Порядок использования электронной подписи в электронных документах Клирингового терминала

Оглавление

1. Требования к электронной подписи

1.1. Электронные документы Клирингового терминала, определенные в пространстве имен ed (см. Форматы электронных сообщений), подписываются электронной подписью (ЭП).

1.2. Для документов в формате XML используется формат представления электронной подписи «XML Signature Syntax and Processing (Second Edition)» (http://www.w3.org/TR/xmldsig-core/), краткое обозначение XML DSig.
Стандарт данного формата определяется международной организацией The World Wide Web Consortium (W3C), xsd-схема формата находится по адресу "http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/xmldsig-core-schema.xsd".

1.3. В электронных документах Клирингового терминала ЭП содержится непосредственно в теле XML-документа в виде элемента Signature, см. Таблица 1. Элемент Signature должен содержать ограниченный набор полей, перечисленных в таблице. Допускается включение нескольких экземпляров ЭП (элементов Signature), если правилами документооборота предусмотрено наличие двух и более подписей.

Таблица 1: Структура элемента, содержащего ЭП в формате XML DSig

Элемент	**Описание**
<Signature>	ЭП
<SignedInfo>	Подписываемые данные
<CanonicalizationMethod>	Алгоритм канонизации XML-документа
Algorithm	Обозначение алгоритма
</CanonicalizationMethod>	
<SignatureMethod>	Алгоритм формирования подписи
Algorithm	Обозначение алгоритма
</SignatureMethod>	
<Reference>	
<Transforms>	Дополнительные преобразования
<Transform>	
Algorithm	Обозначение алгоритма дополнительного преобразования
</Transform>	
</Transforms>	
<DigestMethod>	Алгоритм вычисления хэш-значения
Algorithm	Обозначение алгоритма
</DigestMethod>	
<DigestValue>	Хэш-значение
</Reference>	
</SignedInfo>	
<SignatureValue>	Значение **подписи**
</Signature>	

1.4. Согласно спецификации XML DSig, в процессе формирования и проверки ЭП применяются следующие операции обработки исходного XML-документа:

- Канонизация, canonicalization;
- Дополнительные преобразования, transform;
- Вычисление хэш-значения, digest;
- Генерация подписи, signature.

1.5. При формировании ЭП электронных документов Клирингового терминала в приведенных операциях обработки должны применяться следующие алгоритмы:

Операция	Алгоритм	Обозначение в атрибуте Algorithm
Канонизация	Алгоритм канонизации XML 1.1 с исключением комментариев, описание алгоритма находится по адресу: http://www.w3.org/TR/2001/REC-xml-c14n-20010315	http://www.w3.org/2006/12/xml-c14n11
Дополнительные преобразования	Обработка обёрнутой цифровой подписи (enveloped signature transform), описание алгоритма находится по адресу: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/Overview.html#enveloped-signature	http://www.w3.org/2000/09/xmldsig#enveloped-signature
Вычисление хэш-значения	Кодирования данных base64, RFC4648, описание алгоритма находится по адресу: https://tools.ietf.org/html/rfc4648#section-4	urn:ietf:base64
Генерация подписи, должна осуществляться с использованием инфраструктуры X.509	Для квалифицированных сертификатов ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".	urn:moex:gostr34.10-2001
	Для квалифицированных сертификатов ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". Описание алгоритма находится по адресу: https://tools.ietf.org/html/rfc7091	urn:moex:gostr34.10-2012
	Алгоритм RSA, описание алгоритма находится по адресу: http://www.ietf.org/rfc/rfc2437.txt	http://www.w3.org/2000/09/xmldsig#rsa-sha1

2. Порядок формирования ЭП

2.1. Формирование ЭП документов Клирингового терминала выполняется в следующем порядке:

1) Входящими данными является исходный XML-документ в формате, описанном в документации на Клиринговый терминал. Допускается наличие в документе ранее сформированных ЭП.
2) Создание элемента Reference (см. Таблица №1):
    a. Над исходным документом выполняется преобразование enveloped signature transform, в результате чего из него исключаются все элементы Signature;
    b. Выполняется процедура канонизации XML-документа по алгоритму C14N11, на выходе которой получается поток байтов, содержащий нормализованный XML-документ;
    c. Нормализованный XML-документ кодируется алгоритмом base64, полученный результат считается хэш-значением исходного электронного документа (полученное таким образом хэш-значение допускает обратное преобразование к исходному XML-формату);
    d. Создается XML-элемент Reference, содержащий полученное хэш-значение и указания на использованные алгоритмы дополнительного преобразования и вычисления хэш-функции;
3) Создание элемента SignedInfo, включающего элемент Reference и указания на использованные алгоритмы канонизации и подписи;
4) Канонизация сформированного элемента SignedInfo по алгоритму C14N11, в результате чего получается поток байтов, использующийся на входе алгоритма подписи;
5) Формирование подписи нормализованного элемента SignedInfo по одному из поддерживаемых алгоритмов:
    - ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;
    - RSA;
6) Формирование элемента Signature из элемента SignedInfo, полученного значения подписи и имени владельца сертификата;
7) Включение элемента Signature в исходный XML-документ.

3. Порядок проверки подписи

3.1. Проверка подлинности ЭП под полученным XML-документом выполняется следующей последовательностью операций:

1) На входе используется полученный XML-документ;
2) Каждая включенная в документ ЭП проверяется независимо;
3) Проверка целостности документа:
    a. Над исходным документом выполняется преобразование enveloped signature transform, в результате чего из него исключаются все элементы Signature;
    b. Выполняется канонизация XML-документа по алгоритму C14N11, в результате чего формируется поток байтов, содержащий нормализованный XML-документ;
    c. Нормализованный XML-документ кодируется алгоритмом base64, полученный результат считается хэш-значением исходного электронного документа;
    d. Производится сравнение рассчитанного хэш-значения со значением, указанным в элементе Signature.Reference.DigestValue исходного документа; в случае если строки не совпадают, проверка ЭП завершается с ошибкой;
4) Проверка подписи:
    a. По электронной подписии определяется сертификат ключа проверки подписи (данная возможность обеспечивается использованием инфраструктуры X.509 при формировании электронной подписи);
    b. Проверка, что сертификат проверки ЭП соответствует Участнику клиринга, от имени которого сформирован электронный документ;
    c. Проверка, что владельцу сертификата дано право осуществлять подпись электронных документов (ЕКБД);
    d. Канонизация элемента SignedInfo по алгоритму C14N11, в результате чего получается поток байтов, содержащий подписанное сообщение;
    e. Проверка электронной подписи на основании сертификата ключа проверки электронной подписи, подписанного сообщения и значения подписи, содержащегося в элементе Signature.SignatureValue, методом, определенным стандартом использованного алгоритма подписи.

4. Плагин для работы с ЭП

4.1. Для формирования и проверки ЭП в рамках работы в web-интерфейсе Клирингового терминала используется браузерный плагин Moex browser plugin. Описание функций приведено в соответствующем документе.

5. Коды ошибок проверки ЭП

5.1. Коды ответа прикладных ошибок при работе с подписью, формируемые на HTTP-запросы, приведены в документе Спецификация WEB API к клиринговому терминалу. См. Приложение 2.

6. Пример операции подписания XML-документа

Шаг 1.1: Исходный xml (содержит ранее наложенную подпись)**:**

```
<?xml version="1.0" encoding="UTF-8"?>
<SCodeReq SCodeKind="O" Member="9715500000" DocNum="35" Market="CU" DocTime="12:10:00" SCodeType="S" DocDate="1967-08-13" FirmID="MB9715500000"
DocTypeId="SCodeReq">
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
         <ds:SignatureMethod Algorithm="urn:moex:gostr34.10-2012"/>
         <ds:Reference>
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="urn:ietf:base64"/>
            <ds:DigestValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jTnVtPSIzNSIgRG9j
            VGltZT0iMTI6MTA6MDAiIERvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29k
            ZVR5cGU9IlMiPjwvZWQ6U0NvZGVSZXE+</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>dJDHiGQMaKN8iPuWApAL57eVnxz2BQtyujwfPSgE7HyKoxYtoRB97ocxZ
         8ZU440wHtE39ZwRGIjvwor3WfURxnIgnI1CChMXXwoGpHH//Zc0z4ejaz
         DuCNEq4Mm4OUVTiEVuwcWAOMkfDHaM82awYQiOGcwMbZe38UX0oPJ2DOE=</ds:SignatureValue>
   </ds:Signature>
</SCodeReq>
```

Шаг 1.2: Выполнение преобразования enveloped-signature:

Из документа вырезаются все элементы Signature:

```
<?xml version="1.0" encoding="UTF-8"?>
<SCodeReq SCodeKind="O" Member="9715500000" DocNum="35" Market="CU" DocTime="12:10:00" SCodeType="S" DocDate="1967-08-13" FirmID="ZZ"
DocTypeId="SCodeReq">
</SCodeReq>
```

Шаг 1.3: Канонизация:

Формируется нормализованная байтовая строка:

```
<SCodeReq DocDate="1967-08-13" DocNum="35" DocTime="12:10:00" DocTypeId="SCodeReq" FirmID="ZZ" Market="CU" Member="9715500000" SCodeKind="O"
SCodeType="S"></SCodeReq>
```

Шаг 1.4: Формирование хэш-значения от канонического представления:

С помощью алгоритма base64 формируется хэш-значение от нормализованной байтовой строки:

```
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jTnVtPSIzNSIgRG9jVGltZT0iMTI6M
TA6MDAiIERvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29kZVR5cGU9Il
MiPjwvZWQ6U0NvZGVSZXE+
```

Шаг 1.5: Создание элемента Reference:

Создание элемента Reference, содержащего полученное хэш-значение и указания на использованные алгоритмы дополнительного преобразования и вычисления хэш-функции:

```
<ds:Reference>
   <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
   </ds:Transforms>
   <ds:DigestMethod Algorithm="urn:ietf:base64"/>
   <ds:DigestValue>
   PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jVGltZT0iMTI6MTA6MDAiIERvY
   1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29kZVR5cGU9IlMiPjwvZWQ6U0NvZGVSZXE+</
   ds:DigestValue>
</ds:Reference>
```

Шаг 2: Создание элемента SignedInfo:

Создание элемента SignedInfo, включающего элемент Reference и указания на использованные алгоритмы канонизации и подписи:

```
<ds:SignedInfo>
   <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
   <ds:SignatureMethod Algorithm="urn:moex:gostr34.10-2012"/>
   <ds:Reference>
      <ds:Transforms>
         <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="urn:ietf:base64"/>
      <ds:DigestValue>
      PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jVGltZT0iMTI6MTA6MDAiIE
      RvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29kZVR5cGU9IlMiPjwvZWQ6U0NvZGVS
      ZXE+</ds:DigestValue>
   </ds:Reference>
</ds:SignedInfo>
```

Шаг 3: Канонизация элемента SignedInfo:

Создание нормализованной байтовой строки из сформированного ранее элемента SignedInfo с помощью алгоритма канонизации C14N11:

```
<ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/><ds:SignatureMethod Algorithm="urn:moex:gostr34.10-
2012"/><ds:Reference><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></ds:Transforms><ds:DigestMethod
Algorithm="urn:ietf:base64"/><ds:DigestValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9
jTnVtPSIzNSIgRG9jVGltZT0iMTI6MTA6MDAiIERvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiB
TQ29kZVR5cGU9IlMiPjwvZWQ6U0NvZGVSZXE+</ds:DigestValue></ds:Reference></ds:SignedInfo>
```

Шаг 4: Подпись канонического представления элемента SignedInfo:

Формирование подписи по ГОСТ Р 34.10-2012:

```
MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEfMB0GA1UEChMWVGVzdCBDZXJ0aWZpY2F0ZXMgSW5jLjEQMA4GA1UEAxMHTXkgT
mFtZTAeFw0wNzAxMDMyMTE4MTFaFw0zMTA4MjUy
```

Шаг 5: Формирование элемента Signature:

Создание элемента Signature из элемента SignedInfo, полученного значения подписи и имени владельца сертификата:

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
      <ds:SignatureMethod Algorithm="urn:moex:gostr34.10-2012"/>
      <ds:Reference>
         <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
         </ds:Transforms>
         <ds:DigestMethod Algorithm="urn:ietf:base64"/>
         <ds:DigestValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jTnVtPSIzNSIgRG9jVGl
         tZT0iMTI6MTA6MDAiIERvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29kZVR5cG
         U9IlMiPjwvZWQ6U0NvZGVSZXE+</ds:DigestValue>
      </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue>MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEfMB0GA1UEChMWVGVzdCBDZXJ0aWZpY2F0ZXMgSW5jLjEQMA4GA1UEAx
   MHTXkgTmFtZTAeFw0wNzAxMDMyMTE4MTFaFw0zMTA4MjUy</SignatureValue>
</ds:Signature>
```

Шаг 6: Включение элемента Signature в исходный xml документ:

Созданный элемент Signature включается в исходный xml документ, полученный документ содержит две подписи:

```
<?xml version="1.0" encoding="UTF-8"?>
<ed:SCodeReq SCodeKind="O" Member="9715500000" DocNum="35" Market="CU" DocTime="12:10:00" SCodeType="S" DocDate="1967-08-13" FirmID="ZZ"
DocTypeId="SCodeReq">
   <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
         <ds:SignatureMethod Algorithm="urn:moex:gostr34.10-2012"/>
         <ds:Reference>
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="urn:ietf:base64"/>
            <ds:DigestValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jTnVtPSIzNSIgRG9j
            VGltZT0iMTI6MTA6MDAiIERvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29k
            ZVR5cGU9IlMiPjwvZWQ6U0NvZGVSZXE+</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>dJDHiGQMaKN8iPuWApAL57eVnxz2BQtyujwfPSgE7HyKoxYtoRB97ocxZ
      8ZU440wHtE39ZwRGIjvwor3WfURxnIgnI1CChMXXwoGpHH//Zc0z4ejaz
      DuCNEq4Mm4OUVTiEVuwcWAOMkfDHaM82awYQiOGcwMbZe38UX0oPJ2DOE=</SignatureValue>
   </ds:Signature>
   <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
         <ds:SignatureMethod Algorithm="urn:moex:gostr34.10-2012"/>
         <ds:Reference>
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="urn:ietf:base64"/>
            <ds:DigestValue>
            PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48ZWQ6U0NvZGVSZXEgRG9jRGF0ZT0iMTk2Ny0wOC0xMyIgRG9jVGltZT0iMTI6MTA6
            MDAiIERvY1R5cGVJZD0iU0NvZGVSZXEiIEZpcm1JRD0iWloiIE1hcmtldD0iQ1UiIE1lbWJlcj0iOTcxNTUwMDAwMCIgU0NvZGVLaW5kPSJPIiBTQ29kZVR5cGU9IlMiPjwv
            ZWQ6U0NvZGVSZXE+</DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
      MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEfMB0GA1UEChMWVGVzdCBDZXJ0aWZpY2F0ZXMgSW5jLjEQMA4GA1UEAxMHTXkgTmFtZTAeFw
      0wNzAxMDMyMTE4MTFaFw0zMTA4MjUy</SignatureValue>
   </ds:Signature>
</ed:SCodeReq>
```

7. Коды ответа прикладных ошибок при работе с ЭП от микросервисов EiF

МикроСервис для проверки соответствия имени сертификата Участника Клиринга и получения списка ролей, приписанных лицу, на имя которого выдан сертификат.
Сервис возвращает следующие коды ошибок:

Код	Название	Описание
200	OK	Запрос выполнен успешно
400	Bad Request	Отсутствует один или несколько обязательных параметров запроса
50x	Server Errors	Запрос не может быть выполнен из-за ошибки на стороне сервера
601	No Data	В ЕКБД нет данных соответствующих запросу (не найден участник клиринга и/или сертификат, сертификат пренадлежит другому участнику клиринга и т.д.)

МикроСервис, предназначенный для проверки значения подписи под электронным документом.
Сервис возвращает следующие коды ошибок:

Код	Название	Описание
200	OK	Запрос выполнен успешно
400	Bad Request	Отсутствует один или несколько обязательных параметров запроса
50x	Server Errors	Запрос не может быть выполнен из-за ошибки на стороне сервера
601	Certificate Not Found	Сертификат не найден
602	Certificate Expired	Истек срок сертификата
603	Unknown Signature Verification Algorithm	Неизвестный алгоритм проверки подписи
604	Signature Is Invalid	Подпись неверна
605	Cryptography Error	Ошибка криптографии

МикроСервис для формирования подписи под электронными документами, направляемыми Участниками клиринга.
Сервис возвращает следующие коды ошибок:

Код	Название	Описание
200	OK	Запрос выполнен успешно
400	Bad Request	Отсутствует один или несколько обязательных параметров запроса
50x	Server Errors	Запрос не может быть выполнен из-за ошибки на стороне сервера
601	Certificate Not Found	Сертификат не найден
605	Cryptography Error	Ошибка криптографии