Abstract

This document specifies XML digital signature syntax and methods of including hash-based message authentication code (HMAC) within the XML document to support the Russian cryptographic standard algorithms.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 3, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction .............................................. 3
2. Conventions Used in This Document ................................. 4
3. Basic Terms and Definitions .................................. 4
4. Structure of the document ..................................... 5
5. XML namespaces and prefixes .................................. 6
6. The Signature element schema definition .......................... 7
   6.1. The SignedInfo element ................................... 8
   6.1.1. The SignatureMethod element ............................... 9
   6.1.2. The Reference element .................................. 10
   6.1.2.1. The DigestMethod element ............................... 10
   6.1.2.2. DigestValue element ................................ 11
   6.1.2. The SignatureValue element ............................... 11
   6.2. The KeyInfo element ...................................... 12
   6.3. The KeyValue element ..................................... 13
   6.3.1. The GOSTR34102012-256-KeyValue,
          GOSTR34102012-512-KeyValue and
          GOSTR34102001KeyValue elements .................... 14
   6.3.2. The RetrievalMethod element ............................. 15
   6.3.3. The X509Data element .................................. 16
   6.3.4. The DEREncodedKeyValue element ....................... 17
7. Guidelines on the GOST algorithms ............................... 18
   7.1. GOST algorithms to create an XML document signature ....... 18
   7.1.1. Hash algorithm in DigestMethod element ................. 18
   7.1.1.1. GOST R 34.11-2012 algorithm with 256-bit hash
            code in DigestMethod element ....................... 18
   7.1.1.2. GOST R 34.11-2012 algorithm with 512-bit hash
            code in DigestMethod element ....................... 18
   7.1.1.3. GOST R 34.11-94 algorithm in DigestMethod element .... 19
   7.1.2. Signature algorithm in SignatureMethod element ....... 20
   7.1.2.1. GOST R 34.10-2012 algorithm with 256-bit key in
            SignatureMethod element ............................ 20
   7.1.2.2. GOST R 34.10-2012 algorithm with 512-bit key in
            SignatureMethod element ............................ 20
   7.1.2.3. GOST R 34.10-2001 algorithm in SignatureMethod
            element ............................................. 21
   7.2. GOST algorithms to calculate HMAC value ................. 21
   7.2.1. GOST R 34.11-2012 algorithm with 256-bit key in
            SignatureMethod element ............................ 21
   7.2.2. GOST R 34.11-2012 algorithm with 512-bit key in
            SignatureMethod element ............................ 22
   7.3. The key material ...................... 22
   7.3.1. Verification key in DEREncodedKeyValue element ........ 23
   7.3.2. GOST R 34.10-2012 256-bit verification key in
            .......... 23
This document specifies new identifiers (see Section 7.1) of the following Russian signature and hash algorithms (called GOST algorithms):

- the GOST 34.11-2012 [GOST3411-2012] hash algorithm (the English version can be found in [RFC6986]),

- the GOST 34.10-2012 [GOST3410-2012] signature algorithm (the English version can be found in [RFC7091]).

This document specifies new identifiers (see Section 7.2) of the following Russian HMAC algorithms (called HMAC algorithms):

- the R 50.1.113-2016 [R501113-2016] HMAC algorithms (the English version can be found in [RFC7836]).

In addition, this document specifies new ways of the key material placement within XML document and namespace identifiers, prefixes and XML schema definitions.
2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Basic Terms and Definitions

This document uses the following terms and definitions:

- **XML document** electronic document written in Extensible Markup Language (XML);
- **XML schema** XML document structure description;
- **XML element** part of an XML document from the element start tag to the element end tag;
- **XML schema definition** part of an XML schema describing particular element (element name and type);
- **XML namespace** namespace describing XML schema elements and providing their unicity;
- **XML prefix** set of letters placed at the beginning of an XML element or his type to exclude the collision of equivalent elements from different namespaces;
- **XML attribute** part of an XML element consisting of attribute name and its value;
- **hash-based message authentication code (HMAC)** a function for calculating a message authentication code, based on a hash function in accordance with [RFC2104];
- **verification key** element of data mathematically linked to the signature key data element that is used by the verifier during the digital signature verification process [RFC7091];
- **signature key** element of secret data that is specific to the subject and used only by this subject during the signature generation process [RFC7091].

Note: For brevity, the terms "XML element" and "element", "XML attribute" and "attribute", "XML prefix" and "prefix" are synonymous.
4. Structure of the document

The XML namespaces, prefixes and identifiers are defined in Section 5.

The ds:Signature element is described in Section 6. This element includes XML document signature value, used algorithms identifiers and other parameters, which are used to generate the signature value. Also, this element MAY include the HMAC value and algorithms identifiers which are used to support HMAC algorithms. The ds:Signature element is described by the following XML schemas (defined in Table 1 of Section 5): DS schema, DSIG11 schema and CPXMLSEC schema.

The CPXMLSEC schema is a new schema defined in this document and extends the DS schema in order to support GOST algorithms. The CPXMLSEC schema elements uses XS schema elements (see [XMLSCHEMA-1] and [XMLSCHEMA-2]). The DS schema and DSIG11 schema definitions are described in accordance with [XMLSIG].

Note: In case of using HMAC the name of the ds:Signature element doesn’t represent content type to avoid elements duplication and optimize XML digital signature structure. HMAC algorithm identifier and HMAC value MUST be included in ds:SignatureMethod and ds:SignatureValue respectively.

Note: In this document, some elements inside the comments of XML schema definition are avoided since GOST and HMAC algorithms are not used in these elements. The XML schema comments are not semantical, that is why DS schema and DSIG11 schema definitions in this document are equivalent to [XMLSIG].

The requirements for the elements described in Section 6 are listed in Section 7:

1. Section 7.1 contains requirements for the elements representation during the signature generation and verification processes.
2. Section 7.2 contains requirements for the elements during the HMAC calculation process.
3. Section 7.3 contains requirements for the elements during the key material specifying in signed XML document.
5. XML namespaces and prefixes

This document uses XML elements from four different XML schemas. Every XML schema is assigned to one XML namespace. The following general XML namespace identifier MUST be used as targetNamespace in the XML schema header:

\texttt{urn:ietf:params:xml:ns:cpxmlsec}

The other XML namespaces are external. Their identifiers MUST be specified in XML schema header.

Note: XML schema is explicitly specified by the XML namespace identifier (see Table 1).

<table>
<thead>
<tr>
<th>XML schema name</th>
<th>XML namespace identifier</th>
<th>Prefix</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS schema</td>
<td><a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a></td>
<td>ds</td>
<td>&lt;xref target=&quot;XMLDSIG&quot;/&gt;</td>
</tr>
<tr>
<td>DSG11 schema</td>
<td><a href="http://www.w3.org/2009/xmldsig11#">http://www.w3.org/2009/xmldsig11#</a></td>
<td>dsig11</td>
<td>&lt;xref target=&quot;XMLDSIG&quot;/&gt;</td>
</tr>
<tr>
<td>XS schema</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>xs</td>
<td>&lt;xref target=&quot;XMLSCHEMA-1&quot;/&gt;,&lt;xref target=&quot;XMLSCHEMA-2&quot;/&gt;</td>
</tr>
<tr>
<td>CPXMLSEC schema</td>
<td>urn:ietf:params:xml:ns:cpxmlsec</td>
<td>cpxmlsec</td>
<td>This document</td>
</tr>
</tbody>
</table>

Table 1

Note: The XS schema definitions are assistive and it is unnecessary for describing it in this document.

Any element or attribute whose name starts with the prefix from the Table 1 is considered to be in the corresponding XML schema. The full definition of any XML schema is defined in the document referenced in the "Reference" column of the Table 1. This document uses prefixes to exclude the collision of equivalent elements from different namespaces (see Table 1). The prefixes are no semantical and MAY be replaced by others. Namespaces and prefixes MUST have no line breaks and space characters.

The example of CPXMLSEC schema header:
6. The Signature element schema definition

The ds:Signature element is the root element of an XML signature. It contains the following values:

- for digital signature: signature value, information about algorithms and other parameters, which are used to generate the signature value.

- for HMAC: HMAC value and HMAC algorithm identifier.

The ds:Signature element contains the following descendants:

- The ds:SignedInfo element (Section 6.1). This element contains information about algorithms and other parameters.

- The ds:SignatureValue element (Section 6.2). This element includes the signature value or the HMAC value.

- The ds:KeyInfo element (Section 6.3). This element contains information about verification key and its value or information about HMAC symmetric key location.

- The ds:Object element. This element MAY contain data to be signed or authenticated.

The ds:Signature element is described by the following XML schema definition.
<xs:element name="Signature" type="ds:SignatureType"/>

<xs:complexType name="SignatureType">
    <xs:sequence>
        <xs:element ref="ds:SignedInfo"/>
        <xs:element ref="ds:SignatureValue"/>
        <xs:element ref="ds:KeyInfo" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="Id" type="ID" use="optional"/>
</xs:complexType>

Please refer to [XMLDSIG] for the ds:Signature element full definition.

6.1. The SignedInfo element

The ds:SignedInfo element is a descendant of ds:Signature element. It contains information about algorithms and other parameters, which are used to generate the signature or the HMAC value. The ds:SignedInfo element contains the following descendants:

- The ds:SignatureMethod element (Section 6.1.1). This element specifies the algorithm used for signature or HMAC generation.

- The ds:Reference element (Section 6.1.2). This element describes data to be transformed.

- The ds:CanonicalizationMethod element. This element specifies the canonicalization algorithm applied to the ds:SignedInfo element.

The ds:SignedInfo element is described by the following XML schema definition.
<xs:element name="SignedInfo" type="ds:SignedInfoType"/>

<xs:complexType name="SignedInfoType">
    <xs:sequence>
        <xs:element ref="ds:CanonicalizationMethod"/>
        <xs:element ref="ds:SignatureMethod"/>
        <xs:element ref="ds:Reference" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="Id" type="ID" use="optional"/>
</xs:complexType>

Please refer to [XMLDSIG] for the ds:SignedInfo element full definition.

6.1.1. The SignatureMethod element

The ds:SignatureMethod element is a descendant of ds:SignedInfo element. It specifies the algorithm used for signature generation and verification, or HMAC calculation. The identifier of the algorithm MUST be included in the "Algorithm" attribute.

GOST algorithms identifiers are described in Section 7.1.2.

HMAC algorithms identifiers are described in Section 7.2.

The ds:SignatureMethod element is described by the following XML schema definition.

<xs:element name="SignatureMethod" type="ds:SignatureMethodType"/>

<xs:complexType name="SignatureMethodType" mixed="true">
    <xs:sequence>
        <xs:element name="HMACOutputLength" minOccurs="0" type="ds:HMACOutputLengthType"/>
        <xs:any namespace="##other" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="Algorithm" type="anyURI" use="required"/>
</xs:complexType>

Please refer to [XMLDSIG] for the ds:SignatureMethod element full definition.
6.1.2. The Reference element

The ds:Reference element is a descendant of ds:SignedInfo element. It MAY contain "Id", "URI" and "Type" attributes to specify the transformed data. The ds:Reference element contains the following descendants:

- The ds:Transforms element. This element contains an ordered list of the data transforms specified in ds:Reference element attributes.
- The ds:DigestMethod element (Section 6.1.2.1). This element identifies the hash algorithm to be applied to the data specified in ds:Reference element attributes.
- The ds:DigestValue element (Section 6.1.2.2). This element includes the hash value of the data specified in ds:Reference element attributes.

The ds:Reference element is described by the following XML schema definition.

```xml
<xs:element name="Reference" type="ds:ReferenceType"/>
<xs:complexType name="ReferenceType">
  <xs:sequence>
    <xs:element ref="ds:Transforms" minOccurs="0"/>
    <xs:element ref="ds:DigestMethod"/>
    <xs:element ref="ds:DigestValue"/>
  </xs:sequence>
  <xs:attribute name="Id" type="ID" use="optional"/>
  <xs:attribute name="URI" type="anyURI" use="optional"/>
  <xs:attribute name="Type" type="anyURI" use="optional"/>
</xs:complexType>
```

Please refer to [XMLDSIG] for the ds:Reference element full definition.

6.1.2.1. The DigestMethod element

The ds:DigestMethod element is a descendant of ds:Reference element. This element identifies the hash algorithm to be applied to the data
specified in ds:Reference element attributes. The identifier of the used hash algorithm MUST be included in the "Algorithm" attribute.

The DigestMethod element is described by the following XML schema definition.

```xml
<xs:element name="DigestMethod" type="ds:DigestMethodType"/>
<xs:complexType name="DigestMethodType" mixed="true">
  <xs:sequence>
    <xs:any namespace="##other" processContents="lax"
      minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="Algorithm" type="anyURI" use="required"/>
</xs:complexType>
```

Please refer to [XMLDSIG] for the ds:DigestMethod element full definition.

### 6.1.2.2. DigestValue element

The ds:DigestValue element is a descendant of ds:Reference element. This element includes the hash value of data specified in ds:Reference element attributes. The hash value MUST be represented in accordance with Section 7.1.1.

The ds:DigestValue element is described by the following XML schema definition.

```xml
<xs:element name="DigestValue" type="ds:DigestValueType"/>
<xs:simpleType name="DigestValueType">
  <xs:restriction base="base64Binary"/>
</xs:simpleType>
```

### 6.2. The SignatureValue element

The ds:SignatureValue element is a descendant of ds:Signature element. This element includes the XML document signature value or the HMAC value.
In case of GOST algorithms signature value MUST be represented in accordance with Section 7.1.2.

In case of HMAC algorithms the HMAC value MUST be represented in accordance with Section 7.2.

The ds:SignatureValue element is described by the following XML schema definition.

```xml
<xs:element name="SignatureValue" type="ds:SignatureValueType" />
<xs:complexType name="SignatureValueType">
  <xs:simpleContent>
    <xs:extension base="base64Binary">
      <xs:attribute name="Id" type="ID" use="optional"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

Please refer to [XMLDSIG] for the ds:SignatureValue element full definition.

6.3. The KeyInfo element

The ds:KeyInfo element is a descendant of ds:Signature element. This element contains information about verification key and its value or information about HMAC symmetric key location.

In case of verification key is passed in XML document the following descendants MAY be included in the KeyInfo element:

- The ds:KeyValue element (Section 6.3.1). This element contains the verification key and its parameters.
- The ds:RetrievalMethod element (Section 6.3.2). This element identifies verification key location if the key is stored at external location.
- The ds:X509Data element (Section 6.3.3). This element includes X.509 certificate ([RFC5280]) with verification key.
- Note: The Russian version of [RFC5280] can be found in [R1323565.1.023-2018]. It MUST be used as guidelines on GOST algorithms.
o The dsig11:DEREncodedKeyValue element (Section 6.3.4). This
element contains the verification key and its parameters.

Note: Both ds:KeyValue and dsig11:DEREncodedKeyValue elements MAY be
used for specifying the verification key and its parameters. These
elements use different semantic for the verification key specifying:
in case of ds:KeyValue element the verification key and its
parameters are passed in descendant elements; in case of the
dsig11:DEREncodedKeyValue element the verification key and its
parameters are passed in the SubjectPublicKeyInfo structure
[R1323565.1.023-2018].

In the case of HMAC symmetric key the ds:RetrievalMethod element
(Section 6.3.2) MUST be used.

The ds:KeyInfo element is described by the following XML schema
definition.

<x:s:element name="KeyInfo" type="ds:KeyInfoType"/>
<x:s:complexType name="KeyInfoType" mixed="true">
  <x:s:choice maxOccurs="unbounded">
    <x:s:element ref="ds:KeyName"/>
    <x:s:element ref="ds:KeyValue"/>
    <x:s:element ref="ds:RetrievalMethod"/>
    <x:s:element ref="ds:X509Data"/>
    <x:s:element ref="ds:PGPData"/>
    <x:s:element ref="ds:SPKIData"/>
    <x:s:element ref="ds:MgmtData"/>
    <!-- <x:s:element ref="dsig11:DEREncodedKeyValue"/> -->
    <!-- DEREncodedKeyValue (XMLDsig 1.1) will use the any element -->
    <x:s:any processContents="lax" namespace="##other"/>
    <!-- (1,1) elements from (0,unbounded) namespaces -->
  </x:s:choice>
  <x:s:attribute name="Id" type="ID" use="optional"/>
</x:s:complexType>

Please refer to [XMLDSIG] for the ds:KeyInfo element full definition.

6.3.1. The KeyValue element

The ds:KeyValue element is a descendant of ds:KeyInfo element. This
element contains the verification key and its parameters.
In case of GOST algorithms the following extra descendants MUST be included in the KeyInfo element:

- the cpxmlsec:GOSTR34102012-256-KeyValue element;
- the cpxmlsec:GOSTR34102012-256-KeyValue element;
- the cpxmlsec:GOSTR34102001KeyValue element.

The ds:KeyValue element is described by the following XML schema definition.

```xml
<xs:element name="KeyValue" type="ds:KeyValueType" />  
<xs:complexType name="KeyValueType" mixed="true">  
  <xs:choice>  
    <xs:element ref="ds:DSAKeyValue"/>  
    <xs:element ref="ds:RSAKeyValue"/>  
  </xs:choice>  
</xs:complexType>
```

Please refer to [XMLDSIG] for the ds:KeyValue element full definition.

6.3.1.1. The GOSTR34102012-256-Key Value, GOSTR34102012-512-Key Value and GOSTR34102001KeyValue elements

The cpxmlsec:GOSTR34102012-256-Key Value, cpxmlsec:GOSTR34102012-512-Key Value and cpxmlsec:GOSTR34102001KeyValue elements are a descendants of ds:Key Value element. Each of these elements has cpxmlsec:GOSTKeyValueType type and MUST contain the following descendants:

- the cpxmlsec:NamedCurve element - contains the elliptic curve identifier;
- the cpxmlsec:Public Key element - contains the verification key.
The cpxmlsec:NamedCurve and cpxmlsec:PublicKey elements belong to cpxmlsec namespace. The cpxmlsec namespace identifier is described in Section 5. The cpxmlsec:NamedCurve element has dsig11:NamedCurveType type. The cpxmlsec:PublicKey element has dsig11:ECPointType type. Both types belong to DSIG11 schema [XMLDSIG].

The cpxmlsec:GOSTR34102012-256-KeyValue, cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:GOSTR34102001KeyValue elements data MUST be represented in accordance with Section 7.3.2-Section 7.3.4.

The cpxmlsec:GOSTR34102012-256-KeyValue, cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:GOSTR34102001KeyValue elements are described by the following XML schema definition.

```xml
<xs:element name="GOSTR34102012-256-KeyVal" type="cpxmlsec:GOSTKeyValueType" />
<xs:element name="GOSTR34102012-512-KeyVal" type="cpxmlsec:GOSTKeyValueType" />
<xs:element name="GOSTR34102001KeyVal" type="cpxmlsec:GOSTKeyValueType" />
<xs:complexType name="GOSTKeyValueType">
    <xs:sequence>
        <xs:element name="NamedCurve" type="dsig11:NamedCurveType" />
        <xs:element name="PublicKey" type="dsig11:ECPointType" />
    </xs:sequence>
</xs:complexType>
```

6.3.2. The RetrievalMethod element

The ds:RetrievalMethod element is a descendant of ds:KeyInfo element. This element identifies the verification or symmetric key location if the key is stored at external location. The verification or symmetric key MUST be included in "URI" and "Type" attributes.

The `ds:RetrievalMethod` element is described by the following XML schema definition.

```xml
<xs:element name="RetrievalMethod" type="ds:RetrievalMethodType" />
<xs:complexType name="RetrievalMethodType">
  <xs:sequence>
    <xs:element ref="ds:Transforms" minOccurs="0" />
  </xs:sequence>
  <xs:attribute name="URI" type="anyURI" />
  <xs:attribute name="Type" type="anyURI" use="optional" />
</xs:complexType>
```

Please refer to [XMLDSIG] for the `ds:RetrievalMethod` and `ds:Transforms` elements full definition.

6.3.3. The X509Data element

The `ds:X509Data` element is a descendant of `ds:KeyInfo` element. This element includes the X.509 certificate with the verification key [RFC5280], which are used to generate the signature value, or information about it.

The `ds:X509Data` element is described by the following XML schema definition.
<xs:element name="X509Data" type="ds:X509DataType"/>

<xs:complexType name="X509DataType">
  <xs:sequence maxOccurs="unbounded">
    <xs:choice>
      <xs:element name="X509IssuerSerial" type="ds:X509IssuerSerialType"/>
      <xs:element name="X509SKI" type="base64Binary"/>
      <xs:element name="X509SubjectName" type="string"/>
      <xs:element name="X509Certificate" type="base64Binary"/>
      <xs:element name="X509CRL" type="base64Binary"/>
      <!-- <xs:element ref="dsig11:X509Digest"/> -->
      <!-- The X509Digest element (XMLDSig 1.1) will use the any element -->
      <xs:any namespace="##other" processContents="lax"/>
    </xs:choice>
  </xs:sequence>
</xs:complexType>

Please refer to [XMLDSIG] for the ds:X509Data element full definition.

6.3.4. The DEREncodedKeyValue element

The dsig11:DEREncodedKeyValue element is an extension of ds:KeyInfo element schema. This element contains the verification key and its parameters. Data included in dsig11:DEREncodedKeyValue MUST be represented in accordance with Section 7.3.1.

The dsig11:DEREncodedKeyValue element is described by the following XML schema definition.

<!-- targetNamespace="http://www.w3.org/2009/xmldsig11#" -->

<x:s:element name="DEREncodedKeyValue" type="dsig11:DEREncodedKeyValueType"/>

<x:complexType name="DEREncodedKeyValueType">
  <xs:simpleContent>
    <xs:extension base="base64Binary">
      <xs:attribute name="Id" type="ID" use="optional"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
Please refer to [XMLDSIG] for the dsig11:DEREncodedKeyValue element full definition.

7. Guidelines on the GOST algorithms

This section defines the requirements for the elements (see Section 6) content are intended to use GOST and HMAC algorithms.

7.1. GOST algorithms to create an XML document signature

7.1.1. Hash algorithm in DigestMethod element

7.1.1.1. GOST R 34.11-2012 algorithm with 256-bit hash code in DigestMethod element

In case of GOST R 34.11-2012 algorithm with 256-bit hash code the following identifier MUST be used:

urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256

Test example for GOST R 34.11-2012 algorithm with 256-bit hash code in ds:DigestMethod element:


The hash code MUST be represented in little-endian byte order and base64-encoded [RFC4648]. This string MUST be included in ds:DigestValue element (see Section 6.1.2.2).

7.1.1.2. GOST R 34.11-2012 algorithm with 512-bit hash code in DigestMethod element

In case of GOST R 34.11-2012 algorithm with 512-bit hash code the following identifier MUST be used:


Test example for GOST R 34.11-2012 algorithm with 512-bit hash code in ds:DigestMethod element:
The hash code MUST be represented in little-endian byte order and base64-encoded [RFC4648]. This string MUST be included in the ds:DigestValue element (see Section 6.1.2.2).

7.1.1.3. GOST R 34.11-94 algorithm in DigestMethod element

In case of GOST R 34.11-94 algorithm the following identifier MUST be used:


The ds:DigestMethod element MAY include a descendant element named cpxmlsec:NamedParameters to specify hash algorithm parameters.

Hash algorithm parameters MUST be included in the "URI" attribute of cpxmlsec:NamedParameters element. In case of OIDs hash algorithm parameters SHOULD be assigned in accordance with [RFC3061]. OID’s defined in section 8.2 of [RFC4357] MAY be used.

Parameter set id-GostR3411-94-CryptoProParamSet [RFC4357] MUST be used if cpxmlsec:NamedParameters element does not exist.

The cpxmlsec:NamedParameters element is described by the following XML schema definition.

<xs:element name="NamedParameters"
    type="cpxmlsec:NamedParametersType" />

Test example for GOST R 34.11-94 algorithm in ds:DigestMethod element:

<!-- id-GostR3411-94-CryptoProParamSet -->
    <cpxmlsec:NamedParameters URI="urn:oid:1.2.643.2.2.30.1" />
</ds:DigestMethod>
The hash code MUST be represented in little-endian byte order and base64-encoded [RFC4648]. This string MUST be included in ds:DigestValue element (see Section 6.1.2.2).

7.1.2. Signature algorithm in SignatureMethod element

7.1.2.1. GOST R 34.10-2012 algorithm with 256-bit key in SignatureMethod element

In case of GOST R 34.10-2012 algorithm with 256-bit signature key the following identifier MUST be used (without line break in the identifier):


Test example for GOST R 34.10-2012 algorithm with 256-bit signature key in ds:SignatureMethod element (without line break in the attribute value):


The signature value MUST be represented in accordance with [R1323565.1.023-2018] and base64-encoded [RFC4648]. This string MUST be included in ds:SignatureValue element (see Section 6.2).

7.1.2.2. GOST R 34.10-2012 algorithm with 512-bit key in SignatureMethod element

In case of GOST R 34.10-2012 algorithm with 512-bit signature key the following identifier MUST be used (without line break in the identifier):


Test example for GOST R 34.10-2012 algorithm with 512-bit signature key in ds:SignatureMethod element (without line break in the attribute value):
The signature value MUST be represented in accordance with [R1323565.1.023-2018] and base64-encoded [RFC4648]. This string MUST be included in ds:SignatureValue element (see Section 6.2).

7.1.2.3. GOST R 34.10-2001 algorithm in SignatureMethod element

In case of GOST R 34.10-2001 algorithm the following identifier MUST be used:

```
```

Test example for GOST R 34.10-2001 algorithm in ds:SignatureMethod element:

```
```

The signature value MUST be represented in accordance with [R1323565.1.023-2018] and base64-encoded [RFC4648]. This string MUST be included in ds:SignatureValue element (see Section 6.2).

7.2. GOST algorithms to calculate HMAC value

GOST R 34.11-2012 algorithm MAY be used as HMAC algorithm in accordance with section 6.3.1 [XMLDSIG] and section 4.1.1 [R5011113-2016].

7.2.1. GOST R 34.11-2012 algorithm with 256-bit key in SignatureMethod element

In case of GOST R 34.11-2012 algorithm with 256-bit hash code the following identifier MUST be used:

```
```
Test example for GOST R 34.11-2012 algorithm with 256-bit hash code in ds:SignatureMethod element:

```xml
```

The HMAC_GOSTR3411_2012_256 algorithm result (section 4.1.1 [R501113-2016]) MUST be represented in little-endian byte order and base64-encoded [RFC4648]. This string MUST be included in ds:SignatureValue element (see Section 6.2).

### 7.2.2. GOST R 34.11-2012 algorithm with 512-bit key in SignatureMethod element

In case of GOST R 34.11-2012 algorithm with 512-bit hash code the following identifier MUST be used:

\[urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512\]

Test example for GOST R 34.11-2012 algorithm with 512-bit hash code in ds:SignatureMethod element:

```xml
```

The HMAC_GOSTR3411_2012_512 algorithm result (section 4.1.2 [R501113-2016]) MUST be represented in little-endian byte order and base64-encoded [RFC4648]. This string MUST be included in ds:SignatureValue element (see Section 6.2).

### 7.3. The key material

This document defines new ways of the GOST algorithms verification key specifying: in dsig11:DEREncodedKeyValue (Section 6.3.4) element and in ds:KeyValue (Section 6.3.1) descendants. In addition, the information about the key material MAY be specified in any way in accordance with [XMLDSIG].
7.3.1. Verification key in DEREncodedKeyValue element

This section defines GOST R 34.10-2012 and GOST R 34.10-2001 verification key specifying in dsig11:DEREncodedKeyValue (Section 6.3.4) element.

The verification key and its parameters MUST be included in SubjectPublicKeyInfo structure and encoded in accordance with [R1323565.1.023-2018].

Test example for the dsig11:DEREncodedKeyValue element:

```xml
<dsig11:DEREncodedKeyValue>
  <!-- The verification key value -->
</dsig11:DEREncodedKeyValue>
```

7.3.2. GOST R 34.10-2012 256-bit verification key in GOSTR34102012-256-KeyValue element

If the key is stored at external location, the following identifier MUST be included in the "Type" attribute of ds:Reference or ds:RetrievalMethod elements:

```xml
```

If the key is included in XML document, it MUST be represented in subjectPublicKey field of SubjectPublicKeyInfo structure [R1323565.1.023-2018] without OCTET STRING and DER encoding. This string MUST be base64-encoded [RFC4648] and included in the cpxmlsec:GOSTR34102012-256-KeyValue element similar to the ds:RSAKeyValue [XMLDSIG]. (The cpxmlsec:GOSTR34102012-256-KeyValue element is a descendant of the cpxmlsec:PublicKey element). The XML schema of the cpxmlsec:GOSTR34102012-256-KeyValue and cpxmlsec:PublicKey elements is defined in Section 6.3.1.1.

The elliptic curve identifier (verification key parameters) MUST be included in the "URI" attribute of the cpxmlsec:NamedCurve element (see Section 6.3.1.1). In case of OIDs verification key parameters SHOULD be assigned in accordance with [RFC3061]. OID identifiers for GOST algorithms are defined in [R1323565.1.023-2018].

Test example for cpxmlsec:GOSTR34102012-256-KeyValue element:
7.3.3. GOST R 34.10-2012 512-bit verification key in GOSTR34102012-512-KeyValue element

If the key is stored at external location, the following identifier MUST be included in the "Type" attribute of ds:Reference or ds:RetrievalMethod elements:


If the key is included in XML document, it MUST be represented in subjectPublicKey field of SubjectPublicKeyInfo structure [R1323565.1.023-2018] without OCTET STRING and DER encoding. This string MUST be base64-encoded [RFC4648] and included in the cpxmlsec:GOSTR34102012-512-KeyValue element similar to the ds:RSAKeyValue [XMLDSIG]. (The cpxmlsec:GOSTR34102012-512-KeyValue element is a descendant of the cpxmlsec:PublicKey element). The XML schema of the cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:PublicKey elements is defined in Section 6.3.1.1.

The elliptic curve identifier (verification key parameters) MUST be included in the "URI" attribute of the cpxmlsec:NamedCurve element (see Section 6.3.1.1). In case of OIDs verification key parameters SHOULD be assigned in accordance with [RFC3061]. OID identifiers for GOST algorithms are defined in [R1323565.1.023-2018].

Test example for cpxmlsec:GOSTR34102012-512-KeyValue element:

```xml
<cpxmlsec:GOSTR34102012-512-KeyValue>
  <!-- id-tc26-gost-3410-12-512-paramSetA -->
  <cpxmlsec:NamedCurve URI="urn:oid:1.2.643.7.1.2.1.2.1" />
  <cpxmlsec:PublicKey>
    <!-- The verification key value -->
  </cpxmlsec:PublicKey>
</cpxmlsec:GOSTR34102012-512-KeyValue>
```
7.3.4. GOST R 34.10-2001 verification key in GOSTR34102001KeyValue element

If the key is stored at external location, the following identifier MUST be included in the "Type" attribute of ds:Reference or ds:RetrievalMethod elements:


If the key is included in XML document, it MUST be represented in subjectPublicKey field of SubjectPublicKeyInfo structure [R1323565.1.023-2018] without OCTET STRING and DER encoding. This string MUST be base64-encoded [RFC4648] and included in the cpxmlsec:GOSTR34102001KeyValue element similar to the ds:RSAKeyValue [XMLDSIG]. (The cpxmlsec:GOSTR34102001KeyValue element is an descendant of the cpxmlsec:PublicKey element). The XML schema of the cpxmlsec:GOSTR34102001KeyValue and cpxmlsec:PublicKey elements is defined in Section 6.3.1.1.

The elliptic curve identifier (verification key parameters) MUST be included in the "URI" attribute of the cpxmlsec:NamedCurve element (see Section 6.3.1.1). In case of OIDs verification key parameters SHOULD be assigned in accordance with [RFC3061]. OID identifiers for GOST algorithms are defined in section 8.4 of [RFC4357].

Test example for cpxmlsec:GOSTR34102001KeyValue element:

```xml
<cpxmlsec:GOSTR34102001KeyValue>
  <!-- id-GostR3410-2001-CryptoPro-A-ParamSet -->
  <cpxmlsec:NamedCurve URI="urn:oid:1.2.643.2.2.35.1" />
  <cpxmlsec:PublicKey>
    <!-- The verification key value -->
  </cpxmlsec:PublicKey>
</cpxmlsec:GOSTR34102001KeyValue>
```

8. IANA Considerations

8.1. XML sub-namespace registration

This section registers a new XML sub-namespace, "urn:ietf:params:xml:ns:cpxmlsec" (see Section 5) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec
Registrant Contact: See the "Authors’ Addresses" section of this document.

XML: None.  Namespace URIs do not represent an XML specification.

8.2.  XML schema registration

This section registers an XML schema per the guidelines in [RFC3688]:


Registrant Contact: See the "Authors’ Addresses" section of this document.

XML: The XML can be found in Appendix A.

9.  References

9.1.  Normative References


9.2. Informative References


Appendix A.  CPXMLSEC XML schema
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE schema [ 
  <!ENTITY xmldsiguri "http://www.w3.org/TR/2008/REC-xmldsig-core-20080610"> ]>

<xsd:schema
  xmlns:cpxmlsec="urn:ietf:params:xml:ns:cpxmlsec"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:dsig11="http://www.w3.org/2009/xmldsig11#"
  targetNamespace="urn:ietf:params:xml:ns:cpxmlsec"
  elementFormDefault="qualified"
  version="0.4">
  <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="&xmldsiguri;/xmldsig-core.xsd"/>
  <xs:import namespace="http://www.w3.org/2009/xmldsig11#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core1/xmldsig11-schema.xsd"/>
  <xs:element name="NamedParameters"
    type="cpxmlsec:NamedParametersType" />
  <xs:complexType name="NamedParametersType">
    <xs:attribute name="URI" type="xs:anyURI" use="required" />
  </xs:complexType>
  <xs:complexType name="GOSTKeyValueType">
    <xs:sequence>
      <xs:element name="NamedCurve"
        type="dsig11:NamedCurveType" />
      <xs:element name="PublicKey" type="dsig11:ECPointType" />
    </xs:sequence>
  </xs:complexType>
  <xs:element name="GOSTR34102012-256-KeyValue"
    type="cpxmlsec:GOSTKeyValueType" />
  <xs:element name="GOSTR34102012-512-KeyValue"
    type="cpxmlsec:GOSTKeyValueType" />
  <xs:element name="GOSTR34102001KeyValue"
    type="cpxmlsec:GOSTKeyValueType" />
</xsd:schema>
Appendix B. Test Examples

Note: Line breaks in the coordinates, identifiers, XML elements or in the attribute values MUST be ignored.

B.1. Signed XML document with GOST R 34.10-2012 algorithm and 256-bit hash code in DigestMethod element

The X.509 certificate from Appendix A of [R1323565.1.023-2018] was used.

The x-coordinate of verification key:

0x971566C6DA436EE7678F7E07E84EBB7217406C0B4747AA8FD2AB1453C3D0DFBA

The y-coordinate of verification key:

0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E2E24FF71F9CE643

Corresponding signature key (d):

0xBFCF1D623E5CDD3032A7C6EABB4A923C46E43D640FFEAAF2C3ED39A8FA399924

The k value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEFE33B0E270318857C

The h-bar value:

0x054D1DABB161D63424F8DABB2800708B00F78DA7582699E8F2F0A521C7CE8144

The signed XML document:
<?xml version="1.0" encoding="utf-8"?>
<root>
  <DataToSign Id="ToSign">Data</DataToSign>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <Reference URI="#ToSign">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestValue>9QLsxPPc7LLX6IXqwzjcNDmbFuCCGivQ1s61hcPuITM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>jcQJhWtWbTCV7bjFky5vGXXUFigc74FXRi79iZnFHK7pMjpeIN2H+3xyQ40//nzs1Ln/oqwzu9zpaH3Q0BPaw==</SignatureValue>
    <KeyInfo>
      <KeyValue>
        <GOSTR34102012-256-KeyValue xmlns="urn:ietf:params:xml:ns:cpxmlsec">
          <NamedCurve URI="urn:oid:1.2.643.2.2.36.0"/>
          <PublicKey>ut/Qw1MUq9KPqkdHC2xAF3K7TugHfo9n525D2s5mFzd5w9f90/i4vF0mFmr9nfRwMYP4o0Pg1mOn5RlaxNYrQ==</PublicKey>
        </GOSTR34102012-256-KeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</root>
The base64-encoded signed XML document:

```
77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXJs会ZiIKPD8ODGAgICAgICAgPD86IEJ1
aWZpb3cgb2x1aWxtLC5jbi5wYXJhbmNlcy5jeCAKICAgICAgICAgIGh0dHA6Ly93d3cuZ29ya
XyYW5zZW4uY29tIiAgICAgICAgICAgICAgIDwvU2lnbmF0dXJlPg0KPC9yb290Pg==
```

B.2. Signed XML document with GOST R 34.10-2012 algorithm and 512-bit hash code in DigestMethod element

The X.509 certificate from Appendix A of [R1323565.1.023-2018] was used.

The x-coordinate of verification key:

```
0x07134627CE7FC6770953ABA4714B38AF8DE764B8870A502C2F4C2D0551459A18DA3B9
```

The y-coordinate of verification key:

```
0x07134627CE7FC6770953ABA4714B38AF8DE764B8870A502C2F4C2D0551459A18DA3B9
```
Corresponding signature key (d):

0x3FC01CDCD4EC5F972EB482774C41E66DB7F380528DFE9E67992BA05AEE462435757530
E641077CE587B976C8EEB48C48FD33FD175F0C7DE6A44E014E6BCB074B

The k value:

0x72ABB44536656BF1618CE10BF7EADD40582304A51EE4E2A25A0A32CB0E773ABB23B7D8
FDD8FA5EEE91B4AE452F2272C86E1E2221215D405F51B5D5015616E1F6

The h-bar value:

0x33DEF8422879AA68482339BC65E5DCA9A5D77E80C5C0371DB13D3B88F4CCA8A89ED3CE
85849231DD61B35E4B47A3722317663859A2BE088C1BB6EEC87410DAF2

The signed XML document:

```xml
<?xml version="1.0" encoding="utf-8"?>
<root>
  <DataToSign Id="ToSign">Data</DataToSign>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <Reference URI="#ToSign"/>
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </Transforms>
      <DigestMethod Algorithm=
```
<SignedInfo>
    <DigestValue>
        wiOFD9D7zKHNlo58t/9tUtCJA5Z09vmdMlt3H1kyXZvQxI5PE+txwsI
        AVfUIUULvGTfxAZ1wuHTB+qD5a54g==
    </DigestValue>
</SignedInfo>

<SignatureValue>
    dn+6oWg6n3zJ0bkBmOlGurc4suZ3h3XkWVY4uHdmeS2n1l1NWFKca4fTBlc+fp
    nCS8IEVNFX25Ndh4UXJLLN12/L0wtaNCFiA+xRyzFgsUGW+pwIfyfVbdsSpbwe
    ZyjUwajN31DR2dzchycEAmyN1qDpTtes88BrNvXSh+Cpg+c=
</SignatureValue>

<KeyInfo>
    <KeyVal>
        <GOSTR34102012-512-KeyVal xmlns="urn:ietf:params:xml:ns:cpxmlsec">
            <NamedCurve URI="urn:oid:1.2.643.7.1.2.1.2" />
        </GOSTR34102012-512-KeyValue>
    </KeyVal>
</KeyInfo>

<Signature>
</Signature>

The base64-encoded signed XML document:

77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTGiPzi48cm9vdD4NCiAgIDxB
YXRhVG9TaWwuIEIkJPSVJub1NpZ24iPkRhdeGBL0RhdGFUb1NpZ24iDQogICA8ICAgPC9U
cmFuc2Zvcm1zPg0KICAgICAgPC9UcmFuc2Zvcm1zPgoKICAgICAgICAgPC9ENhbm9uaWN
hbG16YXRpb25nZXRob2ogiPz4NCiAgICAgPC9UcmFuc2Zvcm1zPg0KICAgICAgICAgPC9
ENhbm9uaWNhbG16YXRpb25nZXRob2ogiPz4NCiAgICAgPC9UcmFuc2Zvcm1zPgoKICAg
ICAgPC9UcmFuc2Zvcm1zPgoKICAgICAgICAgPC9ENhbm9uaWNhbG16YXRpb25nZXRob2o

Signed XML document with GOST R 34.10-2001 algorithm in SignatureMethod element

The X.509 certificate from section 4.2 of [RFC4491] was used.

The x-coordinate of verification key:

0x577E324FE70F2B6DF45C437A0305E5FD2C89318C13CD0875401A26075689584

The y-coordinate of verification key:

0x601AEACBC660DFDB0C8BC7567EBBA6EA8DE40FAE857C9AD0038895B916CCEB8F

Corresponding signature key (d):

0x0B293BE050D0082BDAE785631A6BAB68F35B42786D6DDA56AFAF169891040F77

The k value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEFE33B0E270318857C
The h-bar value:

0xEF3E03620C2B0E87E43F503A839AB7868071EA28CA38AABD915D56A5F74400F4

The signed XML document:
<?xml version="1.0" encoding="utf-8"?>
<root>
  <DataToSign Id="ToSign">Data</DataToSign>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <Reference URI="#ToSign">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestValue>FVQbzF2djfNNJO3JG0OLfSOD1ZkibTcUmF2DS4nnuPY==</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>n2UHtdu25fPzJNYyojbNTq52V1D3UBVQqI5xNhdYopDpMjpeIN2H+3xyQ40/\nzslLn/owzvuu9zpaH3Q0BPaw==</SignatureValue>
    <KeyInfo>
      <KeyValue>
        <GOSTR34102001KeyValue xmlns="urn:ietf:params:xml:ns:cpxmlsec">
          <NamedCurve URI="urn:oid:1.2.643.2.2.36.0"/>
          <PublicKey>
            hJVodWACGkB1CM0TjDGJLP31BQN6Q1z0bSsP508yf1eP68wWuZWIA9
            CafIwu+SN6qa7flbHy7DfD2a8yuoaYA==
          </PublicKey>
        </GOSTR34102001KeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</root>
The base64-encoded signed XML document:

```
77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZw==
```

B.4. Signed XML document with X.509 certificate in KeyInfo element

The X.509 certificate from Appendix A of [R1323565.1.023-2018] was used.

The x-coordinate of verirification key:

```
0x971566CEDA436EE7678F7E84EBB721746C0B4747AA8FD2AB1453D0DFBA
```

The y-coordinate of verification key:

```
0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E2E24FF71F9CE643
```

Corresponding signature key (d):

0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E2E24FF71F9CE643
The k value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEFE33B0E270318857C

The h-bar value:

0x054D1DABB161D63424F8DABB2800708B00F78DA7582699E8F2F0A521C7CE8144

The signed XML document:

```xml
<?xml version="1.0" encoding="utf-8"?>
<root>
  <DataToSign Id="ToSign">Data</DataToSign>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <Reference URI="#ToSign">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestValue>9QLsxPPo7L1X6IXqwzjcNDmbFuCCGivQ1s61hcPuITM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>jcQJhWtWbTCV7bjFky5vGXXUFigc74FXRi791ZnFHK7pMjpeiN2H+3xyQ4O//nz</SignatureValue>
  </Signature>
</root>
```
The base64-encoded signed XML document:

```
77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0
XJl IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWdjIj4NCiAgI
CAgIDxT aWduZWRJbmZzPjpwYXJhbXM6 eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6
mAxjMjAxNjI1OS0yMDItMDMtMDMtMDQgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQWx
nbmNhcmQgPSJ3d3cuWjJnIj4NCiAgICAgICAgIDxT aWduZWRJbmZzPjpwYXJhbXM6 eG
1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6
```


[Page 40]
Signed XML document with GOST R 34.10-2012 algorithm and 256-bit verification key in DEREncodedKeyValue

The X.509 certificate from Appendix A of [R1323565.1.023-2018] was used.

The x-coordinate of verification key:

0x971566C6DA4366E7678F7E07E84EBB7217406C0B4747A8FD2B1453C3D0DFBA

The y-coordinate of verification key:

0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E24FF71F9CE643

Corresponding signature key:

0xBFCF1D623E5C3D30237A4923C46E43D640FFEAAF2C3ED39A8FA399924

The k value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEEF33B0E270318857C

The h-bar value:

0x05D1DABB161D63424F8DABB2800708B00F78DA7582699E8F2F0A521C7CE8144

The signed XML document:
<?xml version="1.0" encoding="utf-8"?>
<root>
  <DataToSign Id="ToSign">Data</DataToSign>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <Reference URI="#ToSign">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestValue>9QLsxPPc7LlX6IXqwzjcnDmbFvCCGivQ1s61hcPuITM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>jcQJhWtWbTCV7bJFky5vGXXUFigc74FXRi791zhFK7pmJpeIN2H+3xyQ40//nzss1Ln/owzvu92paH3Q0BPaw==</SignatureValue>
    <KeyInfo>
      <DEREncodedKeyValue xmlns="http://www.w3.org/2009/xmldsig11#">MGYwHwYIKoUDBwEBAQEwExYHkoUDAgIkAAyIKoUDBwEBAgIDQwAEQlrf0MNTFKvSj6pHrwtsQbduy07oB36Pz+duO9rOZhWXQ+acH/dP4uLxqJeHzq2Z30cDGd+KND4NZjp+UZwlzWKO==</DEREncodedKeyValue>
    </KeyInfo>
  </Signature>
</root>

The base64-encoded signed XML document:
Appendix C. Acknowledgments

We thank Ekaterina Smyshlyaeva and Evgeny Alekseev for their useful comments.

Authors’ Addresses

Pavel Smirnov (editor)
CryptoPro
18, Suschevsky val
Moscow 127018
Russian Federation

Phone: +7 (495) 995-48-20
Email: spv@cryptopro.ru