ЕДИНАЯ АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ТАМОЖЕННЫХ ОРГАНОВ

Электронная подпись
Правила формирования и обработки в электронных документах и сообщениях

48 страниц

Редакция 3.2

Федеральная таможенная служба
Москва

СОДЕРЖАНИЕ

1. Область применения

Настоящий документ предназначен для использования при разработке программных средств и баз данных, входящих в состав Единой автоматизированной информационной системы (ЕАИС) таможенных органов, а также иных информационных систем и программных средств, предназначенных для осуществления автоматизированного информационного взаимодействия с ЕАИС таможенных органов с использованием электронной подписи (ЭП). При применении электронной подписи в ходе проектирования и разработки программных средств и баз данных требуется указывать ссылку на настоящий документ.

Объектами документа являются: структура и синтаксис XML-ЭП, правила формирования и проверки XML-ЭП. Все программные средства, входящие в состав ЕАИС таможенных органов и использующие ЭП, а также иные информационные системы и программные средства, осуществляющие информационное взаимодействие с ЕАИС таможенных органов с использованием ЭП, должны соответствовать настоящему документу.

Электронная подпись по отношению к подписываемому документу может использоваться в двух видах: оборачивающая (enveloping) и оборачиваемая (enveloped). Оборачивающая подпись содержит в себе подписываемый объект (XML-документ) и может использоваться как единственная подпись для документа. Оборачиваемая подпись содержится внутри подписываемого документа как подчиненный узел корневого узла документа (указывается в конце). Для одного XML-документа может быть указано несколько равнозначных оборачиваемых электронных подписей.

2. Нормативные ссылки

В настоящем документе использованы ссылки на следующие стандарты и нормативные документы.

ГОСТ Р 34.11 «Информационная технология. Криптографическая защита информации. Функция хэширования».

ГОСТ Р 34.10 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

ГОСТ 28147 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

XML «Extensible Markup Language (XML) 1.0 (Second Edition)». Опубликован в Интернете по адресу: http://www.w3.org/TR/RECxml.

nsXML «Namespaces in XML». Опубликован в Интернете по адресу: http://www.w3.org/TR/REC-xml-names.

XML-Schema «XML Schema Part 1: Structures» Опубликован в Интернете по адресам: http://www.w3.org/TR/xmlschema-1/ и http://www.w3.org/TR/xmlschema-2/.

XML-Schema «XML Schema Part 2: Datatypes». Опубликован в Интернете по адресам: http://www.w3.org/TR/xmlschema-1/ и http://www.w3.org/TR/xmlschema-2/.

XML-C14N «Canonical XML». Опубликован в Интернете по адресу: http://www.w3.org/TR/2001/REC-xml-c14n-20010315.

XMLDSIG-CORE «XML-Signature Syntax and Processing». Опубликован в Интернете по адресу: http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/.

RFC 2396 «Uniform Resource Identifiers (URI): Generic Syntax», August, 1998.

«Using GOST 28147-89, GOST R 34.10, and GOST R 34.11 Algorithms for XML Security». Опубликован в Интернете по адресу: https://tools.ietf.org/html/draft-chudov-cryptopro-cpxmldsig-08

XPath «XML Path Language» Version 1.0. 16 November 1999. W3C Recommendation. URL: http://www.w3.org/TR/1999/REC-xpath-19991116/

3. Определения

В настоящем документе применяются следующие термины с соответствующими определениями.

3.1. Электронное сообщение – информация, структурированная в соответствии с порядком, определенным настоящим документом, и передаваемая в рамках ЕАИС таможенных органов. Может включать в себя один или несколько электронных документов. Электронное сообщение может быть заверено электронной подписью.

3.2. Электронный документ – электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

3.3. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. В данном стандарте электронная подпись применяется к электронному XML-документу в соответствии с Федеральным законом Российской Федерации от 27.07.2017 «Об информации, информационных технологиях и о защите информации» с учетом п.1 статьи 6 Федерального закона Российской Федерации от 6.04.2017 № 63-ФЗ «Об электронной подписи» (в ред. Федеральных законов от 01.07.2011 N 169-ФЗ, от 10.07.2012 N 108-ФЗ, от 05.04.2013 N 60-ФЗ, от 02.07.2013 N 171-ФЗ, от 02.07.2013 N 185-ФЗ, от 12.03.2014 N 33-ФЗ, от 28.06.2014 N 184-ФЗ, от 30.12.2015 N 445-ФЗ, от 23.06.2016 N 220-ФЗ).

3.3. XML-документ – электронный документ в формате XML.

3.4. XML-схема (XML-Schema) – язык описания структуры документа. Предусматривает описание допустимой структуры документа и, возможно, типов данных в значениях атрибутов и содержимом элементов.

3.5. XML-ЭП – электронная подпись, представленная в виде XML-документа.

3.6. Пространство имен XML - идентифицируемая с помощью ссылки URI [RFC2396] коллекция имен, используемых в XML документах для обозначения типов элементов и именования атрибутов.

4. Обозначения и сокращения

Мн.	–	множественность;
ЭД	–	электронный документ;
ЭП	–	электронная подпись;
ISO	–	International Organization for Standardization – международная организация по стандартизации;
SOAP	–	Simple Object Access Protocol – простой протокол доступа к объектам, протокол SOAP;
URI	–	Uniform Resource Identifier – универсальный идентификатор ресурса;
W3C	–	World Wide WEB Consortium – консорциум всемирной сети;
XML	–	Extensible Markup Language – расширяемый язык разметки.
XML DSig	–	XML digital signature – международный стандарт ЭП для XML документов
PKI	–	Public Key Infrastructure – Инфраструктура открытых ключей
МЧД	–	Машино-читаемая доверенность
ПУМЧД	–	Подсистема управления машино-читаемыми доверенностями
UUID	–	Universally unique identifier «универсальный уникальный идентификатор»

5. Общие сведения о XML-ЭП

Электронная подпись – это один из способов защиты электронных документов от подделки.

Для обеспечения соответствия электронного документа равнозначным документу на бумажном носителе, подписанному собственноручной подписью уполномоченного лица, используется квалифицированная электронная подпись.

Механизм защиты электронных данных с помощью ЭП должен обеспечивать:

1) Проверку подлинности данных (защиту от искажений) – если подписанные данные были модифицированы, то это обнаружится при проверке ЭП.

2) Установление авторства (владельца подписи) – ЭП позволяет идентифицировать владельца ключа подписи, который использовался при формировании ЭП.

Для формирования ЭП используется ключ электронной подписи.

Для проверки ЭП используется соответствующий ему ключ проверки электронной подписи.

Ключ электронной подписи позволяет сформировать ЭП от лица владельца подписи. Он должен быть доступен только владельцу подписи, и храниться в тайне от посторонних.

Соответствующий ключ проверки электронной подписи может быть доступен всем. Он не позволяет сформировать ЭП от лица её владельца, но позволяет проверить целостность подписанных данных и установить идентификатор ключа электронной подписи, который использовался при формировании ЭП.

Помимо ЭП необходимо выполнять контроль за сертификатами владельцев ЭП. А именно контроль за

- подлинностью сертификата (подтверждается ЭП самого сертификата по цепочке сертификатов)
- сроком действия сертификата
- статусом сертификата (действующий, аннулированный, отозванный)
- полномочиями, указанными в сертификате для наложения ЭП на определенные виды документов

Данный стандарт описывает следующие виды ЭП

- Оборачивающая ЭП (Enveloping). В этом случае, подписываемый XML документ помещается внутри сигнатуры.
- Оборачиваемая ЭП (Enveloped). В этом случае сигнатура (одна или несколько), помещаются внутри подписываемого XML документа. Позволяет подписывать документ несколькими субъектами, а так же подписывать различные части одного документа.
    - Подписание всего XML документа в целом
    - Подписание части XML документа с использованием XPath выражения.

Правовое регулирование отношений в области использования ЭП осуществляется в соответствии с Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (в ред. Федеральных законов от 01.07.2011 N 169-ФЗ, от 10.07.2012 N 108-ФЗ, от 05.04.2013 N 60-ФЗ, от 02.07.2013 N 171-ФЗ, от 02.07.2013 N 185-ФЗ, от 12.03.2014 N 33-ФЗ, от 28.06.2014 N 184-ФЗ, от 30.12.2015 N 445-ФЗ, от 23.06.2016 N 220-ФЗ).

6. XML СХЕМА ДОКУМЕНТОВ

Оформление подписанных электронных документов должно соответствовать нижеприведенной схеме.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:ns="http://www.w3.org/2000/09/xmldsig#"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.w3.org/2000/09/xmldsig#"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.1">
      <xs:annotation>
            <xs:documentation xml:lang="ru">Описание структуры конверта
электронной подписи</xs:documentation>
      </xs:annotation>
      <xs:element name="Signature" type="ns:SignatureType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Конверт электронной
подписи.</xs:documentation>
            </xs:annotation>
      </xs:element>
      <xs:element name="Object" type="ns:ObjectType">
            <xs:annotation>
                  <xs:documentation>Данные предметной области, содержащиеся в
конверте электронной подписи.</xs:documentation>
            </xs:annotation>
      </xs:element>
      <xs:element name="SignedInfo" type="ns:SignedInfoType">
            <xs:annotation>
                  <xs:documentation>Информация, защищаемая механизмом
электронной подписи.</xs:documentation>
            </xs:annotation>
      </xs:element>
      <xs:element name="KeyInfo" type="ns:KeyInfoType">
            <xs:annotation>
                  <xs:documentation>Значение электронной
подписи.</xs:documentation>
            </xs:annotation>
      </xs:element>
      <xs:complexType name="CanonicalizationMethodType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Тип элемента информация о
методе преобразования документа перед наложением электронной
подписи.</xs:documentation>
            </xs:annotation>
            <xs:attribute name="Algorithm" type="xs:anyURI" use="required"
fixed="urn:xml-dsig:transformation:v1.1">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Алгоритм преобразования
в бинарное представление</xs:documentation>
                  </xs:annotation>
            </xs:attribute>
      </xs:complexType>
      <xs:complexType name="DigestMethodType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Информации о методе вычисления
хеш-суммы.</xs:documentation>
            </xs:annotation>
            <xs:attribute name="Algorithm" use="required">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Алгоритм формирования
хеш-суммы</xs:documentation>
                  </xs:annotation>
```

```
                  <xs:simpleType>
                        <xs:restriction base="xs:anyURI">
                              <xs:enumeration
value="http://www.w3.org/2001/04/xmldsig-more#gostr3411"/>
                              <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411"/>
                              <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256"/>
                              <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512"/>
                        </xs:restriction>
                  </xs:simpleType>
            </xs:attribute>
      </xs:complexType>
      <xs:simpleType name="DigestValueType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Хеш-сумма в
Base64.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:base64Binary"/>
      </xs:simpleType>
      <xs:complexType name="KeyInfoType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">X.509-сертификат, с помощью
которого получили ЭП документа.</xs:documentation>
            </xs:annotation>
            <xs:choice maxOccurs="unbounded">
                  <xs:element name="X509Data" type="ns:X509DataType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры X.509
сертификата.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="MCDId" minOccurs="0">
                        <xs:annotation>
                              <xs:documentation>Идентификатор доверенности
(МЧД)</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                              <xs:restriction base="xs:token">
                                    <xs:minLength value="1"/>
                                    <xs:maxLength value="36"/>
                                    <xs:pattern value="[0-9A-Fa-f]{8}-[0-9A-Fa-
f]{4}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{12}"/>
                              </xs:restriction>
                        </xs:simpleType>
                  </xs:element>
                  <xs:element name="INNPrincipal" minOccurs="0">
                        <xs:annotation>
                              <xs:documentation>ИНН юридического лица от имени
которого подписан документ</xs:documentation>
                        </xs:annotation>
                        <xs:simpleType>
                              <xs:restriction base="xs:string">
                                    <xs:pattern value="[0-9]{10}|[0-9]{12}"/>
                              </xs:restriction>
                        </xs:simpleType>
                  </xs:element>
            </xs:choice>
            <xs:attribute name="Id" type="xs:ID" use="required">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Уникальный, в пределах
конверта электронной подписи, идентификатор</xs:documentation>
                  </xs:annotation>
```

```
            </xs:attribute>
      </xs:complexType>
      <xs:complexType name="ObjectType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Данные предметной области,
содержащиеся в конверте электронной подписи.</xs:documentation>
            </xs:annotation>
            <xs:sequence>
                  <xs:any namespace="##any" processContents="skip">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Элемент. Содержит
данные предметной области, защищаемые электронной подписью</xs:documentation>
                        </xs:annotation>
                  </xs:any>
            </xs:sequence>
            <xs:attribute name="Id" type="xs:ID" use="required">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Уникальный, в пределах
конверта электронной подписи, идентификатор</xs:documentation>
                  </xs:annotation>
            </xs:attribute>
      </xs:complexType>
      <xs:complexType name="ReferenceType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Информации о заверяемых
подписью частях документа.</xs:documentation>
            </xs:annotation>
            <xs:sequence>
                  <xs:element name="Transforms" type="ns:TransformsType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Список
преобразований.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="DigestMethod" type="ns:DigestMethodType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры
формирования хеш-суммы.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="DigestValue" type="ns:DigestValueType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Значение хеш-
суммы.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
            </xs:sequence>
            <xs:attribute name="URI" type="xs:anyURI" use="required">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Адрес
элемента.</xs:documentation>
                  </xs:annotation>
            </xs:attribute>
      </xs:complexType>
      <xs:complexType name="SignatureMethodType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Информация о криптографическом
алгоритме, с помощью которого была подготовлена подпись.</xs:documentation>
            </xs:annotation>
            <xs:attribute name="Algorithm" use="required">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Содержит алгоритм
формирования электронной подписи</xs:documentation>
                  </xs:annotation>
```

```
                  <xs:simpleType>
                        <xs:restriction base="xs:anyURI">
                              <xs:enumeration
value="http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411"/>
                              <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411"/>
                              <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-
256"/>
                              <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-
512"/>
                        </xs:restriction>
                  </xs:simpleType>
            </xs:attribute>
      </xs:complexType>
      <xs:complexType name="SignatureType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Конверт электронной подписи.
Содержит защищаемые данные, значение электронной подписи и параметры
идентификации автора подписи.</xs:documentation>
            </xs:annotation>
            <xs:sequence>
                  <xs:element name="SignedInfo" type="ns:SignedInfoType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Набор данных,
защищаемый механизмом электронной подписи</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="SignatureValue"
type="ns:SignatureValueType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Значение
электронной подписи.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="KeyInfo" type="ns:KeyInfoType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры проверки
достоверности наложения электронной подписи.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="Object" type="ns:ObjectType" minOccurs="0">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Данные предметной
области для оборачивающей ЭП.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
            </xs:sequence>
      </xs:complexType>
      <xs:simpleType name="SignatureValueType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Значение электронной
подписи.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:base64Binary"/>
      </xs:simpleType>
      <xs:complexType name="SignedInfoType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Информация о подписываемом
объекте.</xs:documentation>
            </xs:annotation>
            <xs:sequence>
```

```
                  <xs:element name="CanonicalizationMethod"
type="ns:CanonicalizationMethodType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры
преобразования элемента SignedInfo перед наложением электронной
подписи</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="SignatureMethod"
type="ns:SignatureMethodType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры
наложения электронной подписи</xs:documentation>
                        </xs:annotation>
                  </xs:element>
                  <xs:element name="Reference" type="ns:ReferenceType"
minOccurs="2" maxOccurs="2">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры проверки
неизменности данных</xs:documentation>
                        </xs:annotation>
                  </xs:element>
            </xs:sequence>
      </xs:complexType>
      <xs:complexType name="TransformType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Преобразования над
пописываемой частью документа.</xs:documentation>
            </xs:annotation>
            <xs:attribute name="Algorithm" use="required">
                  <xs:annotation>
                        <xs:documentation xml:lang="ru">Атрибут. Содержит
алгоритм преобразования</xs:documentation>
                  </xs:annotation>
                  <xs:simpleType>
                        <xs:restriction base="xs:anyURI">
                              <xs:enumeration value="urn:xml-
dsig:transformation:v1.1"/>
                              <xs:enumeration
value="http://www.w3.org/TR/1999/REC-xpath-19991116"/>
                        </xs:restriction>
                  </xs:simpleType>
            </xs:attribute>
      </xs:complexType>
      <xs:complexType name="TransformsType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Список применяемых к
подписываемому объекту преобразований.</xs:documentation>
            </xs:annotation>
            <xs:sequence>
                  <xs:element name="Transform" maxOccurs="unbounded">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Параметры
преобразования части документа перед формированием хеш-суммы</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                              <xs:complexContent>
                                    <xs:extension base="ns:TransformType">
                                          <xs:sequence minOccurs="0">
                                                <xs:element name="XPath"
type="xs:string" fixed="not(ancestor-or-self::dsig:Signature)">
                                                      <xs:annotation>
```

```
      <xs:documentation>XPath для алгоритма трансформации
http://www.w3.org/TR/1999/REC-xpath-19991116</xs:documentation>
                                                        </xs:annotation>
                                                  </xs:element>
                                            </xs:sequence>
                                      </xs:extension>
                                </xs:complexContent>
                          </xs:complexType>
                    </xs:element>
              </xs:sequence>
      </xs:complexType>
      <xs:complexType name="X509DataType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Параметры X.509
сертификата.</xs:documentation>
            </xs:annotation>
            <xs:sequence>
                  <xs:element name="X509Certificate"
type="ns:X509CertificateType">
                        <xs:annotation>
                              <xs:documentation xml:lang="ru">Бинарное
представление X.509 сертификата.</xs:documentation>
                        </xs:annotation>
                  </xs:element>
            </xs:sequence>
      </xs:complexType>
      <xs:simpleType name="X509CertificateType">
            <xs:annotation>
                  <xs:documentation xml:lang="ru">Бинарное представление X.509
сертификата.</xs:documentation>
            </xs:annotation>
            <xs:restriction base="xs:base64Binary"/>
      </xs:simpleType>
</xs:schema>
```

7. Виды подписи по отношению к подписанному документу

В описании структуры ЭП, а также в алгоритмах наложения и проверки ЭП могут быть уточнения к какому из видов подписи относится тот или иной элемент, применен тот или иной алгоритм.

7.1. Оборачивающая (Enveloping)

Вид электронной подписи которая содержит объект подписи внутри себя (см. Рисунок 1). Данный вид ЭП используется для подписания документа одним лицом. Оборачивающая подпись полностью совместима с ЭП, использовавшейся в предыдущей редакции стандарта.

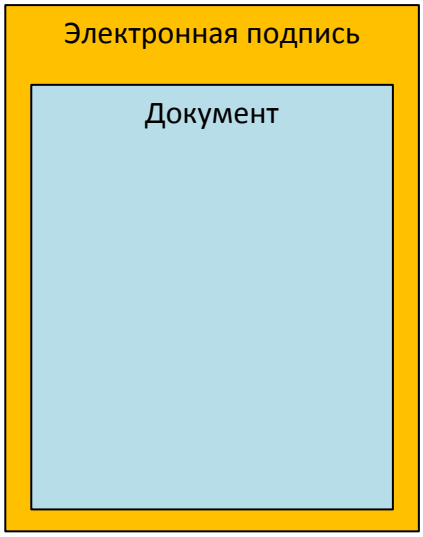

Рисунок 1. Оборачивающая электронная подпись

7.2. Оборачиваемая (Enveloped)

Вид электронной подписи, которая внедрена в сам подписываемый документ (см. Рисунок 2). Такой тип ЭП рекомендуется использовать для формирования нескольких равнозначных подписей на один документ. Для исключения самой подписи из расчета используется XPath трансформация, исключающая элементы Signature, подчиненные корневому элементу документа.

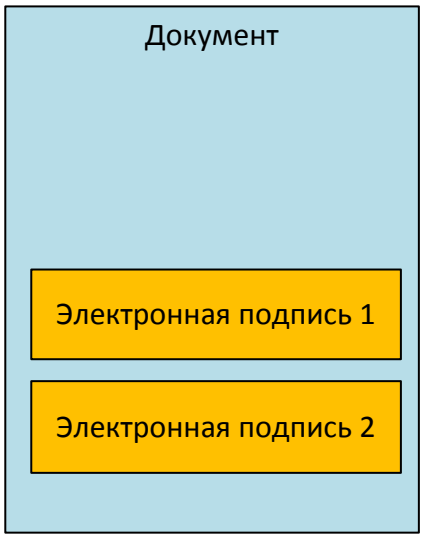

Рисунок 2. Оборачиваемая электронная подпись

8. Описание элементов XML-схемы

8.1. Элемент Signature

Элемент Signature объединяет в себе подписываемые данные и значение ЭП.

8.1.1. Пространство имен

Элемент Signature Должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#»

8.1.2. Атрибуты

Элемент Signature атрибутов не имеет.

8.1.3. Дочерние узлы

Элемент Signature содержит следующие дочерние элементы:

1) SignedInfo – Информацию о подписываемом объекте;

2) *KeyInfo* –X.509-сертификат и информация о МЧД.

3) *SignatureValue* – содержит обозначение ЭП.

4) *Object* – XML-Документ

8.1.4. Соответствующий элемент XML-схемы

```
<xs:element name="Signature" type="ns:SignatureType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Конверт электронной
подписи.</xs:documentation>
  </xs:annotation>
</xs:element>

<xs:complexType name="SignatureType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Конверт электронной подписи. Содержит
защищаемые данные, значение электронной подписи и параметры идентификации автора
подписи.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="SignedInfo" type="ns:SignedInfoType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Набор данных, защищаемый механизмом
электронной подписи</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="SignatureValue" type="ns:SignatureValueType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Значение электронной
подписи.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="KeyInfo" type="ns:KeyInfoType">
```

```
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры проверки достоверности
наложения электронной подписи.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="Object" type="ns:ObjectType" minOccurs="0">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Данные предметной области для
оборачивающей ЭП.</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

Рисунок 3 Элемент Signature

8.2. Элемент SignedInfo

Элемент SignedInfo содержит информацию о подписываемом объекте.

8.2.1. Пространство имен

Элемент Signature Должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.2.2. Атрибуты

Элемент SignedInfo атрибутов не имеет.

8.2.3. Дочерние узлы

CanonicalizationMethod – метод преобразования SignedInfo к канонической форме.

1) *SignatureMethod* – алгоритм формирования ЭП.

2) *Reference* – Ссылка на элемент документа, для которого вычисляется хеш-сумма. Элементов *Reference* должно быть два. Первый элемент *Reference* должен ссылаться на элемент *KeyInfo*. Второй элемент *Reference* должен ссылаться на элемент *Object* для оборачивающей ЭП или на элемент документа, полученный в результате трансформаций для оборачиваемой ЭП.

8.2.4. Соответствующий элемент XML схемы

```
<xs:element name="SignedInfo" type="ns:SignedInfoType">
  <xs:annotation>
    <xs:documentation>Информация, защищаемая механизмом электронной
подписи.</xs:documentation>
  </xs:annotation>
</xs:element>

<xs:complexType name="SignedInfoType">
```

```
  <xs:annotation>
    <xs:documentation xml:lang="ru">Информация о подписываемом
объекте.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="CanonicalizationMethod"
type="ns:CanonicalizationMethodType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры преобразования элемента
SignedInfo перед наложением электронной подписи</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="SignatureMethod" type="ns:SignatureMethodType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры наложения электронной
подписи</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="Reference" type="ns:ReferenceType" minOccurs="2"
maxOccurs="2">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры проверки неизменности
данных</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

Рисунок 4 Элемент SignedInfo

8.3. Элемент CanonicalizationMethod

Элемент CanonicalizationMethod содержит информацию об алгоритме приведения содержимого элемента SignedInfo к канонической форме.

Приведение к канонической форме XML-документа должно проводиться в соответствии с алгоритмом «urn:xml-dsig:transformation:v.1.1» (описан в соответствующем разделе данного стандарта).

8.3.1. Пространство имен

Элемент CanonicalizationMethod должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.3.2. Атрибуты

Algorithm – должен иметь фиксированное значение «urn:xml-dsig:transformation:v1.1».

8.3.3. Дочерние узлы

Дочерние узлы отсутствуют.

8.3.4. Соответствующий элемент XML схемы

```
<xs:complexType name="CanonicalizationMethodType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Тип элемента информация о методе
преобразования документа перед наложением электронной
подписи.</xs:documentation>
  </xs:annotation>
  <xs:attribute name="Algorithm" type="xs:anyURI" use="required" fixed="urn:xml-
dsig:transformation:v1.1">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Алгоритм преобразования в бинарное
представление</xs:documentation>
    </xs:annotation>
  </xs:attribute>
</xs:complexType>
```

Рисунок 5 Элемент CanonicalizationMethod

8.4. Элемент SignatureMethod

Элемент SignatureMethod содержит информацию об алгоритме, который используется для вычисления ЭП. Идентификатор данного алгоритма задается в атрибуте Algorithm.

8.4.1. Пространство имен

Элемент SignatureMethod должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.4.2. Атрибуты

Algorithm – идентификатор алгоритма, используемого для вычисления ЭП. Может иметь два варианта значений

- «http://www.w3.org/2001/04/xmldisig-more#gostr34102001-gostr3411» при использовании алгоритма в соответствии с ГОСТ Р 34.10-2001
- «http://www.w3.org/2001/04/xmldsig-more#gostr34102012-gostr34112012» при использовании алгоритма в соответствии с ГОСТ Р 34.10-2012

Должен быть задан явно.

8.4.3. Дочерние узлы

Дочерние узлы отсутствуют.

8.4.4. Соответствующий элемент XML схемы

```
<xs:complexType name="SignatureMethodType">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Информация о криптографическом алгоритме,
с помощью которого была подготовлена подпись.</xs:documentation>
    </xs:annotation>
    <xs:attribute name="Algorithm" use="required">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Содержит алгоритм формирования
электронной подписи</xs:documentation>
      </xs:annotation>
      <xs:simpleType>
        <xs:restriction base="xs:anyURI">
          <xs:enumeration value="http://www.w3.org/2001/04/xmldsig-
more#gostr34102001-gostr3411"/>
          <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411"/>
          <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-
256"/>
          <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-
512"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:complexType>
```

Рисунок 6 Элемент SignatureMethod

8.5. Элемент Reference

Элемент Reference сопоставляет элементу XML-документа хеш-код, гарантирующий неизменность указанной части XML-документа, дополненный информацией, необходимой для повторного вычисления хеш-кода.

Значением атрибута URL является ссылка на Id сопоставляемого элемента. Во всей XML-ЭП существует два элемента Reference, первый сопоставлен элементу KeyInfo, а второй, в зависимости от вида подписи или на элемент Object (для оборачивающей) или на корневой элемент документа (для оборачиваемой). Первый элемент Reference, заданный в элементе SignedInfo, сопоставляется элементу KeyInfo, поэтому значение атрибута URI первого элемента Reference должно ссылаться на элемент KeyInfo. Если второй элемент Reference сопоставляется элементу Object, то значение атрибута URI второго элемента Reference должно ссылаться на атрибут Id элемента Object, если второй элемент Reference сопоставляется корневому элементу документа, то значение атрибута URI должно быть равно пустому значению "". Не пустое значение атрибута URI формируется из суммы префикса «#» и значения атрибута Id указываемого элемента.

В дочерних элементах Transforms, DigestMethod и DigestValue содержится информация о преобразовании документа перед вычислением хеш-суммы, метода вычисления хеш-суммы, и значение хеш-суммы.

8.5.1. Пространство имен

Элемент Reference должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#»

8.5.2. Атрибуты

URI – Ссылка на сопоставляемый хеш-сумме элемент.

8.5.3. Дочерние узлы

Transforms – Список трансформаций, которые должны быть применены к заданному элементу XML-ЭП перед вычислением хеш-суммы.

1) *DigestMethod* – метод вычисления хеш-суммы.

2) *DigestValue* – хеш-сумма трансформированной версии элемента указанного в атрибуте URI, вычисленная по алгоритму, задаваемому в элементе *DigestMethod*.

8.5.4. Соответствующий элемент XML схемы

```
<xs:complexType name="ReferenceType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Информации о заверяемых подписью частях
документа.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Transforms" type="ns:TransformsType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Список
преобразований.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="DigestMethod" type="ns:DigestMethodType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры формирования хеш-
суммы.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="DigestValue" type="ns:DigestValueType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Значение хеш-суммы.</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
  <xs:attribute name="URI" type="xs:anyURI" use="required">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Адрес элемента.</xs:documentation>
    </xs:annotation>
```

```
  </xs:attribute>
</xs:complexType>
```

Рисунок 7 Элемент Reference

8.6. Элемент Transforms

Элемент Transforms содержит список преобразований документа, которые необходимо выполнить для узла документа, указываемого значением атрибута URI, для вычисления значения элемента DigestValue в соответствии с алгоритмом, определяемым значением атрибута Algorithm элемента DigestMethod.

8.6.1. Пространство имен

Элемент Transforms должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#»

8.6.2. Атрибуты

Элемент Transforms атрибутов не имеет.

8.6.3. Дочерние узлы

Transform – элемент, определяющий преобразование, которое необходимо применить перед вычислением значения хеш-суммы.

Для оборачиваемой ЭП, при подписании всего XML документа, используется два элемента Transform, в первом из них указывается алгоритм преобразования «http://www.w3.org/TR/1999/REC-xpath-19991116», позволяющий исключить из расчета хэш-суммы элементов оборачиваемой подписи(ей), а во втором алгоритм «urn:xml-dsig:transformation:v1.1».

Для оборачиваемой ЭП, при подписании части XML документа, используется три элемента Transform, в первом из них указывается алгоритм преобразования «http://www.w3.org/TR/1999/REC-xpath-19991116», позволяющий исключить из расчета хэш-суммы элементов оборачиваемой подписи(ей), во втором так же указывается алгоритм преобразования «http://www.w3.org/TR/1999/REC-xpath-19991116», но с указанием XPath выражения в дочернем элементе, отбирающий нужную часть документа для подписи, и в третьем алгоритм «urn:xml-dsig:transformation:v1.1».

Для оборачивающей ЭП достаточно указать только алгоритм «urn:xml-dsig:transformation:v1.1».

8.6.4. Соответствующий элемент XML схемы

```
<xs:complexType name="TransformsType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Список применяемых к подписываемому объекту
преобразований.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Transform" maxOccurs="unbounded">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры преобразования части документа
перед формированием хеш-суммы</xs:documentation>
      </xs:annotation>
      <xs:complexType>
        <xs:complexContent>
          <xs:extension base="ns:TransformType">
            <xs:sequence minOccurs="0">
              <xs:element name="XPath" type="xs:string" fixed="not(ancestor-or-
self::dsig:Signature)">
                <xs:annotation>
                  <xs:documentation>XPath для алгоритма трансформации
http://www.w3.org/TR/1999/REC-xpath-19991116</xs:documentation>
                </xs:annotation>
              </xs:element>
            </xs:sequence>
          </xs:extension>
        </xs:complexContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

Рисунок 8 Элемент Transforms

8.7. Элемент Transform

Элемент Transform определяет преобразование, которое необходимо совершить над элементом, указываемым при помощи атрибута URI родительского элемента Reference.

8.7.1. Пространство имен

Элемент Transform должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.7.2. Атрибуты

Элемент трансформ должен иметь обязательный атрибут Algorithm с одним из значений:

- «http://www.w3.org/TR/1999/REC-xpath-19991116», используется только для оборачиваемых ЭП.
- «urn:xml-dsig:transformation:v1.1».

8.7.3. Дочерние узлы

Элемент XPath – предназначен для указания XPath выражения, либо исключающего расчет хэш-суммы по всем узлам Signature, указанных в документе, в этом случае значение заполняется как «not(ancestor-or-self::dsig:Signature)», либо указывающего узел, для которого будет рассчитана хэш-сумма для наложения ЭП на часть XML документа. Узел заполняется при указании алгоритма трансформации «http://www.w3.org/TR/1999/REC-xpath-19991116». Используется только для оборачиваемой ЭП.

8.7.4. Соответствующий элемент XML схемы

```
<xs:complexType name="TransformType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Преобразования над пописываемой частью
документа.</xs:documentation>
  </xs:annotation>
  <xs:attribute name="Algorithm" use="required">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Атрибут. Содержит алгоритм
преобразования</xs:documentation>
    </xs:annotation>
    <xs:simpleType>
      <xs:restriction base="xs:anyURI">
        <xs:enumeration value="urn:xml-dsig:transformation:v1.1"/>
        <xs:enumeration value="http://www.w3.org/TR/1999/REC-xpath-19991116"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:complexType>
```

Рисунок 9 Элемент Transform

8.8. Элемент DigestMethod

Элемент DigestMethod определяет метод вычисления хеш-суммы.

8.8.1. Пространство имен

Элемент DigestMethod должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.8.2. Атрибуты

Элемент DigestMethod должен иметь атрибут Algorithm с одним из значений

- «http://www.w3.org/2001/04/xmldsig-more#gostr3411» (или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), при

использовании алгоритма вычисления хэш-суммы по стандарту ГОСТ Р 34.11-94

- «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256», при использовании алгоритма вычисления хэш-суммы по стандарту ГОСТ Р 34.11-2012 с длиной ключа 256 бит.
- «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512», при использовании алгоритма вычисления хэш-суммы по стандарту ГОСТ Р 34.11-2012 с длиной ключа 256 бит.

8.8.3. Дочерние узлы

Элемент DigestMethod дочерних узлов не имеет.

8.8.4. Соответствующий элемент XML схемы

```
<xs:complexType name="DigestMethodType">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Информации о методе вычисления хеш-
суммы.</xs:documentation>
    </xs:annotation>
    <xs:attribute name="Algorithm" use="required">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Алгоритм формирования хеш-
суммы</xs:documentation>
      </xs:annotation>
      <xs:simpleType>
        <xs:restriction base="xs:anyURI">
          <xs:enumeration value="http://www.w3.org/2001/04/xmldsig-
more#gostr3411"/>
          <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411"/>
          <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256"/>
          <xs:enumeration
value="urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:complexType>
```

Рисунок 10 Элемент DigestMethod

8.9. Элемент DigestValue

8.9.1. Пространство имен

Элемент DigestValue содержит значение хеш-суммы, вычисляемой для результата преобразования элемента, указываемого при помощи значения атрибута URI, родительского элемента Reference.

8.9.2. Атрибуты

Элемент DigestValue атрибутов не имеет.

8.9.3. Дочерние узлы

Элемент DigestValue содержит текстовый узел, являющийся значением хеш-суммы.

Хеш-сумма кодируется по алгоритму Base64, после чего, из полученной строки удаляются все символы, не входящие в алфавит Base64. Пробельные символы недопустимы.

8.9.4. Соответствующий элемент XML схемы

```
<xs:simpleType name="DigestValueType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Хеш-сумма в Base64.</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:base64Binary"/>
</xs:simpleType>
```

Рисунок 11 Элемент DigestValue

8.10. Элемент KeyInfo

Элемент KeyInfo содержит ключевую информацию, используемую для проверки ЭП. Данная информация должна быть представлена в виде X.509-сертификата ключа, использованного для подписи XML-документа и идентификатора МЧД в виде UUID.

Хранящаяся в элементе KeyInfo информация должна быть включена в список объектов, которые защищаются ЭП. Таким образом, часть служебной информации XML-ЭП будет заверена этой же самой ЭП.

8.10.1. Пространство имен

Элемент KeyInfo должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.10.2. Атрибуты

Id – обязательный атрибут. Значение атрибута Id используется для ссылки на элемент KeyInfo из элемента Reference. Поле Id должно быть уникальным в пределах XML-ЭП, за исключением элементов самого подписываемого документа.

8.10.3. Дочерние узлы

Элемент KeyInfo имеет три дочерних элемента X509Data, MCDId и INNPrincipal. Два последних элемента заполняются только при необходимости прикладывать МЧД для удостоверения полномочий подписавшего лица.

8.10.4. Соответствующий элемент XML схемы

```
<xs:complexType name="KeyInfoType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">X.509-сертификат, с помощью которого
получили ЭП документа.</xs:documentation>
  </xs:annotation>
  <xs:choice maxOccurs="unbounded">
    <xs:element name="X509Data" type="ns:X509DataType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Параметры X.509
сертификата.</xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="MCDId" minOccurs="0">
      <xs:annotation>
        <xs:documentation>Идентификатор доверенности (МЧД)</xs:documentation>
      </xs:annotation>
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:minLength value="1"/>
          <xs:maxLength value="36"/>
          <xs:pattern value="[0-9A-Fa-f]{8}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{4}-[0-9A-
Fa-f]{4}-[0-9A-Fa-f]{12}"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="INNPrincipal" minOccurs="0">
      <xs:annotation>
        <xs:documentation>ИНН юридического лица от имени которого подписан
документ</xs:documentation>
      </xs:annotation>
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:pattern value="[0-9]{10}|[0-9]{12}"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:choice>
  <xs:attribute name="Id" type="xs:ID" use="required">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Уникальный, в пределах конверта
электронной подписи, идентификатор</xs:documentation>
    </xs:annotation>
  </xs:attribute>
</xs:complexType>
```

Рисунок 12 Элемент KeyInfo

8.11. Элемент X509Data

8.11.1. Пространство имен

Элемент X509Data должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.11.2. Атрибуты

Элемент X509Data атрибутов не имеет.

8.11.3. Дочерние узлы

Элемент X509Data содержит дочерний элемент с именем X509Certificate.

8.11.4. Соответствующий элемент XML схемы

```
<xs:complexType name="X509DataType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Параметры X.509
сертификата.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="X509Certificate" type="ns:X509CertificateType">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Бинарное представление X.509
сертификата.</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

8.12. Рисунок 13 Элемент X509DataX509Certificate

Элемент X509Certificate содержит закодированный в соответствии с алгоритмом «http://www.w3.org/2000/09/xmldisg#base64» квалифицированный сертификат пользователя[1] (X.509 версии 3), подписавшего XML-документ.

8.12.1. Пространство имен

Элемент X509Certificate должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.12.2. Атрибуты

Элемент X509Certificate атрибутов не имеет.

[1] В соответствии с приказом ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи"

8.12.3. Дочерние узлы

Дочерним узлом элемента является текстовый узел, содержащий X509-сертификат закодированный в соответствии с алгоритмом «http://www.w3.org/2000/09/xmldisg#base64». В текстовом узле элемента X509Certificate могут содержаться только символы алфавита Base64, пробельные символы недопустимы. Сам сертификат должен быть указан в DER кодировке (до кодирования в Base64).

8.12.4. Соответствующий элемент XML схемы

```
<xs:simpleType name="X509CertificateType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Бинарное представление X.509
сертификата.</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:base64Binary"/>
</xs:simpleType>
```

Рисунок 14 Элемент X509Certificate

8.13. Элемент MCDId

8.13.1. Пространство имен

Элемент MCDId должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.13.2. Атрибуты

Элемент MCDId атрибутов не имеет.

8.13.2.1 Дочерние узлы

Дочерним узлом элемента является текстовый узел, содержащий UUID идентификатор МЧД

8.13.3. Соответствующий элемент XML схемы

```
<xs:element name="MCDId" minOccurs="0">
  <xs:annotation>
    <xs:documentation>Идентификатор доверенности (МЧД)</xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:token">
      <xs:minLength value="1"/>
      <xs:maxLength value="36"/>
```

```
      <xs:pattern value="[0-9A-Fa-f]{8}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{4}-[0-9A-Fa-
f]{4}-[0-9A-Fa-f]{12}"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
```

Рисунок 155 Элемент MCDId

8.14. Элемент INNPrincipal

8.14.1. Пространство имен

Элемент INNPrincipal должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.14.2. Атрибуты

Элемент INNPrincipal атрибутов не имеет.

8.14.2.1 Дочерние узлы

Дочерним узлом элемента является текстовый узел, ИНН юридического лица доверителя (10 цифр)

8.14.3. Соответствующий элемент XML схемы

```
<xs:element name="INNPrincipal" minOccurs="0">
  <xs:annotation>
    <xs:documentation>ИНН юридического лица от имени которого подписан
документ</xs:documentation>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]{10}|[0-9]{12}"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
```

Рисунок 166 Элемент INNPrincipal

8.15. Элемент SignatureValue

Элемент SignatureValue содержит обозначение ЭП, которое должно быть получено как результат вычисления функции криптографического преобразования элемента SignedInfo, преобразованного в соответствии с алгоритмом, указанным в элементе CanonicalizationMethod. Информация об идентификаторе алгоритма данного криптографического преобразования содержится в элементе SignedInfo.

8.15.1. Пространство имен

Элемент SignatureValue должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.15.2. Атрибуты

Элемент SignatureValue атрибутов не имеет.

8.15.3. Дочерние узлы

Дочерним узлом SignatureValue является текстовый узел, содержащий данные, закодированный в соответствии с алгоритмом «http://www.w3.org/2000/09/xmldisg#base64». В текстовом узле элемента SignatureValue могут содержаться только символы алфавита Base64, пробельные символы недопустимы.

8.15.4. Соответствующий элемент XML схемы

```
<xs:simpleType name="SignatureValueType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Значение электронной
подписи.</xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:base64Binary"/>
</xs:simpleType>
```

Рисунок 177 Элемент SignatureValue

8.16. Элемент Object

Для оборачивающей ЭП элемент содержит исходный (подписываемый) XML-документ, для оборачиваемой ЭП элемент не заполняется.

8.16.1. Пространство имен

Элемент Object должен находиться в пространстве имен «http://www.w3.org/2000/09/xmldsig#».

8.16.2. Атрибуты

Id – Уникальный идентификатор элемента.

8.16.3. Дочерние элементы

Элемент Object должен иметь один дочерний элемент, который является либо корневым элементом XML-документа, либо текстовым узлом.

8.16.4. Соответствующий элемент XML схемы

```
<xs:element name="Object" type="ns:ObjectType">
  <xs:annotation>
    <xs:documentation>Данные предметной области, содержащиеся в конверте
электронной подписи.</xs:documentation>
  </xs:annotation>
</xs:element>

<xs:complexType name="ObjectType">
  <xs:annotation>
    <xs:documentation xml:lang="ru">Данные предметной области, содержащиеся в
конверте электронной подписи.</xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:any namespace="##any" processContents="skip">
      <xs:annotation>
        <xs:documentation xml:lang="ru">Элемент. Содержит данные предметной
области, защищаемые электронной подписью</xs:documentation>
      </xs:annotation>
    </xs:any>
  </xs:sequence>
  <xs:attribute name="Id" type="xs:ID" use="required">
    <xs:annotation>
      <xs:documentation xml:lang="ru">Уникальный, в пределах конверта
электронной подписи, идентификатор</xs:documentation>
    </xs:annotation>
  </xs:attribute>
</xs:complexType>
```

Рисунок 188. Элементы Object

9. Алгоритм формирования XML-ЭП

Формирование XML-документа с ЭП состоит из следующих этапов:

1. Формирование шаблона документа

1.1. Создается элемент *Signature*

1.2. Для оборачиваемой ЭП элемент *Signature* добавляется как последний дочерний элемент корневого элемента документа.

1.3. К элементу *Signature* добавляется дочерний элемент *SignedInfo*

1.4. К элементу *SignedInfo* добавляется дочерний элемент *CanonicalizationMethod*

1.5. К элементу *SignedInfo* добавляется дочерний элемент *SignatureMethod*

1.6. К элементу *SignedInfo* добавляется первый дочерний элемент *Reference*

1.7. К первому элементу *Reference* добавляется дочерний элемент *Transforms*

1.8. К элементу *Transforms* первого элемента *Reference* добавляется дочерний элемент *Transform*

1.9. К первому элементу *Reference* добавляется элемент *DigestMethod*

1.10. К первому элементу *Reference* добавляется элемент *DigestValue*

1.11. К элементу *SignedInfo* добавляется второй дочерний элемент *Reference*

1.12. Ко второму элементу *Reference* добавляется элемент *Transforms*

1.13. Для оборачиваемой ЭП к элементу *Transforms* второго элемента *Reference* добавляется дочерний элемент *Transform* к которому добавляется элемент *XPath*.

1.14. Для оборачиваемой ЭП, в случае необходимости подписать часть XML документа, к элементу *Transforms* второго элемента *Reference* добавляется дочерний элемент *Transform* к которому добавляется элемент *XPath*.

1.15. К элементу *Transforms* второго элемента *Reference* добавляется дочерний элемент *Transform*

1.16. Ко второму элементу *Reference* добавляется элемент *DigestMethod*

1.17. Ко второму элементу *Reference* добавляется элемент *DigestValue*

1.18. К элементу *Signature* добавляется дочерний элемент *SignatureValue*

1.19. К элементу *Signature* добавляется дочерний элемент *KeyInfo*

1.20. К элементу *KeyInfo* добавляется дочерний элемент *X509Data*

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

1.22. Добавление сведений о МЧД. Осуществляется, если дата начала действия сертификата с 01.09.2023, не заполнен атрибут ИНН юридического лица (INNLE, OID: 1.2.643.100.4) и на прикладном уровне требуется наличие МЧД. Дополнительно ограничения по указанию МЧД могут накладываться спецификацией взаимодействия между ИС. Для добавления информации по МЧД

1.22.1. К элементу *KeyInfo* добавляется дочерний элемент *MCDId* с указанием идентификатора МЧД

1.22.2. К элементу *KeyInfo* добавляется дочерний элемент *INNPrincipal* с указанием ИНН доверителя

1.23. К элементу *Signature* добавляется дочерний элемент *Object*

2. Установка предопределенных значений

2.1. Для элемента *CanonicalizationMethod* значение атрибута *Algorithm* устанавливается в «urn:xml-dsig:transformation:v1.1»

2.2. Для элемента *Transform* первого элемента *Reference* значение атрибута *Algorithm* устанавливается в «urn:xml-dsig:transformation:v1.1»

2.3. Для оборачиваемой подписи, при подписании всего XML документа атрибуту *Algorithm* первого элемента *Transform* второго элемента *Reference* устанавливается значение «http://www.w3.org/TR/1999/REC-xpath-19991116», а элементу XPath значение «not(ancestor-or-self::dsig:Signature)». Атрибуту *Algorithm* второго элемента *Transform* второго элемента *Reference* устанавливается значение «urn:xml-dsig:transformation:v1.1»

2.4. Для оборачиваемой подписи, при подписании части XML документа атрибуту *Algorithm* второго элемента *Transform* второго элемента *Reference* устанавливается значение «http://www.w3.org/TR/1999/REC-xpath-19991116», а элементу XPath значение определяющее узел XML документа, содержимое которого будет подписано. Если XPath выражение возвращает набор узлов, то для подписи отбирается только первый из них. Атрибуту *Algorithm* третьего элемента *Transform* второго элемента *Reference* устанавливается значение «urn:xml-dsig:transformation:v1.1»

2.5. Для оборачивающей подписи атрибуту *Algorithm* элемента *Transform* второго элемента *Reference* устанавливается значение «urn:xml-dsig:transformation:v1.1»

2.6. Для элементов DigestMethod первого и второго элементов Reference значения атрибута Algorithm устанавливается в одно из значений «http://www.w3.org/2001/04/xmldsig-more#gostr3411» (возможно использование «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512» в зависимости от используемого алгоритма ГОСТ Р при вычислении хэш-суммы и используемой длины ключа.

2.7. Для элемента SignatureMethod в зависимости от используемого алгоритма ГОСТ Р для наложения ЭП значение атрибута Algorithm устанавливается в одно из значений

- При использовании стандарта ГОСТ Р 34.10-2001 «http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411» или допустимо указание «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411».
- При использовании ГОСТ Р 34.10-2012 в зависимости от размера ключа
    - Для ключа длиной 256 бит - «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-256»
    - Для ключа длиной 512 бит - «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-512»

2.8. Выбирается уникальный идентификатор, отвечающий правилам для формирования идентификаторов, для связи первого элемента Reference и элемента KeyInfo. Рекомендуется использовать значение «#KeyInfo».

2.9. Атрибут URI первого элемента Reference и атрибут Id элемента KeyInfo заполняются выбранным уникальным значением («#KeyInfo»).

2.10. Для оборачивающей ЭП выбирается уникальный идентификатор, отвечающий правилам для формирования идентификаторов, для связи второго элемента *Reference* и элемента *Object*. Рекомендуется использовать значение («#InputData»).

2.11. Для оборачивающей ЭП атрибут URI второго элемента Reference и атрибут Id элемента Object заполняются выбранным уникальным значением идентификатора («#InputData»).

2.12. Для оборачиваемой ЭП атрибут URI второго элемента Reference не заполняется, что означает, что ссылка идет на корневой элемент XML документа.

3. Установка подписываемой части для оборачивающей ЭП

3.1. К элементу Object добавляется дочерний элемент, являющийся корневым элементом подписываемого xml-документа.

4. Установка подписи

4.1. Квалифицированный сертификат подписи, содержащий открытый ключ, 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.

4.2. Для оборачивающей ЭП элемент Object трансформируется в соответствии с алгоритмом «urn:xml-dsig:transformation:v1.1», для полученной строки вычисляется хеш-сумма в соответствии с выбранным алгоритмом «http://www.w3.org/2001/04/xmldsig-more#gostr3411» («urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512». Полученное значение кодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64» и добавляется как дочерний текстовый узел к элементу DigestValue второго элемента Reference.

4.3. Для оборачиваемой ЭП корневой элемент документа трансформируется сначала по алгоритму «http://www.w3.org/TR/1999/REC-xpath-19991116» с использованием условия «not(ancestor-or-self::dsig:Signature)», то есть исключаются все элементы Signature из XML документа, затем, если необходимо подписать часть

XML документа, используя XPath выражение (алгоритм «http://www.w3.org/TR/1999/REC-xpath-19991116») выбирается конкретный узел в документе, иначе используется корневой узел документа, затем результат трансформируется в соответствии с алгоритмом «urn:xml-dsig:transformation:v1.1», для полученной строки вычисляется хеш-сумма в соответствии с выбранным алгоритмом «http://www.w3.org/2001/04/xmldsig-more#gostr3411» («urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512». Полученное значение кодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64» и добавляется как дочерний текстовый узел к элементу DigestValue второго элемента Reference.

4.4. Элемент KeyInfo трансформируется в соответствии с алгоритмом «urn:xml-dsig:transformation:v1.1», для полученной строки вычисляется хеш-сумма в соответствии с выбранным алгоритмом «http://www.w3.org/2001/04/xmldsig-more#gostr3411» («urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512». Полученное значение кодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64», все символы, не входящие в алфавит Base64 удаляются и полученная строка добавляется как дочерний текстовый узел к элементу DigestValue первого элемента Reference.

4.5. При наличии настройки на сервер доверенного времени (TSP). Осуществляется обращение к серверу доверенного времени в соответствии со стандартом RFC3161. Полученное значение времени кодируется в соответствии с алгоритмом PKCS_7_ASN_ENCODING | X509_ASN_ENCODING.

4.6. Элемент SignedInfo трансформируется в соответствии с алгоритмом «urn:xml-dsig:transformation:v1.1». Затем на основании полученной строки, закодированного времени подписи и ключа подписи формируется значение ЭП в соответствии с выбранным алгоритмом ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012, а так же в соответствии с выбранной длинной ключа для второго алгоритма. Полученное значение ЭП кодируется в соответствии с алгоритмом Base64, символы,

не входящие в алфавит Base64, удаляются и полученное значение добавляется как дочерний текстовый узел к элементу SignatureValue.

10. Алгоритм проверки XML-ЭП

1. Проверка структуры

1.1. Определяется вид ЭП, если корневым элементом является элемент Signature, значит это «оборачивающая» электронная подпись, иначе подпись является оборачиваемой и каждая из указанных подписей проходит проверку. Подписи находятся в подчинении у корневого элемента подписанного документа последними.

1.2. Для оборачивающей подписи выполняется проверка документа валидирующим XML парсером с использованием схемы документа (Signature.xsd).

1.3. Для оборачиваемой подписи, из документа последовательно извлекается каждый присутствующей у корневого элемента документа элемент Signature и выполняется проверка с помощью валидирующего XML парсера с использованием схемы документа (Signature.xsd)

2. Проверка значений атрибутов (для оборачиваемой подписи, для каждой из присутствующих в документе ЭП)

2.1. Если значение атрибута URL первого элемента Reference не совпадает со значением атрибута Id элемента KeyInfo, то документ не проходит проверку.

2.2. Если для оборачиваемой ЭП значение атрибута URL второго элемента Reference не пустое, то документ не проходит проверку.

2.3. Если для оборачивающей ЭП значение атрибута URL второго элемента Reference не совпадает со значением атрибута Id элемента Object, то документ не проходит проверку.

2.4. Если значение атрибута Algorithm элемента Transform первого элемента Reference не равно «dsig:transformation:v1.1», то документ не проходит проверку.

2.5. Если для оборачиваемой ЭП значение атрибута Algorithm первого элемента Transform подчиненного второму элементу Reference не равно «http://www.w3.org/TR/1999/REC-xpath-19991116» или у такого элемента Transform отсутствует элемент XPath, то документ не проходит проверку.

2.6. Если для оборачиваемой ЭП элементов Transform три, то значение атрибута Algorithm второго элемента Transform подчиненного второму элементу Reference не равно «http://www.w3.org/TR/1999/REC-xpath-19991116» или у такого элемента Transform отсутствует элемент XPath, то документ не проходит проверку.

2.7. Если для оборачиваемой ЭП значение атрибута Algorithm последнего элемента Transform подчиненного второму элементу Reference не равно «dsig:transformation:v1.1», то документ не проходит проверку.

2.8. Если для оборачивающей ЭП значение атрибута Algorithm элементов Transform соответствующих второму элементу Reference не равно «dsig:transformation:v1.1», то документ не проходит проверку.

3. Проверка хеш-сумм

3.1. Проверка элемента KeyInfo

3.1.1. Элемент KeyInfo трансформируется по алгоритму «urn:xml-dsig:transformation:v1.1»

3.1.2. Для полученной строки, по указанному алгоритму «http://www.w3.org/2001/04/xmldsig-more#gostr3411» («urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512» вычисляется хеш-сумма

3.1.3. Извлекается значение элемента DigestValue первого элемента Reference.

3.1.4. Полученное значение декодируется в соответствии с алгоритмом «http://www.w3.org/2000/09/xmldsig#base64».

3.1.5. Если значение декодированного элемента DigestValue первого элемента Reference не совпадает со значением хеш-суммы трансформированного элемента KeyInfo, то документ не проходит проверку.

3.2. Проверка элемента Object (для оборачивающей ЭП)

3.2.1. Элемент Object трансформируется по алгоритму «urn:xml-dsig:transformation:v1.1».

3.2.2. Для полученной строки вычисляется хеш-сумма по указанному алгоритму «http://www.w3.org/2001/04/xmldsig-more#gostr3411»

(«urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512».

3.2.3. Извлекается значение элемента DigestValue второго элемента Reference.

3.2.4. Полученное значение декодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64».

3.2.5. Если декодированное значение элемента DigestValue второго элемента Reference не совпадает со значением хеш-суммы трансформированного элемента Object, то документ не проходит проверку.

3.3. Проверка корневого элемента (либо указанного элемента) XML документа для каждой из указанных в документе ЭП (для оборачиваемых ЭП).

3.3.1. Корневой элемент документа транформируется по алгоритму «http://www.w3.org/TR/1999/REC-xpath-19991116» с использованием выражения «not(ancestor-or-self::dsig:Signature)», то есть исключаются все подчиненные корневому узлу элементы Signature.

3.3.2. Если во втором элементе Transform значение атрибута Algorithm так же рано «http://www.w3.org/TR/1999/REC-xpath-19991116», то выполняется поиск узла, по указанному XPath выражению.

3.3.3. Полученный после первой и второй (если имело место быть) трансформации XML документ затем трансформируется по алгоритму «urn:xml-dsig:transformation:v1.1».

3.3.4. Для полученной строки вычисляется хеш-сумма по указанному алгоритму «http://www.w3.org/2001/04/xmldsig-more#gostr3411» («urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411»), «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256» или «urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512».

3.3.5. Извлекается значение элемента DigestValue второго элемента Reference.

3.3.6. Полученное значение декодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64».

3.3.7. Если декодированное значение элемента DigestValue второго элемента Reference не совпадает со значением рассчитанной хеш-суммы трансформированного корневого элемента, то документ не проходит проверку.

3.4. Проверка сертификата

3.4.1. Из элемента SignatureValue извлекается значение подписи и декодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64».

3.4.2. Из полученного значения подписи извлекается время формирования подписи.

3.4.3. Из элемента KeyInfo извлекается X509 сертификат

3.4.4. На основе извлеченного значения сертификата и времени проставления подписи проверяется действительность сертификата по сроку действия.

3.4.5. Выполняется проверка всей цепочки сертификатов (используется принципы PKI)

3.4.6. На основе извлеченного значения сертификата и времени проставления подписи проверяется достоверность сертификата и наличие в списке отозванных сертификатов (при наличии настроек OCSP серверов проверка выполняется с использованием последовательных запросов к ним).

3.4.7. Если сертификат не проходит проверку, или находится в списке отозванных сертификатов, то документ не проходит проверку.

3.5. Проверка доверенности. Осуществляется, если заполнены узлы MCDId и INNPrincipal. Дополнительно ограничения по проверке МЧД могут накладываться спецификацией взаимодействия между ИС

3.5.1. Из элемента KeyInfo извлекается идентификатор МЧД (MCDId)

3.5.2. Из элемента KeyInfo извлекается ИНН доверителя (INNPrincipal)

3.5.3. Выполняется запрос в ПУМЧД с передачей следующих сведений, в соответствии со спецификаций взаимодействия с ПУМЧД

- Идентификатор МЧД из MCDId
- ИНН доверителя из INNPrincipal
- ИНН или СНИЛС лица, сформировавшего ЭП. Извлекается из соответствующих атрибутов сертификата

- Идентификатор(ы) полномочий, которые необходимо проверить. Прикладная информация. Ссылка на кодификацию содержится в спецификации интерфейса взаимодействия с ПУМЧД
- Дата и время наложения ЭП. Извлекается из атрибутов ЭП, либо из прикладных сведений документа

3.5.4. Если ПУМЧД возвращает результат об отсутствии такой МЧД, либо несоответствии полномочий, то документ не проходит проверку

4. Проверка ЭП

4.1. Из элемента SignatureValue извлекается значение подписи и декодируется по алгоритму «http://www.w3.org/2000/09/xmldsig#base64».

4.2. Элемент SignedInfo трансформируется по алгоритму «urn:xml-dsig:transformation:v1.1».

4.3. Из элемента X509Certificate извлекается сертификат пользователя.

4.4. Трансформированная версия элемента SignedInfo и X509 сертификат используются для проверки достоверности ЭП, используя указанный в атрибуте Algorithm узла SignatureMethod.

4.5. Если при проверке достоверности наложения ЭП, был получен отрицательный результат (ЭП недействительна), то документ не проходит проверку.

5. Если документ прошел все проверки, то документ считается достоверным.

11. Соответствие идентификаторов алгоритмов и ГОСТ

В таблице 1 приведено соответствие между криптографическими алгоритмами, используемыми в текущем документе, и ГОСТ, в которых описаны соответствующие алгоритмы.

Таблица 1. Идентификаторы алгоритмов вычисления хэш-функции и ЭП

Назначение алгоритма	Обозначение ГОСТа	Идентификатор ГОСТа
Алгоритм вычисления хэш-функции	ГОСТ Р 34.11-94	http://www.w3.org/2001/04/xmldsig-more#gostr3411 или urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411
Алгоритм вычисления ЭП	ГОСТ Р 34.10-2001	http://www.w3.org/2001/04/xmldsig-more#gostr34102001-gostr3411 или urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411
Алгоритм вычисления хэш-функции	ГОСТ Р 34.11-2012	urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256 или urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512
Алгоритм вычисления ЭП	ГОСТ Р 34.10-2012	urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-256 (для длины ключа 256 бит) или urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-512 (для длины ключа 512 бит)

12. Описание алгоритмов

12.1. Трансформация

12.1.1. Идентификатор алгоритма

Для ссылок на описываемый алгоритм используется идентификатор «urn:xml-dsig:transformation:v1.1».

12.1.2. Описание алгоритма

Алгоритмом «urn:xml-dsig:transformation:v1.1» выполняется в два шага.

Для выбранного узла DOM-представления XML-документа выполняется нормализация в соответствии с алгоритмом «urn:xml-dsig:normalization:v1.1».

Полученное нормализованное представление узла приводится к канонической форме в соответствии с алгоритмом «http://www.w3.org/TR/2001/REC-xml-c14n-20010315».

Результат приведения к канонической форме является результатом работы алгоритма «urn:xml-dsig:transformation:v1.1».

12.2. Приведение к канонической форме

12.2.1. Идентификатор алгоритма

Для ссылок на описываемый алгоритм используется идентификатор «http://www.w3.org/TR/2001/REC-xml-c14n-20010315».

12.2.2. Описание алгоритма

Алгоритм описан в rfc3076. Необходимо использовать неэксклюзивную и не сохраняющую комментарии версию алгоритма.

12.3. Нормализация

12.3.1. Идентификатор алгоритма

Для ссылок на описываемый алгоритм используется идентификатор «urn:xml-dsig:normalization:v1.1».

12.3.2. Описание алгоритма

Поскольку процедура нормализации XML-документа всегда выполняется вместе с процессом канонизации, нормализация может включать любые преобразования, выполняемые на этапе канонизации XML-документа. Ниже

представлен минимальный список необходимых преобразований XML-документа для приведения к нормализованному виду:

1. Удаление из XML-документа инструкций обработки.

2. Удаление из элементов XML-документа атрибутов из пространства имен «*http://www.w3.org/2001/XMLSchema-instance*».

3. Упорядочение во всех элементах XML-документа префиксов пространств имен по заданному правилу.

4. Удаление в каждом элементе XML-документа дочерних текстовых узлов, содержащих только пробельные символы, если в данном элементе имеются дочерние элементы.

Порядок выполнения преобразований имеет значение и должен быть именно такой, как указан.

12.3.2.1 Удаление из XML-документа инструкций обработки

Для каждого узла дерева, представляющего XML-документ, выполняется следующее преобразование:

1. если данный узел является узлом инстркуции обработки, он удаляется.

12.3.2.2 Удаление из элементов XML-документа атрибутов из пространства имен “http://www.w3.org/2001/XMLSchema-instance”

Для каждого узла дерева, представляющего XML-документ, выполняется следующее преобразование:

1. если данный узел является узлом элемента, для каждого его дочернего узла выполняется следующее преобразование:

2. если данный дочерний узел является узлом атрибута, причем данный атрибут принадлежит пространству имен «*http://www.w3.org/2001/XMLSchema-instance*» и локальное имя элемента одно из: *schemaLocation*, *noNamespaceSchemaLocation*, *type*, *nil*, то он удаляется.

12.3.2.3 Упорядочение во всех элементах XML-документа префиксов пространств имен по заданному правилу

Преобразование приводит XML-документ к виду, удовлетворяющему следующим требованиям:

1. Используемые префиксы пространств имен задаются в форме n1, n2 и т.п. Положительное целое число, следующее за n, именуется индексом префикса.

2. Пространства имен никогда не наследуются.

3. Пространства имен по умолчанию никогда не применяются.

В элементе должны быть объявлены только те пространства имен, которым принадлежат элемент и его атрибуты. Объявления прочих пространств имен необходимо удалить, чтобы предотвратить конфликт имен.

Алгоритм для упорядочения во всех элементах XML-документа префиксов пространств имен по заданному правилу:

Для каждого узла элемента дерева, представляющего XML-документ, выполняется следующее преобразование:

1. составляется список названий пространств имен (URI):

1.1. элементами списка являются названия пространств имен, которым принадлежат элемент и его атрибуты;

1.2. список названий пространств имен сортируется в лексикографическом порядке, все повторяющиеся названия пространств имен удаляются;

1.3. согласно отсортированному порядку каждому названию пространства имен из списка присваивается префикс n1, n2, …, nXX (индексы префиксов всегда задаются последовательными целыми числами, начиная с 1);

2. часть имени элемента, представляющая префикс пространства имен, приводится в соответствие со списком названий пространств имен;

3. для каждого дочернего узла данного узла элемента выполняется следующее преобразование:

3.1. если данный дочерний узел является узлом пространства имен, он удаляется;

3.2. если данный дочерний узел является узлом атрибута, часть имени атрибута, представляющая префикс пространства имен, приводится в соответствие со списком названий пространств имен.

4. к узлу элемента добавляются дочерние узлы пространств имен согласно списку названий пространств имен.

12.3.2.4 Удаление в каждом элементе XML-документа дочерних

текстовых узлов, содержащих только пробельные символы, если в данном элементе имеются дочерние элементы

Символьные данные группируются в узлы текста. В каждый из таких узлов помещается столько символьных данных, сколько возможно: с текстовым узлом ни до, ни после не может соседствовать какой-либо другой текстовый узел, имеющий того же родителя. Строковым значением текстового узла являются эти самые текстовые данные. Текстовый узел всегда содержит по крайней мере один символ данных.

Алгоритм для удаления из элементов XML-документа дочерних текстовых узлов, содержащих только пробельные символы, если в данном элементе имеются дочерние элементы:

Для каждого узла дерева, представляющего XML-документ, выполняется следующее преобразование:

1. Если данный узел является узлом элемента, который содержит дочерние узлы элементов, то для каждого его дочернего узла выполняется следующее преобразование:

    а) если данный дочерний узел является текстовым узлом, который содержит только пробельные символы, то он удаляется.

12.4. BASE64

12.4.1. ИДЕНТИФИКАТОР АЛГОРИТМА

Для ссылок на описываемый алгоритм используется идентификатор «http://www.w3.org/2000/09/xmldsig#base64».

12.4.2. ОПИСАНИЕ АЛГОРИТМА

Алгоритм [base64] разработан для представления последовательности октетов в форме, которая не предназначена для чтения человеком. Алгоритмы кодирования и раскодирования просты, однако закодированные данные занимают больший объем по сравнения с исходными данными примерно на 33%.

Для кодирования используется 65 символов US-ASCII, позволяющие представить 6-битовую последовательность в виде печатного символа (65-й символ используется в качестве заполнителя).

Алгоритм кодирования представляет 24-битовую группу входных бит в виде выходной строки из 4-х символов. Обработка входного потока происходит слева направо, 24-битовая группа формируется путем конкатенации трех 8-битовых входных групп. Полученные подобным образом 24 бита трактуются как четыре объединенных 6-битовых группы, каждая из которых транслируется в отдельный символ из алфавита Base64.

Каждая 6-битовая группа используется в качестве индекса для массива из 64 печатных символа. Символ, полученный по индексу, помещается в выходную строку. Таблица F.1 демонстрирует символы, используемые при кодировании, которые составляют алфавит Base64.

Таблица 2: Алфавит Base64

Индекс	Символ	Индекс	Символ	Индекс	Символ	Индекс	Символ
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1

Продолжение таблицы 2

3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v	Заполнитель	=
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

Выходной поток может представляться строками не более, чем по 76 символов в каждой. Символы, не являющиеся символами алфавита Base64 или пробельными символами недопустимы.

Если последняя группа бит во входном потоке содержит менее 24 бит, требуется специальная обработка: справа добавляются нулевые биты до тех пор, пока не будет сформировано целое число 6-битовых групп. Если в результате получилось менее четырех 6-битовых групп, недостающие группы заменяются символами заполнителями (=). Поскольку входной поток всегда содержит целое число октетов (8-битовых групп), возможны три ситуации:

1) Финальная группа во входном потоке содержит точно 24 бита. В этом случае финальная группа в выходном потоке содержит 4 символа без символов-заполнителей.

2) Финальная группа во входном потоке содержит точно 8 бит. В этом случае финальная группа в выходном потоке содержит 2 символа, за которыми следуют два символа-заполнителя (=).

3) Финальная группа во входном потоке содержит точно 16 бит. В этом случае финальная группа в выходном потоке содержит 3 символа, за которыми следует один символ-заполнитель (=).

Для XML-документов существует два варианта форматирования данных, закодированных в кодировке Base64. Результат форматируется как строка, произвольным образом разбитая пробельными символами. Это вариант является предпочтительным. Альтернативным вариантом является разбиение результата кодирования на строки фиксированной длинны, и оформление концов строк по заданному правилу. Данный документ предъявляет следующие требования к оформлению строки, закодированной по Base64 алгоритму: Допустимы только символы алфавита Base64, и пробельные символы недопустимы. Это связанно с тем, что формат оформления закодированных данных влияет на результат вычисления ЭП, и требуются четкие требования, не допускающие разногласий.