

Workgroup: Network Working Group  
Internet-Draft: draft-smirnov-xmldsig-05  
Published: 5 May 2022  
Intended Status: Informational  
Expires: 6 November 2022

A P.V. Smirnov, Ed. M.V. Paramonova M.V. Khomenko  
uCryptoPro CryptoPro CryptoPro  
t  
h  
o  
r  
s  
:  
A.O. Makarov  
CryptoPro

## Using GOST Algorithms for XML Digital Signatures

### Abstract

This document defines new algorithm identifiers for GOST cryptographic algorithms and methods of including GOST-based digital signature and hash-based message authentication code (HMAC) within the XML document. All statements in this document are technically equivalent to [[R1323565.1.033-2020](#)].

### 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 6 November 2022.

### Copyright Notice

Copyright (c) 2022 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

- [1. Introduction](#)
- [1.1. Requirements language](#)
- [2. XML Namespaces and Prefixes](#)
- [3. Using GOST Algorithms to Construct an XML Digital Signature Elements](#)
  - [3.1. Hash Algorithm in DigestMethod Element](#)
    - [3.1.1. GOST R 34.11-2012 Algorithm with 256-bit Hash Code in DigestMethod Element](#)
    - [3.1.2. GOST R 34.11-2012 Algorithm with 512-bit Hash Code in DigestMethod Element](#)
    - [3.1.3. GOST R 34.11-94 Algorithm in DigestMethod Element](#)
  - [3.2. Signature Algorithm in SignatureMethod Element](#)
    - [3.2.1. GOST R 34.10-2012 Algorithm with 256-bit Key in SignatureMethod Element](#)
    - [3.2.2. GOST R 34.10-2012 Algorithm with 512-bit Key in SignatureMethod Element](#)
    - [3.2.3. GOST R 34.10-2001 Algorithm in SignatureMethod Element](#)
  - [3.3. HMAC Algorithm in SignatureMethod Element](#)
    - [3.3.1. GOST R 34.11-2012 algorithm with 256-bit key in SignatureMethod Element](#)
    - [3.3.2. GOST R 34.11-2012 algorithm with 512-bit key in SignatureMethod Element](#)
- [4. Including GOST-based Key Material in XML Digital Signature](#)
  - [4.1. Public Key in DEREncodedKeyValue Element](#)
  - [4.2. Public Key in KeyValue Element](#)
    - [4.2.1. GOST R 34.10-2012 256-bit Public Key in GOSTR34102012-256-KeyValue Element](#)
    - [4.2.2. GOST R 34.10-2012 512-bit Public Key in GOSTR34102012-512-KeyValue Element](#)
    - [4.2.3. GOST R 34.10-2001 Public Key in GOSTR34102001KeyValue Element](#)
  - [4.3. Public Key Reference in RetrievalMethod Element](#)
- [5. IANA Considerations](#)
  - [5.1. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec](#)
  - [5.2. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-256](#)
  - [5.3. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34112012-512](#)
  - [5.4. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr3411](#)
  - [5.5. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-256](#)
  - [5.6. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-gostr34112012-512](#)
  - [5.7. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102001-gostr3411](#)
  - [5.8. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-256](#)
  - [5.9. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:algorithms:hmac-gostr34112012-512](#)
  - [5.10. XML Sub-namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyvalue](#)

- [5.11. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyvalue](#)
- [5.12. XML Sub-Namespace Registration for urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue](#)
- [5.13. XML Schema Registration](#)
- 6. References**
  - [6.1. Normative References](#)
  - [6.2. Informative References](#)
- [Appendix A. CPXMLSEC XML Schema](#)
- [Appendix B. Test Examples](#)
  - [B.1. Signed XML document with GOST R 34.10-2012 algorithm and 256-bit hash code in DigestMethod element](#)
  - [B.2. Signed XML document with GOST R 34.10-2012 algorithm and 512-bit hash code in DigestMethod element](#)
  - [B.3. Signed XML document with GOST R 34.10-2001 algorithm in SignatureMethod element](#)
  - [B.4. Signed XML document with X.509 certificate in KeyInfo element](#)
  - [B.5. Signed XML document with GOST R 34.10-2012 algorithm and 256-bit public key in DEREncodedKeyValue](#)
- [Appendix C. Acknowledgments](#)
- [Authors' Addresses](#)

## 1. Introduction

This document specifies identifiers (see [Section 3](#)) for the following Russian digital signature and hash algorithms (GOST algorithms):

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

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

This document specifies identifiers (see [Section 3.3](#)) for GOST-based HMAC transformations defined in the R 50.1.113-2016 [[R501113-2016](#)] (the English version can be found in [[RFC7836](#)]).

These identifiers are meant to use in XML Digital Signature Syntax (see [[XMLDSIG](#)]).

In addition, new methods of carrying GOST-based key material within XML documents are defined (see [Section 4](#)).

Also included are namespace identifiers, prefixes and XML schema definition required to make specification complete (see [Section 2](#)).

### 1.1. Requirements language

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](#)].

## 2. XML Namespaces and Prefixes

This document uses XML elements from four different XML schemas (see Table 1). Every XML schema is assigned to one XML namespace. The

following XML namespace identifier MUST be used as targetNamespace in the XML schema preamble:

urn:ietf:params:xml:ns:cpxmlsec

The other XML namespaces are external. Their identifiers are specified in XML schema preamble in corresponding attributes.

Table 1 lists full set of XML namespaces used in this document, identifiers and assigned prefixes. Table 1 also defines abbreviations for corresponding XML schemas.

XML schema name	XML namespace identifier	Prefix	Re
DS schema	http://www.w3.org/2000/09/xmldsig#	ds	[
DSIG11 schema	http://www.w3.org/2009/xmldsig11#	dsig11	[
XS schema	http://www.w3.org/2001/XMLSchema	xs	[XM [XM
CPXMLSEC schema	urn:ietf:params:xml:ns:cpxmlsec	cpxmlsec	This

Table 1

Any element or attribute whose name starts with the prefix from the Table 1 is considered to belong to the corresponding XML schema. This document uses prefixes to prevent possible collisions with elements of same names from different namespaces. Chosen prefixes have no special meaning and MAY be replaced by others.

The CPXMLSEC schema extends DS schema to support GOST algorithms. The CPXMLSEC schema uses XS schema elements (see [\[XMLSCHEMA-1\]](#) and [\[XMLSCHEMA-2\]](#)). The DS schema and DSIG11 schema definitions are described in accordance with [\[XMLDSIG\]](#).

The subsequent CPXMLSEC schema preamble is to be used with XML Schema definitions given in the remaining sections of this document.

```
<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">
```

### 3. Using GOST Algorithms to Construct an XML Digital Signature Elements

#### 3.1. Hash Algorithm in DigestMethod Element

##### 3.1.1. GOST R 34.11-2012 Algorithm with 256-bit Hash Code in DigestMethod Element

For 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
```

The following sample includes 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 and base64-encoded [[RFC4648](#)], then it is included in the ds:DigestValue element (see Section 4.4.3.6 of [[XMLDSIG](#)]).

##### 3.1.2. GOST R 34.11-2012 Algorithm with 512-bit Hash Code in DigestMethod Element

For 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
```

The following sample includes GOST R 34.11-2012 algorithm with 512-bit hash code in the ds:DigestMethod element:

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

The hash code MUST be represented in little-endian and base64-encoded [[RFC4648](#)], then it is included in the ds:DigestValue element (see Section 4.4.3.6 of [[XMLDSIG](#)]).

##### 3.1.3. GOST R 34.11-94 Algorithm in DigestMethod Element

The following identifier MUST be used for GOST R 34.11-94 algorithm to provide backward compatibility:

```
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.

If present, hash algorithm parameters MUST be included in the "URI" attribute of the cpxmlsec:NamedParameters element. Parameters are indicated by OIDs and MUST be formatted in accordance with [\[RFC3061\]](#). OIDs defined in section 8.2 of [\[RFC4357\]](#) MAY be used.

If the cpxmlsec:NamedParameters element is not included, id-GostR3411-94-CryptoProParamSet (see [\[RFC4357\]](#)) MUST be presumed.

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

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

The following sample includes GOST R 34.11-94 algorithm in the 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 and base64-encoded [\[RFC4648\]](#), then it is included in the ds:DigestValue element (see Section 4.4.3.6 of [\[XMLDSIG\]](#)).

## 3.2. Signature Algorithm in SignatureMethod Element

### 3.2.1. GOST R 34.10-2012 Algorithm with 256-bit Key in SignatureMethod Element

For GOST R 34.10-2012 algorithm with 256-bit private key the following identifier MUST be used (without line break in the identifier):

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

The following sample includes GOST R 34.10-2012 algorithm with 256-bit private key in the ds:SignatureMethod element (without line break in the attribute value):

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

Digital signature value MUST be represented in accordance with [R1323565.1.023-2018] and base64-encoded [RFC4648], then it is included in the ds:SignatureValue element (see Section 4.3 of [XMLDSIG]).

### 3.2.2. GOST R 34.10-2012 Algorithm with 512-bit Key in SignatureMethod Element

For GOST R 34.10-2012 algorithm with 512-bit private key the following identifier MUST be used (without line break in the identifier):

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

The following sample includes GOST R 34.10-2012 algorithm with 512-bit private key in the ds:SignatureMethod element (without line break in the attribute value):

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

Digital signature value MUST be represented in accordance with [R1323565.1.023-2018] and base64-encoded [RFC4648], then it is included in ds:SignatureValue element (see Section 4.3 of [XMLDSIG]).

### 3.2.3. GOST R 34.10-2001 Algorithm in SignatureMethod Element

The following identifier MUST be used for GOST R 34.10-2001 algorithm to provide backward compatibility:

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

The following sample includes GOST R 34.10-2001 algorithm in the ds:SignatureMethod element:

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

Digital signature value MUST be represented in accordance with [R1323565.1.023-2018] and base64-encoded [RFC4648], then it is included in the ds:SignatureValue element (see Section 4.3 of [XMLDSIG]).

### 3.3. HMAC Algorithm in SignatureMethod Element

GOST R 34.11-2012 algorithm MAY be used in HMAC mechanism in accordance with section 6.3.1 [[XMLDSIG](#)] and section 4.1.1 [[R501113-2016](#)].

#### 3.3.1. GOST R 34.11-2012 algorithm with 256-bit key in SignatureMethod Element

For 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
```

The following sample includes GOST R 34.11-2012 algorithm with 256-bit hash code in the 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 and base64-encoded [[RFC4648](#)], then it is included in the ds:SignatureValue element (see Section 4.3 of [[XMLDSIG](#)]).

#### 3.3.2. GOST R 34.11-2012 algorithm with 512-bit key in SignatureMethod Element

For 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
```

The following sample includes GOST R 34.11-2012 algorithm with 512-bit hash code in the 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 and base64-encoded [[RFC4648](#)], then it is included in the ds:SignatureValue element (see Section 4.3 of [[XMLDSIG](#)]).

## 4. Including GOST-based Key Material in XML Digital Signature

The information about GOST-based key material or HMAC symmetric key MAY be included in XML digital signature in any way in accordance



with [XMLDSIG]. In addition, this document defines new ways to enclose public keys of GOST algorithms: in descendants of the dsig11:DEREncodedKeyValue element (see Section 4.5.9 of [XMLDSIG]), in the ds:KeyValue element (see Section 4.2) and using the "Type" attribute of the ds:RetrievalMethod element (see Section 4.3).

#### 4.1. Public Key in DEREncodedKeyValue Element

The dsig11:DEREncodedKeyValue element is a descendant of the ds:KeyInfo (see Section 4.5 of [XMLDSIG]) element. To include the public key and its parameters into the dsig11:DEREncodedKeyValue element, the SubjectPublicKeyInfo structure MUST be used. This structure MUST be encoded in accordance with [R1323565.1.023-2018]. Then this key material MUST be represented in accordance with Section 4.5.9 of [XMLDSIG].

#### 4.2. Public Key in KeyValue Element

The ds:KeyValue element is a descendant of the ds:KeyInfo (see Section 4.5 of [XMLDSIG]) element. This element contains the public key and its parameters.

For GOST algorithms one of the following extra descendants MUST be included in the ds:KeyValue element:

- \*cpxmlsec:GOSTR34102012-256-KeyValue element;
- \*cpxmlsec:GOSTR34102012-512-KeyValue element;
- \*cpxmlsec:GOSTR34102001KeyValue element.

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

```
<xs:element name="KeyValue" type="ds:KeyValue" />
<xs:complexType name="KeyValue" 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>
```

Each of cpxmlsec:GOSTR34102012-256-KeyValue, cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:GOSTR34102001KeyValue elements have

cpxmlsec:GOSTKeyValue type (see schema definition below) and MUST contain the following descendants:

- \*cpxmlsec:NamedCurve element - contains an elliptic curve identifier;

- \*cpxmlsec:PublicKey element - contains a public key.

Each of cpxmlsec:NamedCurve and cpxmlsec:PublicKey elements belong to cpxmlsec namespace. The cpxmlsec:NamedCurve element has dsig11:NamedCurveType type. The cpxmlsec:PublicKey element has dsig11:ECPointType type. Both types belong to DSIG11 schema [[XMLDSIG](#)].

Each of 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>
```

Each of cpxmlsec:GOSTR34102012-256-KeyValue, cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:GOSTR34102001KeyValue elements MUST be represented in accordance with [Section 4.2.1-Section 4.2.3](#).

#### **4.2.1. GOST R 34.10-2012 256-bit Public Key in GOSTR34102012-256-KeyValue Element**

The elliptic curve identifier (public key parameters) MUST be included in the "URI" attribute of the cpxmlsec:NamedCurve element (see [Section 4.2](#)). In case of public key parameters described by OIDs they SHOULD be represented in accordance with [[RFC3061](#)]. OID identifiers for GOST algorithms are defined in [[R1323565.1.023-2018](#)].

The public key MUST be included in the cpxmlsec:GOSTR34102012-256-KeyValue element. It MUST be represented in the same way as subjectPublicKey field of SubjectPublicKeyInfo structure

[[R1323565.1.023-2018](#)] without enclosing in 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 (see [[XMLDSIG](#)]). The XML schema of cpxmlsec:GOSTR34102012-256-KeyValue and cpxmlsec:PublicKey elements is defined in [Section 4.2](#).

The following sample includes key material in the cpxmlsec:GOSTR34102012-256-KeyValue element:

```
<cpxmlsec:GOSTR34102012-256-KeyValue>
  <!-- id-tc26-gost-3410-2012-256-paramSetA -->
  <cpxmlsec:NamedCurve URI="urn:oid:1.2.643.7.1.2.1.1.1" />
  <cpxmlsec:PublicKey>
    <!-- The public key value -->
  </cpxmlsec:PublicKey>
</cpxmlsec:GOSTR34102012-256-KeyValue>
```

#### **4.2.2. GOST R 34.10-2012 512-bit Public Key in GOSTR34102012-512-KeyValue Element**

The elliptic curve identifier (public key parameters) MUST be included in the "URI" attribute of the cpxmlsec:NamedCurve element (see [Section 4.2](#)). In case of public key parameters described by OIDs they SHOULD be represented in accordance with [[RFC3061](#)]. OID identifiers for GOST algorithms are defined in [[R1323565.1.023-2018](#)].

The public key MUST be included in cpxmlsec:GOSTR34102012-512-KeyValue element. It MUST be represented in the same way as subjectPublicKey field of SubjectPublicKeyInfo structure [[R1323565.1.023-2018](#)] without enclosing in 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 (see [[XMLDSIG](#)]). The XML schema of cpxmlsec:GOSTR34102012-512-KeyValue and cpxmlsec:PublicKey elements is defined in [Section 4.2](#).

The following sample includes key material in the 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 public key value -->
  </cpxmlsec:PublicKey>
</cpxmlsec:GOSTR34102012-512-KeyValue>
```

#### **4.2.3. GOST R 34.10-2001 Public Key in GOSTR34102001KeyValue Element**

The elliptic curve identifier (public key parameters) MUST be included in the "URI" attribute of the cpxmlsec:NamedCurve element (see [Section 4.2](#)). In case of public key parameters described by

OIDs they SHOULD be represented in accordance with [RFC3061]. OID identifiers for GOST algorithms are defined in section 8.4 of [RFC4357].

The public key MUST be included in cpxmlsec:GOSTR34102001KeyValue element. It MUST be represented in the same way as subjectPublicKey field of SubjectPublicKeyInfo structure [R1323565.1.023-2018] without enclosing in OCTET STRING and DER encoding. This string MUST be base64-encoded [RFC4648] and included in the cpxmlsec:GOSTR34102001KeyValue similar to the ds:RSAKeyValue (see [XMLDSIG]). The XML schema of cpxmlsec:GOSTR34102001KeyValue and cpxmlsec:PublicKey elements is defined in Section 4.2.

The following sample includes key material in the 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 public key value -->
  </cpxmlsec:PublicKey>
</cpxmlsec:GOSTR34102001KeyValue>
```

#### 4.3. Public Key Reference in RetrievalMethod Element

The GOST public key MAY be referenced in the ds:RetrievalMethod element. In this case the public key reference MUST be included in the "URI" attribute. If the "Type" attribute is present one of the following identifiers MUST be used.

For GOST R 34.10-2012 algorithm with 256-bit private key:

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

For GOST R 34.10-2012 algorithm with 512-bit private key:

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

For GOST R 34.10-2001 algorithm:

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

## 5. IANA Considerations

### 5.1. 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 2](#)) 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.

### 5.2. 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 3.1.1](#)) 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 4.1.1 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlldsig-0
    draft-smirnov-xmlldsig-05">
  </p>
</body>
</html>

```

### 5.3. 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 3.1.2](#)) 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 4.1.2 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

#### 5.4. 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 3.1.3](#)) 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 4.1.3 in
    <a href="https://tools.ietf.org/html/draft-smirnov-
    draft-smirnov-xmlldsig-05">
    draft-smirnov-xmlldsig-05</a>.
  </p>
</body>
</html>

```

### 5.5. 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 3.2.1](#)) per the guidelines in [\[RFC3688\]](#):

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-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 34.10-2012 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-gos
  </h2>
  <p>
    See Section 4.2.1 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

## 5.6. 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 3.2.2](#)) per the guidelines in [\[RFC3688\]](#):

URI: urn:ietf:params:xml:ns:cpxmlsec:algorithms:gostr34102012-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 34.10-2012 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-gos
  </h2>
  <p>
    See Section 4.2.2 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

### 5.7. 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 3.2.3](#)) 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-gos
  </h2>
  <p>
    See Section 4.2.3 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

### 5.8. 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 3.3.1](#)) 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/xhtml1-basic/xhtml1-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-gostr3411201
  </h2>
  <p>
    See Section 4.3.1 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

### 5.9. 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 3.3.2](#)) 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-gostr3411201
  </h2>
  <p>
    See Section 4.3.2 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

#### 5.10. 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 4.3](#)) 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 public key at external location
  </title>
</head>
<body>
  <h1>
    Namespace identifier for GOST R 34.10-2012 256-bit
    public key at external location
  </h1>
  <h2>
    urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-256-keyv
  </h2>
  <p>
    See Section 5.3 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlldsig-05">
    draft-smirnov-xmlldsig-05</a>.
  </p>
</body>
</html>

```

### 5.11. 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 4.3](#)) 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 public key at external location
  </title>
</head>
<body>
  <h1>
    Namespace identifier for GOST R 34.10-2012 512-bit
    public key at external location
  </h1>
  <h2>
    urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102012-512-keyv
  </h2>
  <p>
    See Section 5.3 in
    <a href="https://tools.ietf.org/html/draft-smirnov-xmlsig-05">
    draft-smirnov-xmlsig-05</a>.
  </p>
</body>
</html>

```

## 5.12. 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 4.3](#)) 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/xhtml1-basic/xhtml1-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 public key at external location
  </title>
</head>
<body>
  <h1>
    Namespace identifier for GOST R 34.10-2001 public
    key at external location
  </h1>
  <h2>
    urn:ietf:params:xml:ns:cpxmlsec:types:gostr34102001-keyvalue
  </h2>
  <p>
    See Section 5.3 in
    <a href="https://tools.ietf.org/html/draft-smirnov-
    draft-smirnov-xmlldsig-05">
  </p>
</body>
</html>

```

### 5.13. XML Schema Registration

This section registers an XML schema 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: The XML schema can be found in [Appendix A](#).

## 6. References

### 6.1. 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>>.

## 6.2. 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.

**[R1323565.1.033-2020]** Technical Committee 26 "Cryptography and Security Mechanisms", "Using Russian algorithms of digital signature with XML-based protocols and messages", TC 26 Recommendation , 2020, <<https://tc26.ru/standarts/rekomendatsii-po-standartizatsii/r-1323565-1-025-2019-informatsionnaya-tehnologiya-kriptograficheskaya-zashchita-informatsii-ispolzovanie-rossiyskikh-algoritmov-elektronnoy-podpisi-v-protokolakh-i-formatakh-soobshcheniy-na-osnove-xml.html/>>.

**[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/xmlsig-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 following sample was constructed using the X.509 certificate from Appendix A of [[R1323565.1.023-2018](#)].

X-coordinate of public key:

0x971566CEDA436EE7678F7E07E84EBB7217406C0B4747AA8FD2AB1453C3D0DFBA

Y-coordinate of public key:

0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E2E24FF71F9CE643

Corresponding private key (d):

0xBFCE1D623E5CDD3032A7C6EABB4A923C46E43D640FFEAAF2C3ED39A8FA399924

K value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEFE33B0E270318857C

H-bar value:

0x054D1DABB161D63424F8DABB2800708B00F78DA7582699E8F2F0A521C7CE8144

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+3xyQ40//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
            F0mFmr9nfRwMYP4o0Pg1m0n5RlaXNYrQ==
          </PublicKey>
        </GOSTR34102012-256-KeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</root>

```

Base64-encoded signed XML document:

```

77u/
PD94bWwgdmVyc2lvbjo9iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIElkaPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0
dXJl
IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWc9Ij4NCiAgICAg
IDxT
aWduZWRJbWZvPg0KICAgICAgICAgPENhbm9uawNhbG16YXRpb25NZXR0b2QgQWxnb3Jp

```



0x7E08A434CB2FA300F8974E3FF69A4BCDF36B6308E1D7A56144693A35E11CBD14D50291  
6E680E35FE1E6ABBA85BD4DAE7065308B16B1CCABFE3D91CE0655B0FFD

Corresponding private key (d):

0x3FC01CDCD4EC5F972EB482774C41E66DB7F380528DFE9E67992BA05AEE462435757530  
E641077CE587B976C8EEB48C48FD33FD175F0C7DE6A44E014E6BCB074B

K value:

0x72ABB44536656BF1618CE10BF7EADD40582304A51EE4E2A25A0A32CB0E773ABB23B7D8  
FDD8FA5EEE91B4AE452F2272C86E1E2221215D405F51B5D5015616E1F6

H-bar value:

0x33DEF8422879AA68482339BC65E5DCA9A5D77E80C5C0371DB13D3B88F4CCA8A89ED3CE  
85849231DD61B35E4B47A3722317663859A2BE088C1BB6EEC87410DAF2

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>
          wi0FD9D7zKHNlo58t/9tUtCJA5Z09vmDhMlt3HIkyXZvQxIp5PE+txwsI
          AVfUIOULvGTFxAZlwuHTB+qD5s54g==
        </DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>
      dn+oWg6n3wJ20kBm01GvURc4SuZ3h3nKXYWy4uHdmeS2n1TlNWFKca4fTB1c+fp
      nCS8IEVNFx25Ndh4UXJLLN12/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>
            ExkPVQoj0RURgkPDBM9hdXQDaowhLssGvAm8Tp072hiaRUFV0MJMLy
            xQCoe4Z0eNrzhLcaSrUwl3xn/OJ0YTB/0PW2XgHNnjv8oca7EIUwbn
            2tRbqLtqHv41DmhukQLVFL0c4TU6aURhpdfhCGNr881LmvY/Tpf4AK
            MvyzSkCH4=
          </PublicKey>
        </GOSTR34102012-512-KeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</root>

```

Base64-encoded signed XML document:

```

77u/
PD94bWwgdmVyc2l1bWVj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVG9TaWduIEElkPSJUb1NpZ24iPkrRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0

```



dXJl  
IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWc jIj4NCiAgICAg  
IDxT  
aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbG16YXRpb25NZXRob2QgQWxnb3Jp  
dGht  
PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yMDAxMDMxNSIg  
Lz4N  
CiAgICAgICAgIDxTawduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1cm46aWV0ZjpwYXJh  
bXM6  
eG1s0m5z0mNweG1sc2Vj0mFsZ29yaXRobXM6Z29zdHIzNDEwMjAxMi1nb3N0cjM0MTEy  
MDEy  
LTUxMiIgZ4NCiAgICAgICAgIDxSZWZlcmVuY2UgVVJPSIjVG9TaWduIj4NCiAgICAg  
ICAg  
ICAgIDxUcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgPFRyYW5zZm9ybSBbbGdvcml0  
aG09  
Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvUkVDLXhtbC1jMTRuLTlwMDEwMzE1IiAv  
Pg0K  
ICAgICAgICAgICAgPC9UcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgPERpZ2VzdE1ldGhv  
ZCBB  
bGdvcml0aG09InVybjppZXRmOnBhcmFtczpz4bWw6bnM6Y3B4bWxzZW6YwXnb3JpdGht  
czpn  
b3N0cjM0MTEyMDEyLTUxMiIgZ4NCiAgICAgICAgICAgIDxEawdlc3RwYXx1ZT53aU9G  
RD1E  
N3pLSE5sbzU4dC85dFV0Q0pBNVpPOXZtRGhNbHQzSElreVhadlF4SXA1UEUrdHh3c0lB  
VmZV  
SU9VTHZHEZ4QVpsd3VIVEIrcUQ1czU0Zz09PC9Eawdlc3RwYXx1ZT4NCiAgICAgICAg  
IDwv  
UmVmZXJlbnNlPg0KICAgICAgPC9TaWduZWRJbmZvPg0KICAgICAgPFNpZ25hdHVyZVZh  
bHVl  
PmRuk29XZzZuM3dKMjBrQm1PMUd2VVJjNFN1WjNoM25LWF1XeTR1SGRtZVMYbmxUbE5X  
Rktj  
YTRmVEJsYytmcG5DUzhJRVZ0RlgyNU5kaDRVWEpMTE5sMi9MMHd0YW5jRmlBK3hSWXpG  
Z3pV  
R1crcFdJZnlmdkJKc1NzcGJ3ZVp5S1VXYWpxTjNsRFJaRGNoeWNFQXB0bHFECFR0ZXM4  
QnB0  
clhTaCtDcGcrYz08L1NpZ25hdHVyZVZhbnHVlPg0KICAgICAgPEtleUluZm8+DQogICAg  
ICAg  
ICA8S2V5VmFsdWU+DQogICAgICAgICAgICA8R09TVFIzNDEwMjAxMi0MTItS2V5VmFs  
dWUg  
eG1sbnM9InVybjppZXRmOnBhcmFtczpz4bWw6bnM6Y3B4bWxzZWMiPg0KICAgICAgICAg  
ICAg  
ICAgPE5hbWkQ3VydmUgVVJPSJ1cm46b2lk0jEuMi42NDMuNy4xLjIuMS4yLjIiIC8+  
DQog  
ICAgICAgICAgICAgICA8UHViG1jS2V5PkV4a1BWUW9qT1JVUmdrUERCTTloZFhRRGFv  
V2hM  
c3NHdkFt0FRwMDcyaGlhUlVGvjBNSk1MeXhrQ29lNFpPZU5yemhMY2FTc1V3bDN4bi9P  
SjBZ  
VEIVMFBXMXlhnSE5uanY4b2NhN0VjVXdibjJ0UmJxTHRxSHY0MURtaHVrUUXWRkwwYzRU  
VTZh  
VVJocGRmaENHTnI40DFMbxZZL1RwZjRBS012EXpTa0NIND08L1B1YmXpY0tleT4NCiAg  
ICAg  
ICAgICAgIDwvR09TVFIzNDEwMjAxMi0MTItS2V5VmFsdWU+DQogICAgICAgICA8L0tl  
eVZh  
bHVlPg0KICAgICAgPC9LZX1JbmZvPg0KICAgPC9TaWduYXR1cmU+DQo8L3Jvb3Q+

### **B.3. Signed XML document with GOST R 34.10-2001 algorithm in SignatureMethod element**

The following sample was constructed using the X.509 certificate from section 4.2 of [[RFC4491](#)].

X-coordinate of public key:

0x577E324FE70F2B6DF45C437A0305E5FD2C89318C13CD0875401A026075689584

Y-coordinate of public key:

0x601AEACABC660FDFB0CBC7567EBBA6EA8DE40FAE857C9AD0038895B916CCEB8F

Corresponding private key (d):

0x0B293BE050D0082BDAE785631A6BAB68F35B42786D6DDA56AF169891040F77

K value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEFE33B0E270318857C

H-bar value:

0xEF3E03620C2B0E87E43F503A839AB7868071EA28CA38AABD915D56A5F74400F4

Signed XML document:



dGht  
PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yMDAxMDMxNSIg  
Lz4N  
CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1cm46aWV0ZjpwYXJh  
bXM6  
eG1s0m5z0mNweG1sc2Vj0mFsZ29yaXRobXM6Z29zdHIzNDEwMjAwMS1nb3N0cjM0MTEi  
IC8+  
DQogICAgICAgICA8UmVmZXJlbnNlIFVSST0iI1RvU2lnbiI+DQogICAgICAgICAgICA8  
VHJh  
bnNmb3Jtcz4NCiAgICAgICAgICAgICAgIDxUcmFuc2Zvcn0gQWxnb3JpdGhtPSJodHRw  
Oi8v  
d3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yMDAxMDMxNSIgLz4NCiAgICAg  
ICAg  
ICAgIDwvVHJhbnNmb3Jtcz4NCiAgICAgICAgICAgIDxEaWdlc3RNZXRob2QgQWxnb3Jp  
dGht  
PSJ1cm46aWV0ZjpwYXJhbXM6eG1s0m5z0mNweG1sc2Vj0mFsZ29yaXRobXM6Z29zdHIz  
NDEw  
IiAvPg0KICAgICAgICAgICAgPERpZ2VzdFZhbnVlPkZWUWJ6RjJkamZ0TkpPM0pHME9M  
ZlNP  
RGxaa2liVGNVbUYyRfM0bm51UFk9PC9EaWdlc3RwYX1ZT4NCiAgICAgICAgIDwvUmVm  
ZXJl  
bnNlPg0KICAgICAgPC9TaWduZWRJbmZvPg0KICAgICAgPFNpZ25hdHVyZVZhbHVlPm4y  
VUh0  
ZHUyNWZQekp0WxlvamJOVHE1MlYxRDNVQlZRCUk1eE5oZF1vcERwTwpwZW10MkgrM3h5  
UTRP  
Ly9uenMxTG4vb3F3enZ10XpwYUgzUTBCUGF3PT08L1NpZ25hdHVyZVZhbHVlPg0KICAg  
ICAg  
PEtleUluZm8+DQogICAgICAgICA8S2V5VmFsdWU+DQogICAgICAgICAgICA8R09TVFIz  
NDEw  
MjAwMjtleVZhbHVlIHhtbG5zPSJ1cm46aWV0ZjpwYXJhbXM6eG1s0m5z0mNweG1sc2Vj  
Ij4N  
CiAgICAgICAgICAgICAgIDx0YW1lZEN1cnZlIFVSST0idXJu0m9pZDoxLjIuNjZzLjIu  
Mi4z  
Ni4wIiAvPg0KICAgICAgICAgICAgICAgICAgPFB1YmxpY0tleT5oSlzVZFdBQ0drQjFDTTBU  
akRH  
SkxQM2xCUU42UTF6MGJtc1A1MDh5ZmxlUDY4d1d1WldJQTlDYWZJV3VEK1N0NnFhN2Zs  
Ykh5  
N0RmRDJhOH11b2FZQT09PC9QdWJsaWNLZXk+DQogICAgICAgICAgICA8L0dPU1RSMzQx  
MDIw  
MDFLZX1wYX1ZT4NCiAgICAgICAgIDwvS2V5VmFsdWU+DQogICAgICA8L0tleUluZm8+  
DQog ICA8L1NpZ25hdHVyZT4NCjwvcn0gQWxnb3JpdGhtPSJ1cm46aWV0ZjpwYXJh  
bXM6eG1s0m5z0mNweG1sc2Vj0mFsZ29yaXRobXM6Z29zdHIzNDEwMjAwMS1nb3N0cjM0MTEi  
IC8+

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

The following sample was constructed using the X.509 certificate from Appendix A of [[R1323565.1.023-2018](#)].

X-coordinate of public key:

0x971566CEDA436EE7678F7E07E84EBB7217406C0B4747AA8FD2AB1453C3D0DFBA

Y-coordinate of public key:

0xAD58736965949F8E59830F8DE20FC6C0D177F6AB599874F1E2E24FF71F9CE643

Corresponding private key (d):

0xBFCF1D623E5CDD3032A7C6EABB4A923C46E43D640FFEAAF2C3ED39A8FA399924

K value:

0x5782C53F110C596F9155D35EBD25A06A89C50391850A8FEFE33B0E270318857C

H-bar value:

0x054D1DABB161D63424F8DABB2800708B00F78DA7582699E8F2F0A521C7CE8144

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+3xyQ40//nz
      s1Ln/oqwzv9zpaH3Q0BPaw==
    </SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>
          MIICYjCCAg+gAwIBAgIBATAKBggqhQMHAQEDAjBWMskwJwYJKoZIHvcNA
          QkBFhpHb3N0UjM0MTAtMjAxMkbleGFtcGx1LmNvbTEpMccGA1UEAxMgR2
          9zdFIZNDEwLTIwMTIIGKDI1NiBiaXQpIGV4YW1wbGUwHhcNMTMxMTA1MTQ
          wMjM3WhcNMzAxMTAxMTQwMjM3WjBWMskwJwYJKoZIHvcNAQkBFhpHb3N0
          UjM0MTAtMjAxMkbleGFtcGx1LmNvbTEpMccGA1UEAxMgR29zdFIZNDEwL
          TIwMTIIGKDI1NiBiaXQpIGV4YW1wbGUwZjAfBggqhQMHAQEBATATBgcqhQ
          MCAiQABggqhQMHAQECAgNDAARAUT/Qw1MUq9KPqkdHC2xAF3K7TugHfo9
          n525D2s5mFZdD5pwf90/i4vF0mFmr9nfRwMYP4o0Pg1mOn5R1aXNYraOB
          wDCBvTAdBgNVHQ4EFgQU1fIeN1HaPbw+XWUzbkKJ+kHJUT0AwCwYDVR0PB
          AQDAGHGMa8GA1UdEwQIMAYBAf8CAQEwfgYDVR0BBHcWdYAU1fIeN1HaPb
          w+XWUzbkKJ+kHJUT0ChWqRYMFYxKtAnBgkqhkiG9w0BCQEWGkdvc3RSMzQ
          xMCOyMDEyYQGV4YW1wbGUuY29tMskwJwYDVQQDEyBHb3N0UjM0MTAtMjAx
          MiAoMjU2IGJpdCkgZXhhbXBsZS9IBATAKBggqhQMHAQEDAgNBAF5bm4BbA
          RR6hJLEoWJk0sYV3Hd7kXQJz3CdQqfmHrz6TI6Xojdh/t8ckODv/587N
          S5/6KsM77vc6Wh90NAT2s=
        </X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</root>
```

Base64-encoded signed XML document:

77u/

PD94bWwgdMvYc2l2vbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE  
YXRhVG9TaWduIElkPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0  
dXJl  
IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWc jIj4NCiAgICAg  
IDxT  
aWduZWRJbmZvPg0KICAgICAgICAgPENhbm9uaWNhbGl6YXRpb25NZXRob2QgQWxnb3Jp  
dGht  
PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yMDAxMDMxNSIq  
Lz4N  
CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1cm46aWV0ZjpwYXJh  
bXM6  
eG1s0m5z0mNweG1sc2Vj0mFsZ29yaXRobXM6Z29zdHIzNDEwMjAxMj0mMTEyMDEy  
MDEy  
LTI1NiIgLz4NCiAgICAgICAgIDxSZWZlcmVuY2UgVWJPSIjVG9TaWduIj4NCiAgICAg  
ICAg  
ICAgIDxUcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgICAgPFRyYW5zZm9ybSBbBbGdvcml0  
aG09  
Imh0dHA6Ly93d3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWc jIj4NCiAgICAgICAg  
Pg0K  
ICAgICAgICAgICAgPC9UcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgICAgPERpZ2Vz  
dE1ldGhv  
ZCBB  
bGdvcml0aG09InVybjppZXRmOnBhcmFtcz4bWw6bnM6Y3B4bWxzZWYwYXnb3JpdGht  
czpn  
b3N0c jM0MTEyMDEyLTI1NiIgLz4NCiAgICAgICAgICAgICAgIDxEawdlc3RWYwX1ZT45  
UUXz  
eFBQ  
bzdMbFg2SVhxd3pqY05EbwJGdUNDR2l2UTFzNjFoY1B1SVRNPTwvRGlnZXN0VmFsdWU+  
DQog  
ICAgICAgICA8L1JlZmVyZW5jZT4NCiAgICAgIDwvU2lnbmVksW5mbz4NCiAgICAgIDxT  
awdu  
YXR1cmVWYwX1ZT5qY1FKaF0V2JUQ1Y3YmpGa3k1dkdYWFVGawdjNzRGWFJpNzlsWm5G  
SEs3  
cE1qcGVpTjJIKzN4eVE0Ty8vbnpzMUxuL29xd3p2dTl6cGFIM1EwQlBhdz09PC9TaWdu  
YXR1  
cmVWYwX1ZT4NCiAgICAgIDxLZXlJbmZvPg0KICAgICAgICAgICAgICAgICAgPFRyYW5z  
Zm9ybSBbBbGdvcml0aG09InVybjppZXRmOnBhcmFtcz4bWw6bnM6Y3B4bWxzZWYwYXnb3  
JpdGht  
ICAgICAgICAgICAgPC9UcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgICAgPERpZ2Vz  
dE1ldGhv  
ZCBB  
aFFN  
SEFRRURBakJXTVNr d0p3WUpLb1pJaHZjTkFRa0JGahBIYjNOMFVqTTBNVEF0TwpBeE1r  
Qmxl  
R0Z0Y0d4bExtTnZiVEVwTUNjR0ExVUVBeE1nUjI5emRGSXp0REV3TFRJd01USWdLREkx  
TmlC  
aWFYUXBJR1Y0WVcx d2JHVXdIaGN0TVRNeE1UQTfNVFF3TwpNM1doY05NekF4TVRBeE1U  
UXdN  
ak0zV2pCV01Ta3dKd1lKS29aSWH2Y05BUWtCRmhwSGIzTjBVak0wTVRbDE1qQXhNa0Js  
ZUdG  
dGNHeGxMbU52YlRFcE1DY0dBmVVFQXhNZ1IyOXpkRkl6TkRfd0xUSXdNVElnS0RJM5p  
Qmlh  
WFFwSudWNFlMXdiR1V3WmpBzkJnZ3FoUU1IQVFFQkFUQVRCZ2NxaFFNQ0FpUUFcz2dx  
aFFN  
SEFRRUNBZ05EQUFsQXV0L1F3MU1VcTlLUHFrZEHDMnhBRjNLN1R1Z0hmbzluNTI1RDJz  
NW1G  
WmRENXB3ZjkwL2k0dkYwbUztcjluZlJ3TVlQNG8wUGcxbU9uNVJsYVh0WXJhT0J3RENC  
d1RB  
ZEJnTlZiUTFRFRmdRVTFmSWVOMUhhUGJ3K1hXVXpia0ora0hKVVQwQXdDd1lEVlIwUEJB  
UURB





```

<?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+3xyQ40//nz
      s1Ln/oqwzvU9zpaH3Q0BPaw==
    </SignatureValue>
    <KeyInfo>
      <DEREncodedKeyValue xmlns="http://www.w3.org/2009/xmldsig11#">
        MGYwHwYIKoUDBwEBAQEwEwYHKoUDAgIkaAYIKoUDBwEBAgIDQwAEQLrf0MNT
        FKvSj6pHRwtsQBdyu07oB36PZ+duQ9r0ZhWXQ+acH/dP4uLxdJhZq/Z30cDG
        D+KND4NZjp+UZWlZWk0=
      </DEREncodedKeyValue>
    </KeyInfo>
  </Signature>
</root>

```

Base64-encoded signed XML document:

```

77u/
PD94bWwgdmVyc2lvdj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48cm9vdD4NCiAgIDxE
YXRhVGV9TawduIElKPSJUb1NpZ24iPkRhdGE8L0RhdGFUb1NpZ24+DQogICA8U2lnbmF0
dXJl
IHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWc9Ij4NCiAgICAg
IDxT
awduZWRJbmZvPg0KICAgICAgICAgPENhbm9uawNhbGl6YXRpb25NZXR0b2QgQWxnb3Jp
dGht
PSJodHRwOi8vd3d3LnczLm9yZy9UUi8yMDAxL1JFQy14bWwtYzE0bi0yMDAxMDMxNSIg
Lz4N

```

CiAgICAgICAgIDxTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJ1cm46aWV0ZjpwYXJh  
bXM6  
eG1sOm5zOmNweG1sc2VjOmFsZ29yaXRobXM6Z29zdHIzNDEwMjAxMi1nb3N0cjM0MTEy  
MDEy  
LTI1NiIgLz4NCiAgICAgICAgIDxSZWZlcmVuY2UgVVJPSIjVG9TaWduIj4NCiAgICAg  
ICAg  
ICAgIDxUcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgPFRyYW5zZm9ybSBbbGdvcml0  
aG09  
Imh0dHA6Ly93d3cudzMub3JnL1RSLzIwMDEvUkVDLXhtbC1jMTRuLTIwMDEwMzE1IiAv  
Pg0K  
ICAgICAgICAgICAgPC9UcmFuc2ZvcmlzPg0KICAgICAgICAgICAgICAgPERpZ2VzdE1ldGhv  
ZCBB  
bGdvcml0aG09InVybjppZXRmOnBhcmFtczpz4bWw6bnM6Y3B4bWxzZWm6YXnb3JpdGht  
czpn  
b3N0cjM0MTEyMDEyLTI1NiIgLz4NCiAgICAgICAgICAgIDxEaWdlc3RwYXx1ZT45UUxz  
eFBQ  
bzdMbFg2SVhxd3pqY05EbWJGdUNDR2l2UTFzNjFoY1B1SVRNPtwvRGlnZXN0VmFsdWU+  
DQog  
ICAgICAgICAgICAgL1JlZmVvZm5jZT4NCiAgICAgIDwvU2lnbmVksW5mbz4NCiAgICAgIDxT  
aWdu  
YXR1cmVWYXx1ZT5qY1FKaF0V2JUQ1Y3YmpGa3k1dkdYWFVGawdjNzRGWFJpNz1sWm5G  
SEs3  
cE1qcGVpTjJIKzN4eVE0Ty8vbnpzMUXuL29xd3p2dTl6cGFIM1EwQlBhdz09PC9TaWdu  
YXR1  
cmVWYXx1ZT4NCiAgICAgIDxLZXlJbmZvPg0KICAgICAgICAgPERFUKVvY29kZWRLZXlW  
YXx1  
ZSB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwOS94bWxkc2lnMTEjIj5NR1l3SHdZ  
SUVv  
VURCd0VCQVFFd0V3WUhlb1VEQWdJa0FBWUllb1VEQndFQkFnSURRd0FFUUXyZjBNTlRG  
S3ZT  
ajZwSFJ3dHNRQmR5dTA3b0IzNlBaK2R1UTlyT1poV1hRK2FjSC9kUDR1THhkSmhacS9a  
MzBj  
REdEK0tORDROWmpwK1VaV2x6V0swPTwvREVSrw5jb2RlZEt1eVZhbHVlPg0KICAgICAg  
PC9LZXlJbmZvPg0KICAgICAgICAgPC9TaWduYXR1cmU+DQo8L3Jvb3Q+

## Appendix C. Acknowledgments

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

## Authors' Addresses

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

Phone: [+7 \(495\) 995-48-20](tel:+7(495)995-48-20)  
Email: [spv@cryptopro.ru](mailto:spv@cryptopro.ru)

Maria Paramonova  
CryptoPro  
18, Sushevsky val  
Moscow  
127018

Russian Federation

Phone: [+7 \(495\) 995-48-20](tel:+7(495)995-48-20)

Email: [mparamonova@cryptopro.ru](mailto:mparamonova@cryptopro.ru)

Mikhail Khomenko  
CryptoPro  
18, Sushevsky val  
Moscow  
127018  
Russian Federation

Phone: [+7 \(495\) 995-48-20](tel:+7(495)995-48-20)

Email: [xmv@cryptopro.ru](mailto:xmv@cryptopro.ru)

Artyom Makarov  
CryptoPro  
18, Sushevsky val  
Moscow  
127018  
Russian Federation

Phone: [+7 \(495\) 995-48-20](tel:+7(495)995-48-20)

Email: [makarov@cryptopro.ru](mailto:makarov@cryptopro.ru)