Network Working Group
Internet-Draft
Intended status: Informational
Expires: October 1, 2020

P. Smirnov, Ed.
M. Paramonova
M. Khomenko
A. Makarov
CryptoPro

March 30, 2020

GOST XML digital signature syntax
draft-smirnov-xmldsig-04

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 October 1, 2020.

Copyright Notice

Table of Contents

1. Introduction

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 [XMLDSIG].

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 [XMLDSIG].

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:

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).

XML schema name	XML namespace identifier	Prefix	Reference
DS schema	http://www.w3.org/2000/09/xmldsig#	ds	XMLDSIG
DSIG11 schema	http://www.w3.org/2009/xmldsig11#	dsig11	XMLDSIG
XS schema	http://www.w3.org/2001/XMLSchema	xs	XMLSCHEMA-1 XMLSCHEMA-2
CPXMLSEC schema	urn:ietf:params:xml:ns:cpxmlsec	cpxmlsec	This document

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:

```
<xs: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">
```

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"/>
        <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"/>
      <!-- (0,unbounded) elements from (1,1) external namespace -->
   </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.

```
<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.

```
<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.

```
<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.

```
<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.
- 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.

```
<xs:element name="KeyInfo" type="ds:KeyInfoType"/>

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

```
  <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:element ref="cpxmlsec:GOSTR34102012-256-KeyValue "/>
        <xs:element ref="cpxmlsec:GOSTR34102012-512-KeyValue "/>
        <xs:element ref="cpxmlsec:GOSTR34102001KeyValue "/> -->
        <!-- cpxmlsec:GOSTR34102012-256-KeyValue,
             cpxmlsec:GOSTR34102012-512-KeyValue,
             cpxmlsec:GOSTR34102001KeyValue will use the any element -->
        <xs:any namespace="##other" processContents="lax"/>
     </xs:choice>
  </xs:complexType>
```

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

6.3.1.1. The GOSTR34102012-256-KeyValue, GOSTR34102012-512-KeyValue and GOSTR34102001KeyValue elements

The cpxmlsec:GOSTR34102012-256-KeyValue, cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:GOSTR34102001KeyValue elements are a descendants of ds:KeyValue 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:PublicKey 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.

```
<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" />

<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 MUST contain the descendant ds:Transforms element. The ds:Transforms element identifies data transforms specified in ds:RetrievalMethod element attributes.

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

```
<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#" -->

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

<xs: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:

```
<ds:DigestMethod Algorithm=
"urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256" />
```

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:

```
urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512
```

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

```
<ds:DigestMethod Algorithm=
"urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512" />
```

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).

7.1.1.3. GOST R 34.11-94 algorithm in DigestMethod element

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

```
urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411
```

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:

```
<ds:DigestMethod Algorithm=
   "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411">
   <!-- 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):

```
urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-
256
```

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):

```
<ds:SignatureMethod Algorithm=
   "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-
   gostr34112012-256" />
```

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):

```
urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-
512
```

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):

```
<ds:SignatureMethod Algorithm=
   "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-
   gostr34112012-512" />
```

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:

```
urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411
```

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

```
<ds:SignatureMethod Algorithm=
   "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411"
/>
```

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 [R501113-2016].

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:

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

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

```
<ds:SignatureMethod Algorithm=
   "urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-256"
/>
```

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:

```
<ds:SignatureMethod Algorithm=
   "urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512"
/>
```

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:

```
<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:

urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyvalue

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 an 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:

```
<cpxmlsec:GOSTR34102012-256-KeyValue>
   <!-- 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:GOSTR34102012-256-KeyValue>
```

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:

urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyvalue

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 an 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:

```
<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:

```
urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue
```

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:

```
<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 for urn:ietf:params:xml:ns:cpxmlsec

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: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

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

8.2. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256" (see Section 7.1.1.1) per the guidelines in [RFC3688]:

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

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
          "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
     content="text/html;charset=iso-8859-1"/>
  <title>
      GOST R 34.11-2012 algorithm with 256-bit hash code in
      DigestMethod element
  </title>
</head>
<body>
  <h1>
      Namespace identifier for GOST R 34.11-2012 algorithm with
      256-bit hash code in DigestMethod element
  </h1>
  <h2>
  urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256
  </h2>
  <p>
      See Section 7.1.1.1 in
      <a href="https://tools.ietf.org/html/draft-smirnov-xmldsig-04">
      draft-smirnov-xmldsig-04</a>.
  </p>
</body>
</html>
```

8.3. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512" (see Section 7.1.1.2) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.11-2012 algorithm with 512-bit hash code in
            DigestMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.11-2012 algorithm with
            512-bit hash code in DigestMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512
        </h2>
        <p>
            See Section 7.1.1.2 in
                       <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.4. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411" (see Section 7.1.1.3) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.11-94 algorithm in DigestMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.11-94 algorithm in
            DigestMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411
        </h2>
        <p>
            See Section 7.1.1.3 in
                        <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.5. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec :algorithms:gostr34102012-gostr34112012-256

This section registers a new XML sub-namespace identifier, "urn:ietf: params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-256" (see Section 7.1.2.1) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34 112012-256

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.10-2012 algorithm with 256-bit key in
            SignatureMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.10-2012 algorithm with
            256-bit key in SignatureMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-
gostr34112012-256
        </h2>
        <p>
            See Section 7.1.2.1 in
                        <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.6. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec :algorithms:gostr34102012-gostr34112012-512

This section registers a new XML sub-namespace identifier, "urn:ietf: params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-512" (see Section 7.1.2.2) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34 112012-512

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.10-2012 algorithm with 512-bit key in
            SignatureMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.10-2012 algorithm with
            512-bit key in SignatureMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-
gostr34112012-512
        </h2>
        <p>
            See Section 7.1.2.2 in
                        <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.7. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411" (see Section 7.1.2.3) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.10-2001 algorithm in SignatureMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.10-2001 algorithm in
            SignatureMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411
        </h2>
        <p>
            See Section 7.1.2.3 in
                        <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.8. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-256

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-256" (see Section 7.2.1) per the guidelines in [RFC3688]:

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

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.11-2012 algorithm with 256-bit key in
            SignatureMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.11-2012 algorithm with
            256-bit key in SignatureMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-256
        </h2>
        <p>
            See Section 7.2.1 in
                       <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.9. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512" (see Section 7.2.2) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.11-2012 algorithm with 512-bit key in
            SignatureMethod element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.11-2012 algorithm with
            512-bit key in SignatureMethod element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512
        </h2>
        <p>
            See Section 7.2.2 in
                       <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.10. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyvalue

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyvalue" (see Section 7.3.2) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyvalue

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.10-2012 256-bit verification key in GOSTR34102012-256-
KeyValue element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.10-2012 256-bit
            verification key in GOSTR34102012-256-KeyValue element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyvalue
        </h2>
        <p>
            See Section 7.3.2 in
                       <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.11. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyvalue

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyvalue" (see Section 7.3.3) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyvalue

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.10-2012 512-bit verification key in GOSTR34102012-512-
KeyValue element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.10-2012 512-bit
            verification key in GOSTR34102012-512-KeyValue element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyvalue
        </h2>
        <p>
            See Section 7.3.3 in
                       <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.12. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue

This section registers a new XML sub-namespace identifier, "urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue" (see Section 7.3.4) per the guidelines in [RFC3688]:

URI: urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML:

```
      <?xml version="1.0"?>
      <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
                "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
      <html xmlns="http://www.w3.org/1999/xhtml">
      <head>
        <meta http-equiv="content-type"
           content="text/html;charset=iso-8859-1"/>
        <title>
            GOST R 34.10-2001 verification key in GOSTR34102001KeyValue element
        </title>
      </head>
      <body>
        <h1>
            Namespace identifier for GOST R 34.10-2001 verification
            key in GOSTR34102001KeyValue element
        </h1>
        <h2>
            urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue
        </h2>
        <p>
            See Section 7.3.4 in
                        <a href="https://tools.ietf.org/html/draft-smirnov-
xmldsig-04">
            draft-smirnov-xmldsig-04</a>.
        </p>
      </body>
      </html>
```

8.13. XML schema registration

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

URI: urn:ietf:params:xml:schema:cpxmlsec

Registrant Contact: Pavel Smirnov (spv@cryptopro.ru), Maria Paramonova (mparamonova@cryptopro.ru).

XML: The XML schema can be found in Appendix A.

9. References

9.1. Normative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3061] Mealling, M., "A URN Namespace of Object Identifiers", RFC 3061, DOI 10.17487/RFC3061, February 2001, <https://www.rfc-editor.org/info/rfc3061>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC4357] Popov, V., Kurepkin, I., and S. Leontiev, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms", RFC 4357, DOI 10.17487/RFC4357, January 2006, <https://www.rfc-editor.org/info/rfc4357>.

[RFC4491] Leontiev, S., Ed. and D. Shefanovski, Ed., "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 4491, DOI 10.17487/RFC4491, May 2006, <https://www.rfc-editor.org/info/rfc4491>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6986] Dolmatov, V., Ed. and A. Degtyarev, "GOST R 34.11-2012: Hash Function", RFC 6986, DOI 10.17487/RFC6986, August 2013, <https://www.rfc-editor.org/info/rfc6986>.

[RFC7091] Dolmatov, V., Ed. and A. Degtyarev, "GOST R 34.10-2012: Digital Signature Algorithm", RFC 7091, DOI 10.17487/RFC7091, December 2013, <https://www.rfc-editor.org/info/rfc7091>.

[RFC7836] Smyshlyaev, S., Ed., Alekseev, E., Oshkin, I., Popov, V., Leontiev, S., Podobaev, V., and D. Belyavsky, "Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012", RFC 7836, DOI 10.17487/RFC7836, March 2016, <https://www.rfc-editor.org/info/rfc7836>.

9.2. Informative References

[GOST3410-2012]
Federal Agency on Technical Regulating and Metrology, "Information technology. Cryptographic data security. Signature and verification processes of [electronic] digital signature", GOST R Version 1.1, 2012.

[GOST3411-2012]
Federal Agency on Technical Regulating and Metrology, "Information technology. Cryptographic Data Security. Hashing function", GOST R 34.11-2012, 2012.

[R1323565.1.023-2018]
Federal Agency on Technical Regulating and Metrology, "Information technology. Cryptographic information security. Usage of GOST R 34.10-2012 and GOST R 34.11-2012 algorithms in certificate, CRL and PKCS#10 certificate request in X.509 public key infrastructure", R 1323565.1.023-2018, 2019.

[R501113-2016]
Federal Agency on Technical Regulating and Metrology, "Information technology. Cryptographic Data Security. Guidelines on the Cryptographic Algorithms, Accompanying the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012", R 50.1.113-2016, 2016.

[XMLDSIG] The World Wide Web Consortium (W3C), "XML Signature Syntax and Processing", W3C Recommendation Version 1.1, 2013, <https://www.w3.org/TR/xmldsig-core1/>.

[XMLSCHEMA-1]
The World Wide Web Consortium (W3C), "XML Schema Part 1: Structures Second Edition", W3C Recommendation , 2004, <https://www.w3.org/TR/2004/REC-xmlschema-1-20041028/>.

[XMLSCHEMA-2]
The World Wide Web Consortium (W3C), "XML Schema Part 2: Datatypes Second Edition", W3C Recommendation , 2004, <https://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>.

Appendix A. CPXMLSEC XML schema

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Declare helper entities to avoid overrunning right margin of text
     while importing schemata.-->
<!DOCTYPE schema [
   <!ENTITY xmldsiguri
      "http://www.w3.org/TR/2008/REC-xmldsig-core-20080610">
]>

<xs: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#" />

   <xs:import namespace="http://www.w3.org/2009/xmldsig11#" />

   <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" />

</xs: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 verirification key:

0x971566CEDA436EE7678F7E07E84EBB7217406C0B4747AA8FD2AB1453C3D0DFBA

The y-coordinate of verirification 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"
         />
         <SignatureMethod Algorithm=
            "urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-
            gostr34112012-256"
         />
         <Reference URI="#ToSign">
            <Transforms>
               <Transform Algorithm=
                  "http://www.w3.org/TR/2001/REC-xml-c14n-
                  20010315"
               />
            </Transforms>
            <DigestMethod Algorithm=
               "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
               gostr34112012-256"
            />
            <DigestValue>
               9QLsxPPo7LlX6IXqwzjcNDmbFuCCGivQ1s61hcPuITM=
            </DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>
         jcQJhWtWbTCV7bjFky5vGXXUFigc74FXRi79lZnFHK7pMjpeiN2H+3xyQ4O//n
         zs1Ln/oqwzvu9zpaH3Q0BPaw==
      </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/Qw1MUq9KPqkdHC2xAF3K7TugHfo9n525D2s5mFZdD5pwf90/i4v
                  F0mFmr9nfRwMYP4o0Pg1mOn5RlaXNYrQ==
               </PublicKey>
            </GOSTR34102012-256-KeyValue>
         </KeyValue>
      </KeyInfo>
   </Signature>
</root>
```

The base64-encoded signed XML document:

77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0d
XJl IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4NCiAgI
CAgIDxT aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQ
Wxnb3JpdGht PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yM
DAxMDMxNSIgLz4N CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1c
m46aWV0ZjpwYXJhbXM6 eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEwM
jAxMi1nb3N0cjM0MTEyMDEy LTI1NiIgLz4NCiAgICAgICAgIDxSZWZlcmVuY2UgVVJJP
SIjVG9TaWduIj4NCiAgICAgICAg ICAgIDxUcmFuc2Zvcm1zPg0KICAgICAgICAgICAgI
CAgPFRyYW5zZm9ybSBBbGdvcml0aG09 Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvU
kVDLXhtbC1jMTRuLTIwMDEwMzE1IiAvPg0K ICAgICAgICAgICAgPC9UcmFuc2Zvcm1zP
g0KICAgICAgICAgICAgPERpZ2VzdE1ldGhvZCBB bGdvcml0aG09InVybjppZXRmOnBhc
mFtczp4bWw6bnM6Y3B4bWxzZWM6YWxnb3JpdGhtczpn b3N0cjM0MTEyMDEyLTI1NiIgL
z4NCiAgICAgICAgICAgIDxEaWdlc3RWYWx1ZT45UUxzeFBQ bzdMbFg2SVhxd3pqY05Eb
WJGdUNDR2l2UTFzNjFoY1B1SVRNPTwvRGlnZXN0VmFsdWU+DQog ICAgICAgICA8L1JlZ
mVyZW5jZT4NCiAgICAgIDwvU2lnbmVkSW5mbz4NCiAgICAgIDxTaWdu YXR1cmVWYWx1Z
T5qY1FKaFd0V2JUQ1Y3YmpGa3k1dkdYWFVGaWdjNzRGWFJpNzlsWm5GSEs3 cE1qcGVpT
jJIKzN4eVE0Ty8vbnpzMUxuL29xd3p2dTl6cGFIM1EwQlBhdz09PC9TaWduYXR1 cmVWY
Wx1ZT4NCiAgICAgIDxLZXlJbmZvPg0KICAgICAgICAgPEtleVZhbHVlPg0KICAgICAg I
CAgICAgPEdPU1RSMzQxMDIwMTItMjU2LUtleVZhbHVlIHhtbG5zPSJ1cm46aWV0ZjpwYX
Jh bXM6eG1sOm5zOmNweG1sc2VjIj4NCiAgICAgICAgICAgICAgIDxOYW1lZEN1cnZlIF
VSST0i dXJuOm9pZDoxLjIuNjQzLjIuMi4zNi4wIiAvPg0KICAgICAgICAgICAgICAgPF
B1YmxpY0tl eT51dC9RdzFNVXE5S1Bxa2RIQzJ4QUYzSzdUdWdIZm85bjUyNUQyczVtRl
pkRDVwd2Y5MC9p NHZGMG1GbXI5bmZSd01ZUDRvMFBnMW1PbjVSbGFYTllyUT09PC9QdW
JsaWNLZXk+DQogICAg ICAgICAgICA8L0dPU1RSMzQxMDIwMTItMjU2LUtleVZhbHVlPg
0KICAgICAgICAgPC9LZXlW
YWx1ZT4NCiAgICAgIDwvS2V5SW5mbz4NCiAgIDwvU2lnbmF0dXJlPg0KPC9yb290Pg==

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 verirification key:

0x07134627CE7FC6770953ABA4714B38AF8DE764B8870A502C2F4CC2D05541459A18DA3B
9D4EBC09BC06CB2EA1856A03747561CF04C34382111539230A550F1913

The y-coordinate of verirification key:

0x7E08A434CB2FA300F8974E3FF69A4BCDF36B6308E1D7A56144693A35E11CBD14D50291
6E680E35FE1E6ABBA85BD4DAE7065308B16B1CCABFE3D91CE0655B0FFD

Corresponding signature key (d):

0x3FC01CDCD4EC5F972EB482774C41E66DB7F380528DFE9E67992BA05AEE462435757530
E641077CE587B976C8EEB48C48FD33FD175F0C7DE6A44E014E6BCB074B

The k value:

0x72ABB44536656BF1618CE10BF7EADD40582304A51EE4E2A25A0A32CB0E773ABB23B7D8
FDD8FA5EEE91B4AE452F2272C86E1E2221215D405F51B5D5015616E1F6

The h-bar value:

0x33DEF8422879AA68482339BC65E5DCA9A5D77E80C5C0371DB13D3B88F4CCA8A89ED3CE
85849231DD61B35E4B47A3722317663859A2BE088C1BB6EEC87410DAF2

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"
         />
         <SignatureMethod Algorithm=
            "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
            gostr34102012-gostr34112012-512"
         />
         <Reference URI="#ToSign">
            <Transforms>
               <Transform Algorithm=
                  "http://www.w3.org/TR/2001/REC-xml-c14n-
                  20010315"
               />
            </Transforms>
            <DigestMethod Algorithm=
```

```
               "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
               gostr34112012-512"
            />
            <DigestValue>
               wiOFD9D7zKHNlo58t/9tUtCJA5ZO9vmDhMlt3HIkyXZvQxIp5PE+txwsI
               AVfUIOULvGTFxAZlwuHTB+qD5s54g==
            </DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>
         dn+oWg6n3wJ20kBmO1GvURc4SuZ3h3nKXYWy4uHdmeS2nlTlNWFKca4fTBlc+fp
         nCS8IEVNFX25Ndh4UXJLLNl2/L0wtancFiA+xRYzFgzUGW+pWIfyfvBdsSspbwe
         ZyJUWajqN3lDRZDchycEApNlqDpTtes8BpNrXSh+Cpg+c=
      </SignatureValue>
      <KeyInfo>
         <KeyValue>
            <GOSTR34102012-512-KeyValue xmlns=
               "urn:ietf:params:xml:ns:cpxmlsec">
               <NamedCurve URI="urn:oid:1.2.643.7.1.2.1.2.2" />
               <PublicKey>
                  ExkPVQojORURgkPDBM9hdXQDaoWhLssGvAm8Tp072hiaRUFV0MJMLy
                  xQCoe4ZOeNrzhLcaSrUwl3xn/OJ0YTB/0PW2XgHNnjv8oca7EIUwbn
                  2tRbqLtqHv41DmhukQLVFL0c4TU6aURhpdfhCGNr881LmvY/Tpf4AK
                  MvyzSkCH4=
               </PublicKey>
            </GOSTR34102012-512-KeyValue>
         </KeyValue>
      </KeyInfo>
   </Signature>
</root>
```

The base64-encoded signed XML document:

```
77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0d
XJl IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4NCiAgI
CAgIDxT aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQ
Wxnb3JpdGht PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yM
DAxMDMxNSIgLz4N CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1c
m46aWV0ZjpwYXJhbXM6 eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEwM
jAxMi1nb3N0cjM0MTEyMDEy LTUxMiIgLz4NCiAgICAgICAgIDxSZWZlcmVuY2UgVVJJP
SIjVG9TaWduIj4NCiAgICAgICAg ICAgIDxUcmFuc2Zvcm1zPg0KICAgICAgICAgICAgI
CAgPFRyYW5zZm9ybSBBbGdvcml0aG09 Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvU
kVDLXhtbC1jMTRuLTIwMDEwMzE1IiAvPg0K ICAgICAgICAgICAgPC9UcmFuc2Zvcm1zP
g0KICAgICAgICAgICAgPERpZ2VzdE1ldGhvZCBB bGdvcml0aG09InVybjppZXRmOnBhc
mFtczp4bWw6bnM6Y3B4bWxzZWM6YWxnb3JpdGhtczpn b3N0cjM0MTEyMDEyLTUxMiIgL
```

z4NCiAgICAgICAgICAgIDxEaWdlc3RWYWx1ZT53aU9GRDlE N3pLSE5sbzU4dC85dFV0Q
0pBNVpPOXZtRGhNbHQzSElreVhadlF4SXA1UEUrdHh3c0lBVmZV SU9VTHZHVEZ4QVpsd
3VIVEIrcUQ1czU0Zz09PC9EaWdlc3RWYWx1ZT4NCiAgICAgICAgIDwv UmVmZXJlbmNlP
g0KICAgICAgICAgPC9TaWduZWRJbmZvPg0KICAgICAgICAgPFNpZ25hdHVyZVZhbHVl PmRuK29XZ
zZuM3dKMjBrQm1PMUd2VVJjNFN1WjNoM25LWFlXeTR1SGRtZVMybmxUbE5XRktj YTRmV
EJsYytmcG5DUzhJRVZORlgyNU5kaDRVWEpMTE5sMi9MMHd0YW5jRmlBK3hSWXpGZ3pV R
1crcFdJZnlmdkJkc1NzcGJ3ZVp5SlVXYWpxTjNsRFJaRGNoeWNFQXBObHFEcFR0ZXM4Qn
BO clhTaCtDcGcrYz08L1NpZ25hdHVyZVZhbHVlPg0KICAgICAgPEtleUluZm8+DQogIC
AgICAg ICA8S2V5VmFsdWU+DQogICAgICAgICAgICA8R09TVFIzNDEwMjAxMi01MTItS2
V5VmFsdWUg eG1sbnM9InVybjppZXRmOnBhcmFtczp4bWw6bnM6Y3B4bWxzZWMiPg0KIC
AgICAgICAgICAg ICAgPE5hbWVkQ3VydmUgVVJJPSJ1cm46b2lkOjEuMi42NDMuNy4xLj
IuMS4yLjIiIC8+DQog ICAgICAgICAgICA8UHVibGljS2V5PkV4a1BWUW9qT1JVUm
drUERCTTloZFhRRGFvV2hM c3NHdkFtOFRwMDcyaGlhUlVGVjBNSk1MeXhRQ29lNFpPZU
5yemhMY2FTclV3bDN4bi9PSjBZ VEIvMFBXMlhnSE5uanY4b2NhN0VJVXdibjJ0UmJxTH
RxSHY0MURtaHVrUUxWRkwwYzRUVTZh VVJocGRmaENHTnI4ODFMbXZZL1RwZjRBS012eX
pTa0NIND08L1B1YmxpY0tleT4NCiAgICAg ICAgICAgICAgIDwvR09TVFIzNDEwMjAxMi01MT
ItS2V5VmFsdWU+DQogICAgICAgICA8L0tleVZh
bHVlPg0KICAgICAgPC9LZXlJbmZvPg0KICAgPC9TaWduYXR1cmU+DQo8L3Jvb3Q+

B.3. 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 verirification key:

0x577E324FE70F2B6DF45C437A0305E5FD2C89318C13CD0875401A026075689584

The y-coordinate of verirification key:

0x601AEACABC660FDFB0CBC7567EBBA6EA8DE40FAE857C9AD0038895B916CCEB8F

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"
         />
         <SignatureMethod Algorithm=
            "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
            gostr34102001-gostr3411"
         />
         <Reference URI="#ToSign">
            <Transforms>
               <Transform Algorithm=
                  "http://www.w3.org/TR/2001/REC-xml-c14n-
                  20010315"
               />
            </Transforms>
            <DigestMethod Algorithm=
               "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
               gostr3411"
            />
            <DigestValue>
               FVQbzF2djfNNJO3JG0OLfSODlZkibTcUmF2DS4nnuPY=
            </DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>
         n2UHtdu25fPzJNYyojbNTq52V1D3UBVQqI5xNhdYopDpMjpeiN2H+3xyQ4O//nz
         s1Ln/oqwzvu9zpaH3Q0BPaw==
      </SignatureValue>
      <KeyInfo>
         <KeyValue>
            <GOSTR34102001KeyValue xmlns=
               "urn:ietf:params:xml:ns:cpxmlsec">
               <NamedCurve URI="urn:oid:1.2.643.2.2.36.0" />
               <PublicKey>
                  hJVodWACGkB1CM0TjDGJLP3lBQN6Q1z0bSsP508yfleP68wWuZWIA9
                  CafIWuD+SN6qa7flbHy7DfD2a8yuoaYA==
               </PublicKey>
            </GOSTR34102001KeyValue>
         </KeyValue>
      </KeyInfo>
   </Signature>
</root>
```

The base64-encoded signed XML document:

77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0d
XJl IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4NCiAgI
CAgIDxT aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQ
Wxnb3JpdGht PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yM
DAxMDMxNSIgLz4N CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1c
m46aWV0ZjpwYXJhbXM6 eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEwM
jAwMS1nb3N0cjM0MTEiIC8+ DQogICAgICAgICA8UmVmZXJlbmNlIFVSST0iI1RvU2lnb
iI+DQogICAgICAgICAgICA8VHJh bnNmb3Jtcz4NCiAgICAgICAgICAgICAgIDxUcmFuc
2Zvcm0gQWxnb3JpdGhtPSJodHRwOi8v d3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtY
zE0bi0yMDAxMDMxNSIgLz4NCiAgICAgICAg ICAgIDwvVHJhbnNmb3Jtcz4NCiAgICAgI
CAgICAgIDxEaWdlc3RNZXRob2QgQWxnb3JpdGht PSJ1cm46aWV0ZjpwYXJhbXM6eG1sO
m5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEx IiAvPg0KICAgICAgICAgICAgP
ERpZ2VzdFZhbHVlPkZWUWJ6RjJkamZOTkpPM0pHME9MZlNP RGxaa2liVGNVbUYyRFM0b
m51UFk9PC9EaWdlc3RWYWx1ZT4NCiAgICAgICAgIDwvUmVmZXJl bmNlPg0KICAgICAgP
C9TaWduZWRJbmZvPg0KICAgICAgPFNpZ25hdHVyZVZhbHVlPm4yVUh0 ZHUyNWZQekpOW
XlvamJOVHE1MlYxRDNVQlZRcUk1eE5oZFlvcERwTWpwZWlOMkgrM3h5UTRP Ly9uenMxT
G4vb3F3enZ1OXpwYUgzUTBCUGF3PT08L1NpZ25hdHVyZVZhbHVlPg0KICAgICAg PEtle
UluZm8+DQogICAgICAgICA8S2V5VmFsdWU+DQogICAgICAgICAgICA8R09TVFIzNDEw M
jAwMUtleVZhbHVlIHhtbG5zPSJ1cm46aWV0ZjpwYXJhbXM6eG1sOm5zOmNweG1sc2VjIj
4N CiAgICAgICAgICAgICAgIDxOYW1lZEN1cnZlIFVSST0idXJuOm9pZDoxLjIuNjQzLj
IuMi4z Ni4wIiAvPg0KICAgICAgICAgICAgICAgPFB1YmxpY0tleT5oSlZvZFdBQ0drQj
FDTTBUakRH SkxQM2xCUU42UTF6MGJTc1A1MDh5ZmxlUDY4d1d1WldJQTlDYWZJV3VEK1
NONnFhN2ZsYkh5 N0RmRDJhOHl1b2FZQT09PC9QdWJsaWNLZXk+DQogICAgICAgICAgIC
A8L0dPU1RSMzQxMDIw MDFLZXlWYWx1ZT4NCiAgICAgICAgIDwvS2V5VmFsdWU+DQogIC
AgICA8L0tleUluZm8+DQog ICA8L1NpZ25hdHVyZT4NCjwvcm9vdD4=

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:

0x971566CEDA436EE7678F7E07E84EBB7217406C0B4747AA8FD2AB1453C3D0DFBA

The y-coordinate of verirification 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"
         />
         <SignatureMethod Algorithm=
            "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
            gostr34102012-gostr34112012-256"
         />
         <Reference URI="#ToSign">
            <Transforms>
               <Transform Algorithm=
                  "http://www.w3.org/TR/2001/REC-xml-c14n-
                  20010315"
               />
            </Transforms>
            <DigestMethod Algorithm=
               "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
               gostr34112012-256"
            />
            <DigestValue>
               9QLsxPPo7LlX6IXqwzjcNDmbFuCCGivQ1s61hcPuITM=
            </DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>
         jcQJhWtWbTCV7bjFky5vGXXUFigc74FXRi79lZnFHK7pMjpeiN2H+3xyQ4O//nz
```

```
         s1Ln/oqwzvu9zpaH3Q0BPaw==
      </SignatureValue>
      <KeyInfo>
         <X509Data>
            <X509Certificate>
               MIICYjCCAg+gAwIBAgIBATAKBggqhQMHAQEDAjBWMSkwJwYJKoZIhvcNA
               QkBFhpHb3N0UjM0MTAtMjAxMkBleGFtcGxlLmNvbTEpMCcGA1UEAxMgR2
               9zdFIzNDEwLTIwMTIgKDI1NiBiaXQpIGV4YW1wbGUwHhcNMTMxMTA1MTQ
               wMjM3WhcNMzAxMTAxMTQwMjM3WjBWMSkwJwYJKoZIhvcNAQkBFhpHb3N0
               UjM0MTAtMjAxMkBleGFtcGxlLmNvbTEpMCcGA1UEAxMgR29zdFIzNDEwL
               TIwMTIgKDI1NiBiaXQpIGV4YW1wbGUwZjAfBggqhQMHAQEBATATBgcqhQ
               MCAiQABggqhQMHAQECAgNDAARAut/Qw1MUq9KPqkdHC2xAF3K7TugHfo9
               n525D2s5mFZdD5pwf90/i4vF0mFmr9nfRwMYP4o0Pg1mOn5RlaXNYraOB
               wDCBvTAdBgNVHQ4EFgQU1fIeN1HaPbw+XWUzbkJ+kHJUT0AwCwYDVR0PB
               AQDAgHGMA8GA1UdEwQIMAYBAf8CAQEwfgYDVR0BBHcwdYAU1fIeN1HaPb
               w+XWUzbkJ+kHJUT0ChWqRYMFYxKTAnBgkqhkiG9w0BCQEWGkdvc3RSMzQ
               xMC0yMDEyQGV4YW1wbGUuY29tMSkwJwYDVQQDEyBHb3N0UjM0MTAtMjAx
               MiAoMjU2IGJpdCkgZXhhbXBsZYIBATAKBggqhQMHAQEDAgNBAF5bm4BbA
               RR6hJLEoWJkOsYV3Hd7kXQQjz3CdqQfmHrz6TI6Xojdh/t8ckODv/587N
               S5/6KsM77vc6Wh90NAT2s=
            </X509Certificate>
         </X509Data>
      </KeyInfo>
   </Signature>
</root>
```

The base64-encoded signed XML document:

```
77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0d
XJl IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4NCiAgI
CAgIDxT aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQ
Wxnb3JpdGht PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yM
DAxMDMxNSIgLz4N CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1c
m46aWV0ZjpwYXJhbXM6 eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEwM
jAxMi1nb3N0cjM0MTEyMDEy LTI1NiIgLz4NCiAgICAgICAgIDxSZWZlcmVuY2UgVVJJP
SIjVG9TaWduIj4NCiAgICAgICAg ICAgIDxUcmFuc2Zvcm1zPg0KICAgICAgICAgICAgI
CAgPFRyYW5zZm9ybSBBbGdvcml0aG09 Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvU
kVDLXhtbC1jMTRuLTIwMDEwMzE1IiAvPg0K ICAgICAgICAgICAgPC9UcmFuc2Zvcm1zP
g0KICAgICAgICAgICAgPERpZ2VzdE1ldGhvZCBB bGdvcml0aG09InVybjppZXRmOnBhc
mFtczp4bWw6bnM6Y3B4bWxzZWM6YWxnb3JpdGhtczpn b3N0cjM0MTEyMDEyLTI1NiIgL
z4NCiAgICAgICAgICAgIDxEaWdlc3RWYWx1ZT45UUxzeFBQ bzdMbFg2SVhxd3pqY05Eb
WJGdUNDR2l2UTFzNjFoY1B1SVRNPTwvRGlnZXN0VmFsdWU+DQog ICAgICAgICA8L1JlZ
mVyZW5jZT4NCiAgICAgICAgIDwvU2lnbmVkSW5mbz4NCiAgICAgICAgIDxTaWdu YXR1cmVWYWx1Z
T5qY1FKaFd0V2JUQ1Y3YmpGa3k1dkdYWFVGaWdjNzRGWFJpNzlsWm5GSEs3 cE1qcGVpT
jJIKzN4eVE0Ty8vbnpzMUxuL29xd3p2dTl6cGFIM1EwQlBhdz09PC9TaWduYXR1 cmVWY
```

Wx1ZT4NCiAgICAgIDxLZXlJbmZvPg0KICAgICAgICAgPFg1MDlEYXRhPg0KICAgICAg I
CAgICAgPFg1MDlDZXJ0aWZpY2F0ZT5NSUlDWWpDQ0FnK2dBd0lCQWdJQkFUQUtCZ2dxaF
FN SEFRRURBakJXTVNrd0p3WUpLb1pJaHZjTkFRa0JGaHBIYjNOMFVqTTBNVEF0TWpBeE
1rQmxl R0Z0Y0d4bExtTnZiVEVwTUNjR0ExVUVBeE1nUjI5emRGSXpOREV3TFRJd01USW
dLREkxTmlC aWFYUXBJR1Y0WVcxd2JHVXdIaGNOTVRNeE1UQTFNVFF3TWpNM1doY05Nek
F4TVRBeE1UUXdN ak0zV2pCV01Ta3dKd1lKS29aSWh2Y05BUWtCRmhwSGIzTjBVak0wTV
RBdE1qQXhNa0JsZUdG dGNHeGxMbU52YlRFcE1DY0dBMVVFQXhNZ1IyOXpkRkl6TkRFd0
xUSXdNVElnS0RJMU5pQmlh WFFwSUdWNFlXMXdiR1V3WmpBZkJnZ3FoUU1IQVFFQkFUQV
RCZ2NxaFFNQ0FpUUFCZ2dxaFFN SEFRRUNBZ05EQUFSQXV0L1F3MU1VcTlLUHFrZEhDMn
hBRjNLN1R1Z0hmbzluNTI1RDJzNW1G WmRENXB3ZjkwL2k0dkYwbUZtcjluZlJ3TVlQNG
8wUGcxbU9uNVJsYVhOWXJhT0J3RENCdlRB ZEJnTlZIUTRFRmdRVTFmSWVOMUhhUGJ3K1
hXVXpia0ora0hKVVQwQXdDd1lEVlIwUEJBUURB Z0hHTUE4R0ExVWRFd1FJTUFZQkFmOE
NBUUV3ZmdZRFZSMEJCSGN3ZFlBVTFmSWVOMUhhUGJ3 K1hXVXpia0ora0hKVVQwQ2hXcV
JZTUZZeEtUQW5CZ2txaGtpRzl3MEJDUUVXR2tkdmMzUlNN elF4TUMweU1ERXlRR1Y0WV
cxd2JHVXVZMjl0TVNrd0p3WURWUVFERXlCSGIzTjBVak0wTVRB dE1qQXhNaUFvTWpVMk
lHSnBkQ2tnWlhoaGJYQnNaWUlCQVRBS0JnZ3FoUU1IQVFFREFnTkJB RjVibTRCYkFSUj
ZoSkxFb1dKa09zWVYzSGQ3a1hRUWp6M0NkcVFmbUhyejZUSTZYb2pkaC90 OGNrT0R2Lz
U4N05TNS82S3NNNzd2YzZXaDkwTkFUMnM9PC9YNTA5Q2VydGlmaWNhdGU+DQog ICAgIC
AgICA8L1g1MDlEYXRhPg0KICAgICAgPC9LZXlJbmZvPg0KICAgPC9TaWduYXR1cmU+
DQo8L3Jvb3Q+

B.5. 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 verirification key:

0x971566CEDA436EE7678F7E07E84EBB7217406C0B4747AA8FD2AB1453C3D0DFBA

The y-coordinate of verirification key:

0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E2E24FF71F9CE643

Corresponding signature key:

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"
         />
         <SignatureMethod Algorithm=
            "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
            gostr34102012-gostr34112012-256"
         />
         <Reference URI="#ToSign">
            <Transforms>
               <Transform Algorithm=
                  "http://www.w3.org/TR/2001/REC-xml-c14n-
                  20010315"
               />
            </Transforms>
            <DigestMethod Algorithm=
               "urn:ietf:params:xml:ns:cpxmlsec:algorithms:
               gostr34112012-256"
            />
            <DigestValue>
               9QLsxPPo7LlX6IXqwzjcNDmbFuCCGivQ1s61hcPuITM=
            </DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>
         jcQJhWtWbTCV7bjFky5vGXXUFigc74FXRi79lZnFHK7pMjpeiN2H+3xyQ4O//nz
         s1Ln/oqwzvu9zpaH3Q0BPaw==
      </SignatureValue>
      <KeyInfo>
         <DEREncodedKeyValue xmlns="http://www.w3.org/2009/xmldsig11#">
            MGYwHwYIKoUDBwEBAQEwEwYHKoUDAgIkAAYIKoUDBwEBAgIDQwAEQLrf0MNT
            FKvSj6pHRwtsQBdyu07oB36PZ+duQ9rOZhWXQ+acH/dP4uLxdJhZq/Z30cDG
            D+KND4NZjp+UZWlzWK0=
         </DEREncodedKeyValue>
      </KeyInfo>
   </Signature>
</root>
```

The base64-encoded signed XML document:

77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0d
XJl IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj4NCiAgI
CAgIDxT aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQ
Wxnb3JpdGht PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yM
DAxMDMxNSIgLz4N CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1c
m46aWV0ZjpwYXJhbXM6 eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEwM
jAxMi1nb3N0cjM0MTEyMDEy LTI1NiIgLz4NCiAgICAgICAgIDxSZWZlcmVuY2UgVVJJP
SIjVG9TaWduIj4NCiAgICAgICAg ICAgICAgIDxUcmFuc2Zvcm1zPg0KICAgICAgICAgICAgI
CAgPFRyYW5zZm9ybSBBBbGdvcml0aG09 Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvU
kVDLXhtbC1jMTRuLTIwMDEwMzE1IiAvPg0K ICAgICAgICAgICAgPC9UcmFuc2Zvcm1zP
g0KICAgICAgICAgICAgPERpZ2VzdE1ldGhvZCBB bGdvcml0aG09InVybjppZXRmOnBhc
mFtczp4bWw6bnM6Y3B4bWxzZWM6YWxnb3JpdGhtczpn b3N0cjM0MTEyMDEyLTI1NiIgL
z4NCiAgICAgICAgICAgIDxEaWdlc3RWYWx1ZT45UUxzeFBQ bzdMbFg2SVhxd3pqY05Eb
WJGdUNDR2l2UTFzNjFoY1B1SVRNPTwvRGlnZXN0VmFsdWU+DQog ICAgICAgICA8L1JlZ
mVyZW5jZT4NCiAgICAgICAgIDwvU2lnbmVkSW5mbz4NCiAgICAgICAgIDxTaWdu YXR1cmVWYWx1Z
T5qY1FKaFd0V2JUQ1Y3YmpGa3k1dkdYWFVGaWdjNzRGWFJpNzlsWm5GSEs3 cE1qcGVpT
jJIKzN4eVE0Ty8vbnpzMUxuL29xd3p2dTl6cGFIM1EwQlBhdz09PC9TaWduYXR1 cmVWY
Wx1ZT4NCiAgICAgICAgIDxLZXlJbmZvPg0KICAgICAgICAgICAgPERFUkVuY29kZWRLZXlWYWx1 Z
SB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwOS94bWxkc2lnMTEjIj5NR1l3SHdZSU
tv VURCd0VCQVFFd0V3WUhLb1VEQWdJa0FBWUlLb1VEQndFQkFnSURRd0FFUUxyZjBNTl
RGS3ZT ajZwSFJ3dHNRQmR5dTA3b0IzNlBaK2R1UTlyT1poV1hRK2FjSC9kUDR1THhkSm
hacS9aMzBj REdEK0tORDROWmpwK1VaV2x6V0swPTwvREVSRW5jb2RlZEtleVZhbHVlPg
0KICAgICAgICAgICAgPC9L ZXlJbmZvPg0KICAgPC9TaWduYXR1cmU+DQo8L3Jvb3Q+

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

Maria Paramonova
CryptoPro
18, Suschevsky val
Moscow 127018
Russian Federation

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

Mikhail Khomenko
CryptoPro
18, Suschevsky val
Moscow 127018
Russian Federation

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

Artyom Makarov
CryptoPro
18, Suschevsky val
Moscow 127018
Russian Federation

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