисом подписи реализуется несколько режимов работы. В зависимости от режима работы, проверка осуществляется путем загрузки списка отозванных сертификатов из свойств самого сертификата, либо из указанного источника. В случае обнаружения проверяемого сертификата в списке, сертификат считается не действительным.

Алгоритм проверки сертификата изображен на рисунке ниже (см. Рисунок 1).

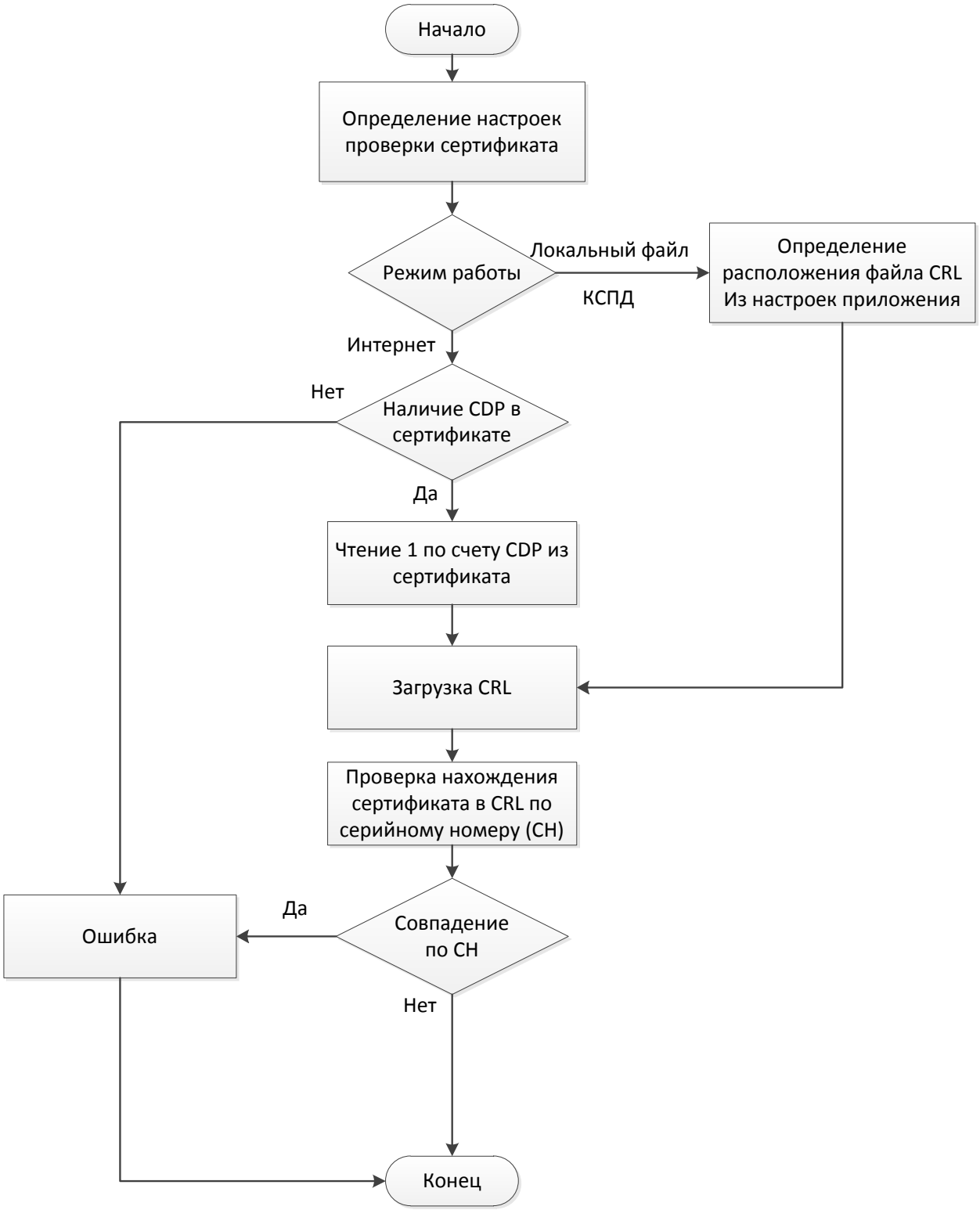

Рисунок 1 – Алгоритм проверки действительности сертификата

5.2. Создание подписи XML-сообщения.

Подпись формируется с использованием методов сертифицированных средств криптозащиты VipNet CSP и КриптоПРО CSP. Перед созданием подписи выполняется проверка действительности сертификата.

Алгоритм создания подписи изображен на рисунке ниже (см. Рисунок 2).

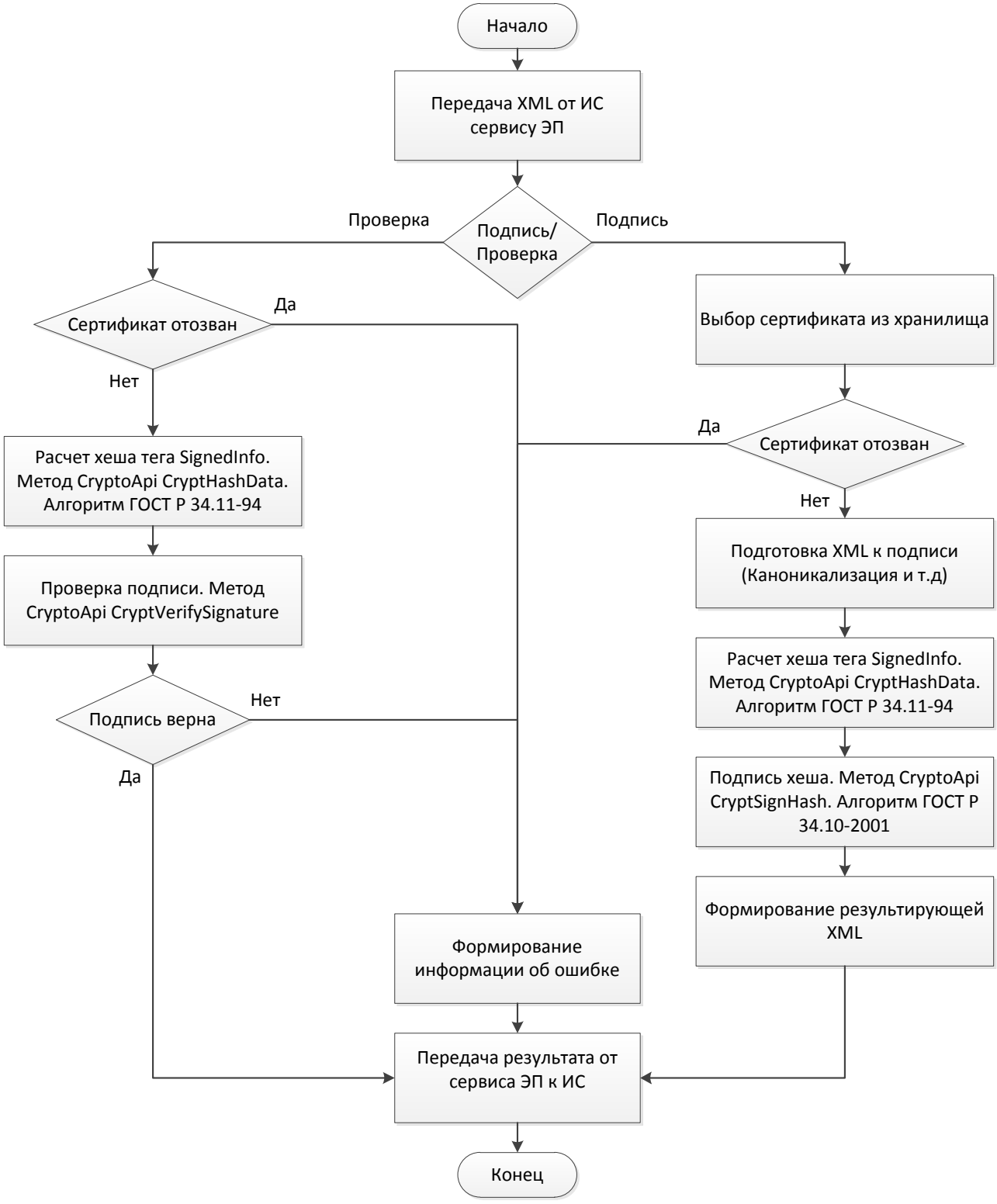

Рисунок 2 – Алгоритм создания и проверки подписи

5.3. Проверка подписи XML сообщения.

Проверка подписи основывается на проверке неизменности подписанного XML-сообщения, путем сравнения подписи сообщения с использованием методов сертифицированных средств криптозащиты VipNet CSP и КриптоПРО CSP. Подпись сообщения считается валидной и сведения достоверными, если проверка подписи пройдена.

Алгоритм проверки подписи изображен на рисунке выше (см. Рисунок 2).

6. Список используемых терминов и сокращений

Термин или сокращение	**Расшифровка**
ИС	Информационная система
ЕПГУ	Единый портал государственных и муниципальных услуг (функций)
ОМСУ	Орган местного самоуправления
РПГУ	Региональный портал государственных и муниципальных услуг (функций)
СМЭВ	Система межведомственного электронного взаимодействия
СМЭВ СО	Государственная информационная система Самарской области «Система межведомственного электронного взаимодействия»
ОИВ	Органы исполнительной власти
ЭП	Электронная подпись
РАИС МФЦ	Единая региональная автоматизированная информационная система поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг Самарской области
Веб-сервис	Электронный сервис, предназначенный для межведомственного электронного взаимодействия посредством СМЭВ

Электронный сервис	Программная система, идентифицируемая строкой URI, чьи публичные интерфейсы и привязки определены и описаны посредством XML. Описание этой программной системы может быть найдено другими программными системами, которые могут взаимодействовать с ней согласно этому описанию посредством сообщений, основанных на XML, и передаваемых с помощью Интернет-протоколов
XML	eXtensible Markup Language –текстовый формат, предназначенный для хранения структурированных данных, для обмена информацией между информационными системами
XSD	XML Schema definition - язык описания структуры XML-документа
URI	Uniform Resource Identifier - унифицированный идентификатор ресурса. Последовательность символов, идентифицирующая абстрактный или физический ресурс.
Потребитель	Участник информационного взаимодействия, выступающий в роли Потребителя информации
Поставщик	Участник информационного взаимодействия, выступающий в роли Поставщика информации
Оператор СМЭВ СО	Орган власти или организация, определенная оператором региональной системы межведомственного электронного взаимодействия в субъекте Российской Федерации в соответствии с постановлением Правительства Российской Федерации от 08.09.2010 № 697