ООО "Крипто-Про"
127 018, Москва, Улица Образцова, 38
Телефон: (095) 933 1168
Факс: (095) 289 4367
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Удостоверяющий центр

Программный комплекс разбора конфликтных ситуаций. Руководство администратора

ЖТЯИ.00009-01 30 09

Листов 40

2003

Содержание

Список рисунков

1. АННОТАЦИЯ

Данный документ содержит описание процесса эксплуатации программного комплекса (ПК) АРМ разбора конфликтных ситуаций (АРМ РКС), входящего в состав системы управления электронными сертификатами (КриптоПро УЦ).

Документ предназначен для администраторов безопасности как руководство эксплуатации АРМ РКС.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Применение электронной цифровой подписи в автоматизированной системе может приводить к конфликтным ситуациям, заключающимся в оспаривании сторонами (участниками системы) авторства и/или содержимого документа, подписанного электронной цифровой подписью (ЭЦП).

Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями формирования самой электронной цифровой подписи требует применения специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭЦП содержимому электронного документа.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем.

Данный разбор основывается на математических свойствах алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации
ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001, гарантирующим невозможность подделки значения ЭЦП любым лицом, не обладающим секретным ключом подписи.

При проверке значения ЭЦП используется открытый ключ, значение которого вычисляется по значению секретного ключа ЭЦП при их формировании.

Система криптографической защиты информации позволяет выполнять проверку значения ЭЦП в течение установленного в системе срока хранения открытых ключей и электронных документов (например, пяти лет), для чего в системе должны быть предусмотрены средства ведения архивов электронных документов с ЭЦП и сертификатов открытых ключей.

Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон, службы безопасности и экспертов. Состав комиссии, порядок ее формирования, регламент работы, рассмотрение результатов определяется в приложении к Регламенту системы (Договору), заключаемому между участниками автоматизированной системы.

Оспаривание результатов работы комиссии и возмещение пострадавшей стороне принесенного ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.

3. ТРЕБОВАНИЯ К СИСТЕМЕ

ПК АРМ РКС предназначен для использования в операционной системе Microsoft Windows 2000 с установленным СКЗИ «Крипто Про CSP» версии 2.0 или выше.

В качестве аппаратных средств используется ПЭВМ типа IBM PC с процессором Pentium-166 (и выше) с минимальным объемом оперативной памяти 64 Мбайт, с жестким диском объемом не менее 2 Гбайт, на котором имеется не менее 650 Мбайт свободного места.

В состав дополнительных аппаратных средств должен входить лазерный принтер для вывода на печать протокола.

4. СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

АРМ РКС реализован в виде исполняемого модуля Referee.EXE. В состав ПК АРМ РКС входят, кроме того, следующие основные модули:

- модуль MFC42.DLL, реализующий функции графического интерфейса операционной системы;
- шаблон template.xsl, используемый при преобразовании документ в формате XML в документ в формате HTML;

5. НАЗНАЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

ПК АРМ РКС входит в состав программного обеспечения «КриптоПро УЦ» и предназначен для проверки соответствия ЭЦП содержанию электронного документа и определения участника автоматизированной системы банковских расчетов, выполнившего ее формирование.

6. ПОРЯДОК РАЗБОРА КОНФЛИКТНОЙ СИТУАЦИИ

Разбор конфликтной ситуации выполняется по инициативе любого участника автоматизированной системы и состоит из:

— предъявления претензии одной стороны другой;

— формирования комиссии;

— разбора конфликтной ситуации;

— взыскания с виновной стороны принесенного ущерба.

Разбор конфликтной ситуации проводится на АРМ РКС (запуском программы Referee.EXE) для электронного документа, авторство или содержание которого оспаривается.

Протокол проверки ЭЦП, формируемый указанной программой, является основным документом работы комиссии и должен быть подписан всеми членами комиссии.

Проверка подписанного электронного документа включает в себя выполнение следующих действий:

- определение сертификата или нескольких сертификатов, необходимых для проверки ЭЦП;
- проверка ЭЦП электронного документа с использованием каждого сертификата;
- определение даты формирования каждой ЭЦП в электронном документе;
- проверка ЭЦП каждого сертификата, путем построения цепочки сертификатов до сертификата Главного ЦС;
- проверка действительности сертификатов на текущий момент времени;
- проверка отсутствия сертификатов в СОС (CRL).

Если сертификат, необходимый для проверки ЭЦП документа, отозван УЦ, комиссия принимает решение о действительности ЭЦП документа, используя дату создания документа и дату отзыва сертификата в CRL.

При необходимости комиссия определяет правомерность использования сертификата на конкретном этапе технологического цикла системы банковских расчетов, опираясь на дополнения "Регламенты использования сертификата" и "Расширенные области использования ключа", зарегистрированные для этого сертификата. Для этого комиссии дополнительно должны быть представлены подтверждения использования данных дополнений в прикладном программном обеспечении.

При проверке ЭЦП документа, верификации цепочки сертификатов, отсутствии сертификата в CRL, авторство подписи под документом считается установленным.

Несовпадение даты формирования документа и сроков действия сертификата и/или сроков действия секретного ключа не влияют на

определение авторства документа. На их основе можно сделать предположение о несоблюдении абонентом регламента в части сроков действия ключей, сертификатов или некорректного использования сертификата в прикладном ПО.

6.1. Случаи невозможности проверки значения ЭЦП

При необнаружении в архиве (базе) сертификата открытого ключа абонента, выполнившего ЭЦП, доказать авторство документа невозможно. В связи с этим, архив с сертификатами открытых ключей необходимо подвергать регулярному резервному копированию и хранить в течение всего установленного срока хранения.

7. РАЗБОР КОНФЛИКТНОЙ СИТУАЦИИ

Для запуска процедуры разбора конфликтной ситуации необходимо запустить исполняемый файл Referee.EXE.

АРМ РКС позволяет проверять подпись электронных документов, сформированных в двух различных форматах (см. документ ЖТЯИ.00005-01 90 06):

- Сообщение отдельно от подписи;
- Сообщение в одном файле с подписью, соответствующем стандарту PKCS#7 Signed.

7.1. Стартовая страница мастера

При запуске программы выводится страница, содержащая краткую информацию о программе

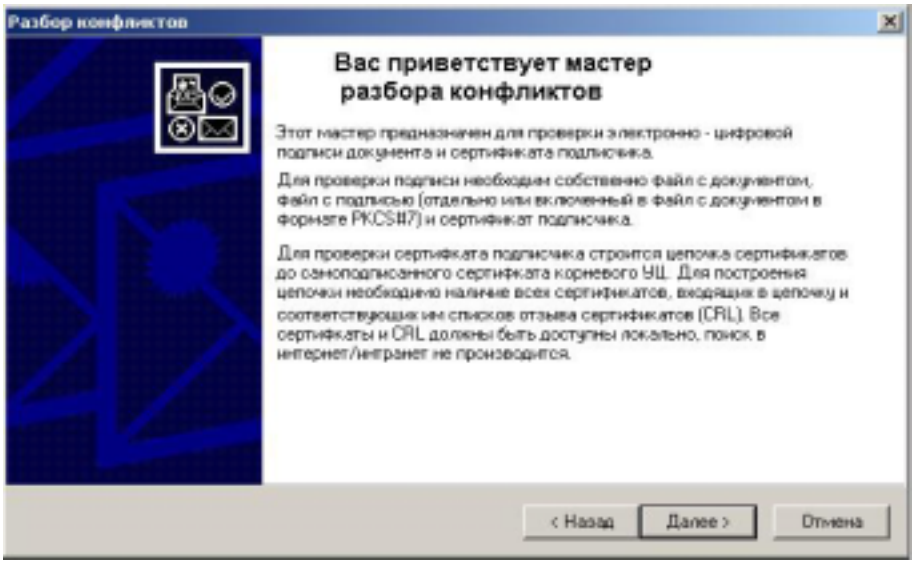

Рис. 1 Стартовая страница

7.2. Выбор электронного документа для проверки

Для выполнения проверки ЭЦП необходимо выбрать файл, который содержит упакованные данные (данные в формате, определенном стандартом PKCS#7),

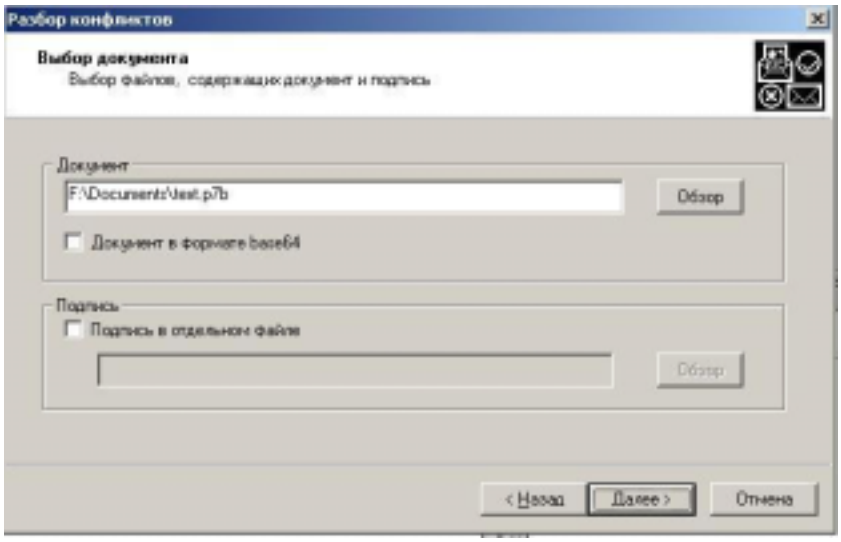

Рис. 2 Диалог выбора файла данных

или файл с подписанным электронным документом в простом формате отдельно от файла подписи.

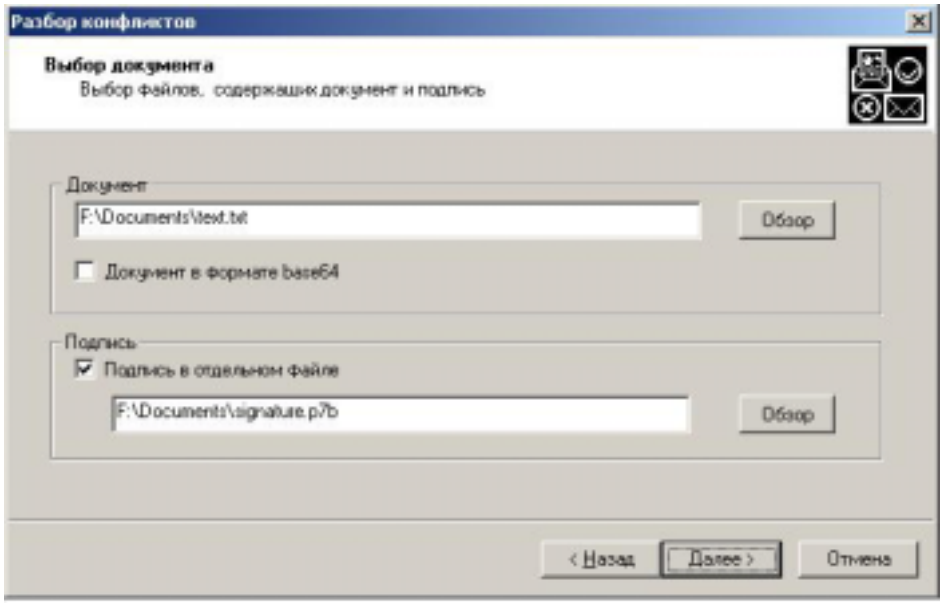

Рис. 3 Диалог выбора файла данных и файла подписи

Документ может быть как в бинарном виде(DER), так и в кодировке base64. Для чтения документов в base64 необходимо установить соответствующий флаг.

Для продолжения нажмите кнопку «**Далее**».

Если не удалось выделить подпись, то возникнет сообщение об ошибке.

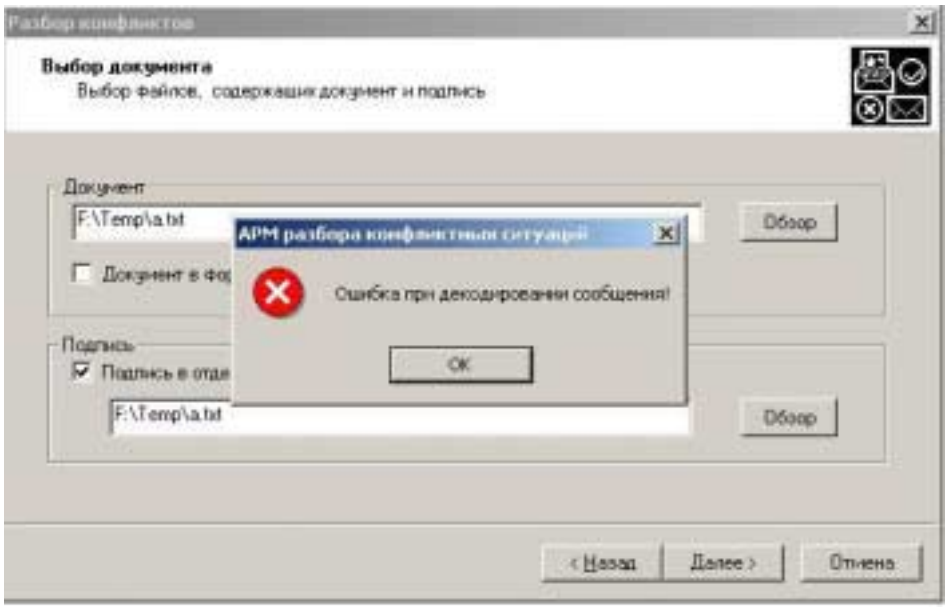

Рис. 4 Ошибка при выборе файла данных

После этого начинается последовательная проверка подписей, которыми был подписан документ.

7.3. Выбор сертификата подписчика

Для криптографической проверки подписи необходимо выбрать сертификат, на котором будет проверяться подпись:

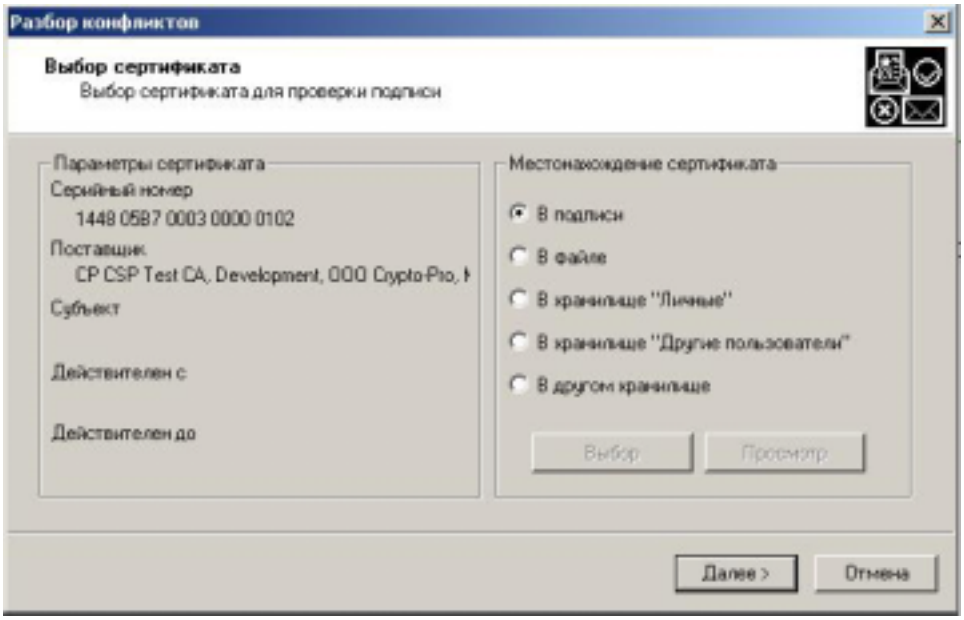

Рис. 5 Выбор сертификата для проверки подписи

Сертификат может находиться

- В самой подписи
- В файле (кодировка DER или base64 без заголовка)
- В хранилище «Личные» (MY)

- В хранилище «Другие пользователи» (AddressBook)
- В любом другом хранилище текущего пользователя

После выбора местонахождения сертификата (кроме «*В подписи*») необходимо его открыть кнопкой «**Выбор**».

При выборе пункта «*В файле*» появится диалог открытия файла.

Рис. 6 Выбор сертификата для проверки из файла

Если выбран файл с сертификатом, не соответствующим тому, которым было подписано сообщение (несовпадение серийного номера или издателя), то появится сообщение об ошибке.

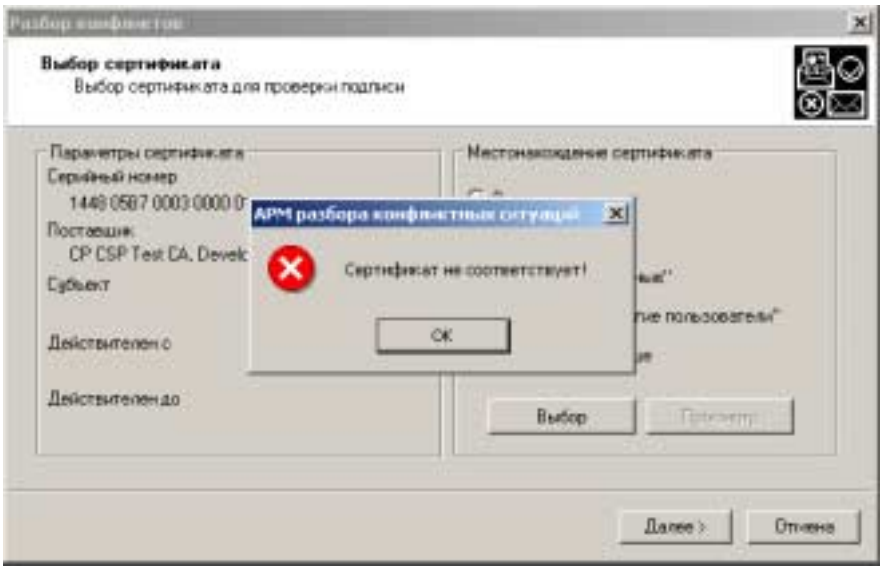

Рис. 7 Ошибка при выборе сертификата для проверки

Если выбраны пункты «*В хранилище «Личные»* или «*В хранилище «Другие пользователи»*, то при нажатии кнопки «**Выбор**» появится окно диалога выбора файла из соответствующего хранилища.

Рис. 8 Выбор сертификат для проверки из хранилища

Если выбран пункт «*В другом хранилище*», то вначале появится диалог выбора хранилища

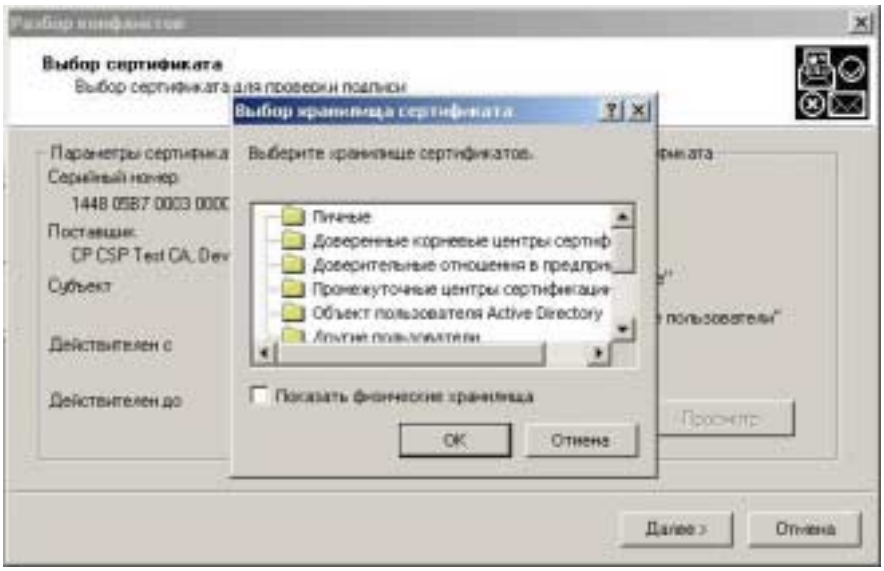

Рис. 9 Выбор хранилища, где находится сертификат для проверки

После выбора хранилища появится диалог выбора сертификата, такой же как и в предыдущем пункте.

Кнопка «**Просмотр**» выводит окно просмотра выбранного сертификата.

Рис. 10 Просмотр сертификата для проверки

Если на данном шаге мастера по какой-то причине сертификат не был выбран, то переход к следующему шагу невозможен – возникнет сообщение об ошибке!

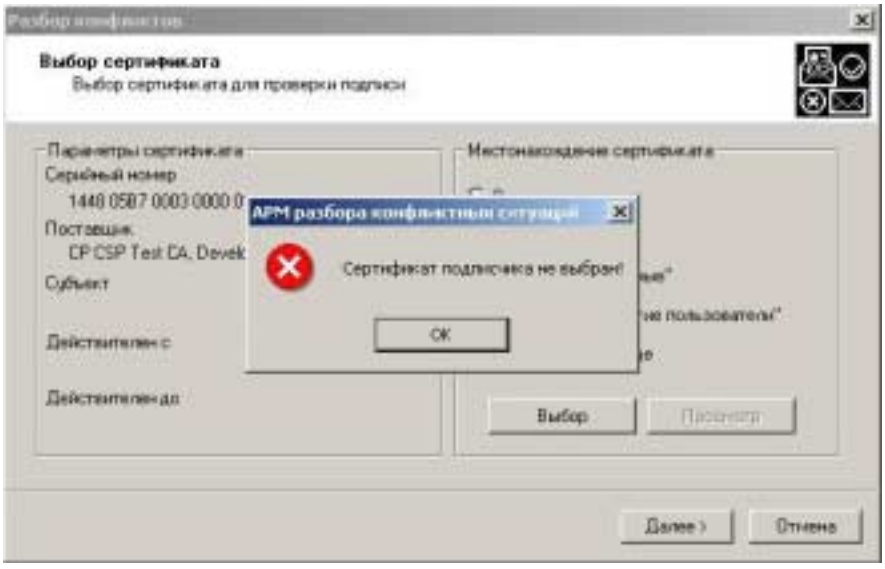

Рис. 11 Сообщение об ошибке при выборе сертификата для проверки

7.4. Проверка цепочки сертификатов

На следующем шаге мастера выбираются сертификаты и списки отзыва, при помощи которых строится цепочка и проверяется сертификат подписчика.

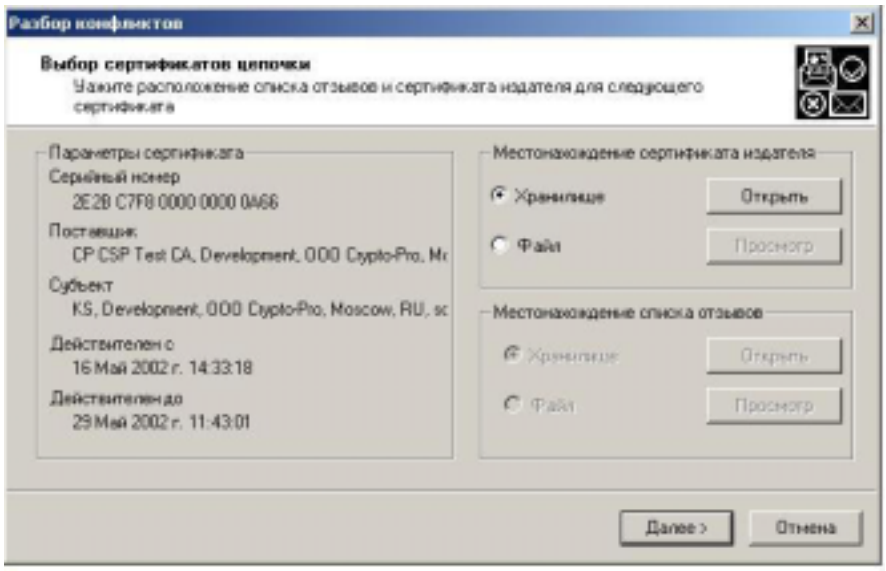

Рис. 12 Диалог выбора сертификатов для построения цепочки для проверки сертификата подписчика

Сертификаты в цепочке перебираются последовательно, от того, которым было подписано до корневого. Для каждого сертификата (кроме корневого) требуется указать соответствующий ему сертификат издателя и список отзыва сертификатов (CRL).

Сертификат издателя может быть выбран из хранилища или прочитан из файла.

При выбранном пункте «*Хранилище*» при нажатии кнопки «**Открыть**» вначале появляется диалог выбора хранилища из всех хранилищ текущего пользователя.

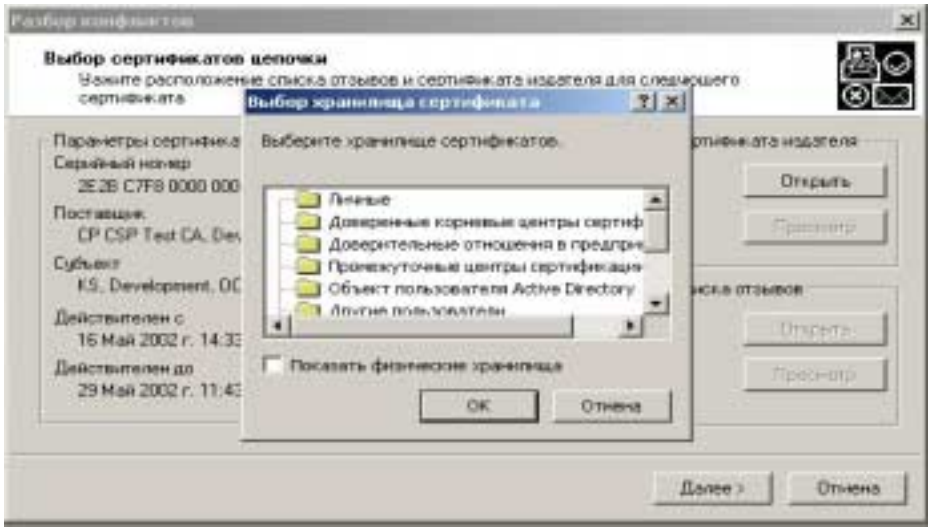

Рис. 13 Диалог выбора хранилища, где находится сертификат из цепочки

После выбора хранилища появляется диалог выбора сертификата из хранилища.

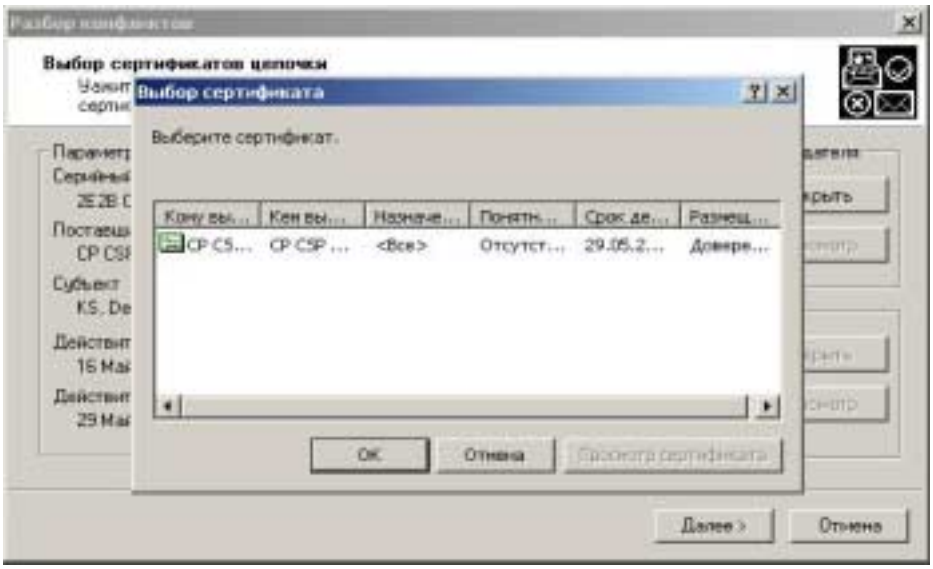

Рис. 14 Диалог выбора сертификата для построения цепочки

При выбранном пункте «*Файл*» появляется диалог открытия сертификата из файла.

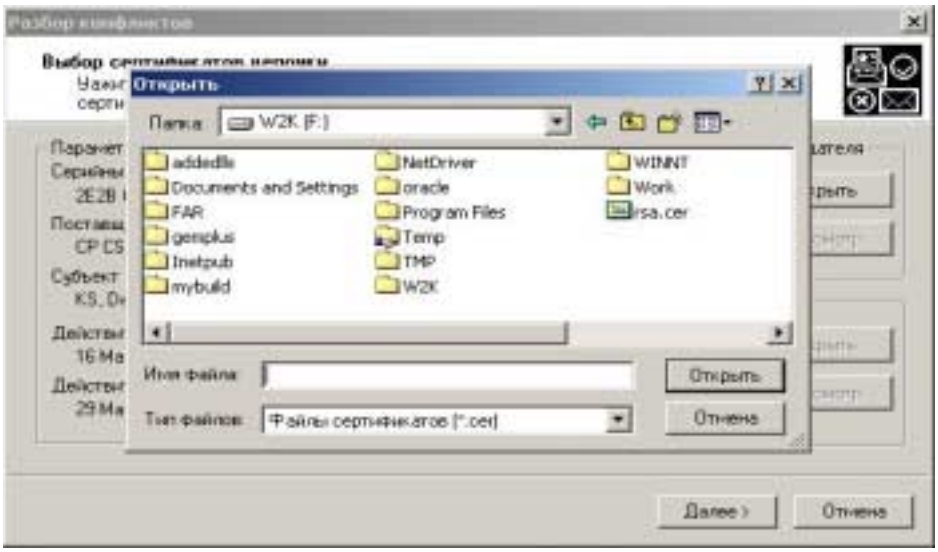

Рис. 15 Диалог открытия файла сертификата для построения цепочки

Если сертификат не является сертификатом издателя, то выводится сообщение об ошибке

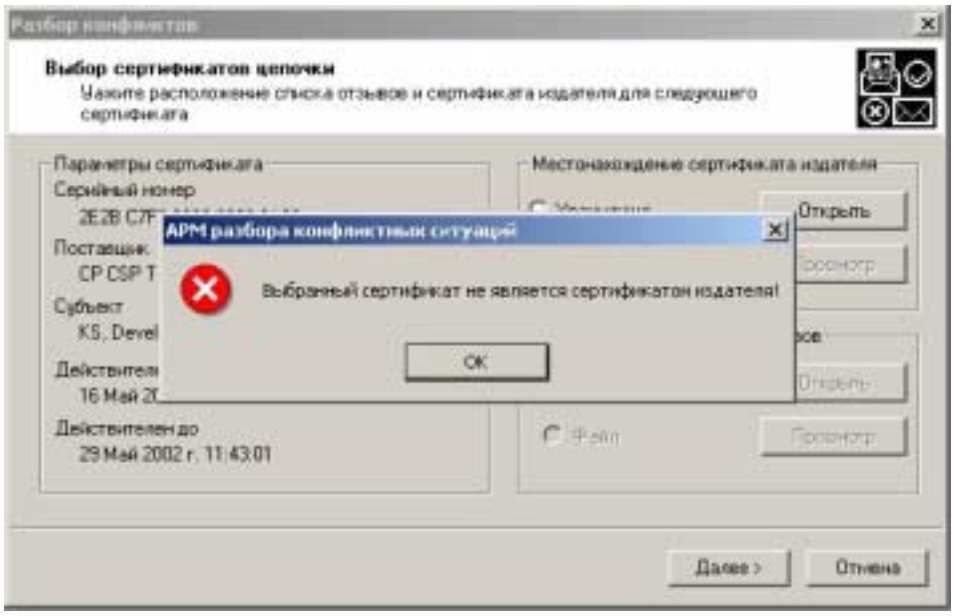

Рис. 16 Ошибка при чтении сертификата цепочки из файла

После выбора сертификата издателя его можно просмотреть нажатием кнопки «**Просмотр**».

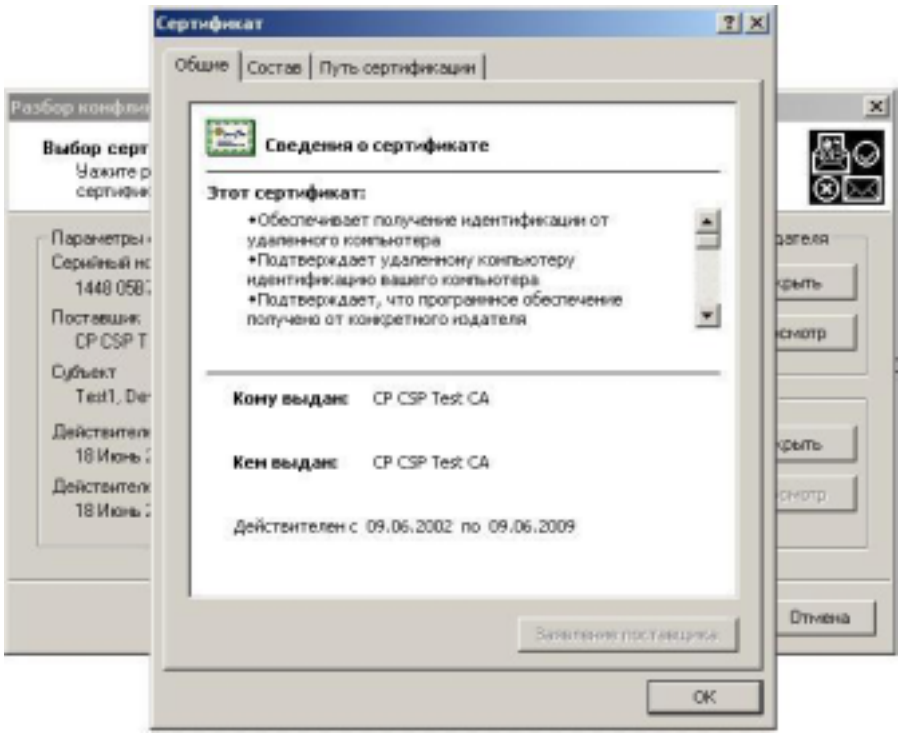

Рис. 17 Окно просмотра выбранного сертификата для построения цепочки

После выбора сертификата издателя появляется возможность выбрать соответствующий ему список отозванных сертификатов (CRL). CRL также может находиться в хранилище или в файле.

При выборе пункта «*Хранилище*» при нажатии кнопки «**Открыть**» появляется диалог выбора хранилища из всех хранилищ текущего пользователя.

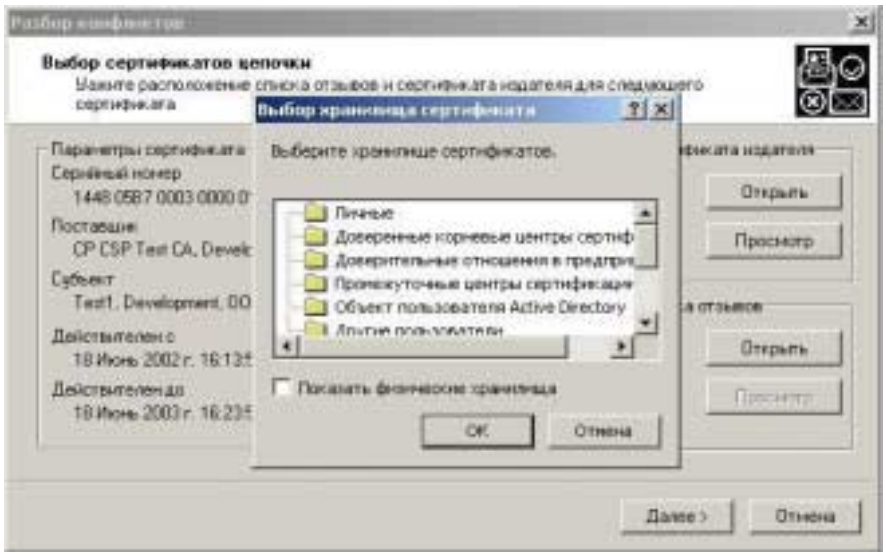

Рис. 18 Диалог выбора хранилища, где находится CRL

После выбора хранилища происходит автоматический поиск подходящего CRL в хранилище. Если таковой не найден, то выводится сообщение об ошибке

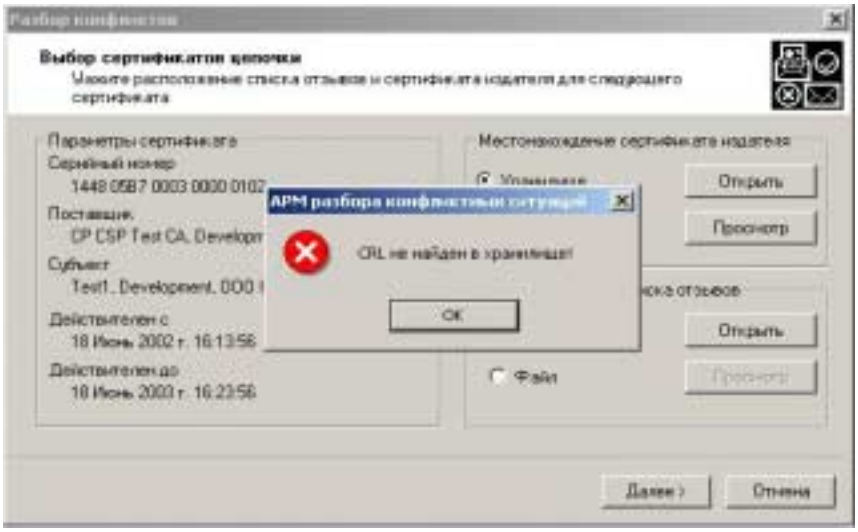

Рис. 19 Сообщение об ошибке поиска CRL в хранилище

При выборе пункта «*Файл*» появляется диалог выбора файла, содержащего CRL.

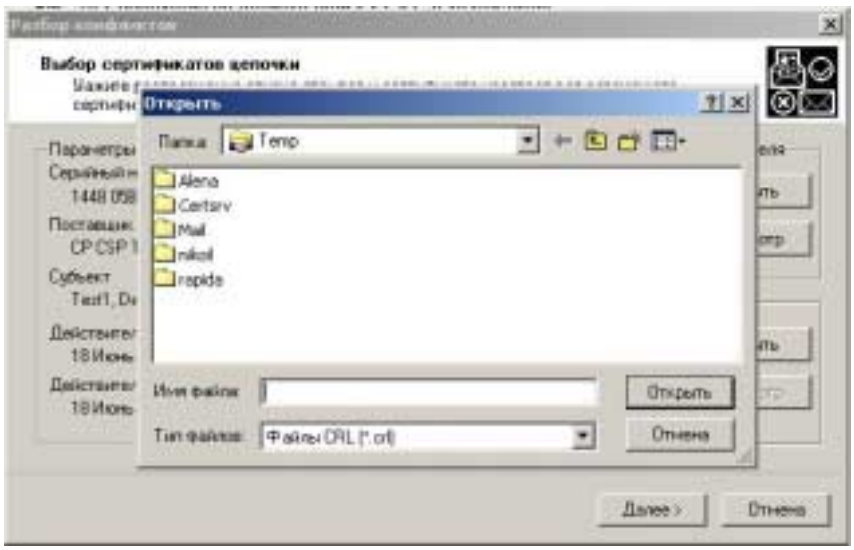

Рис. 20 Диалог открытия CRL из файла

Если был выбран файл CRL, который не был издан выбранным центром, то возникнет сообщение об ошибке.

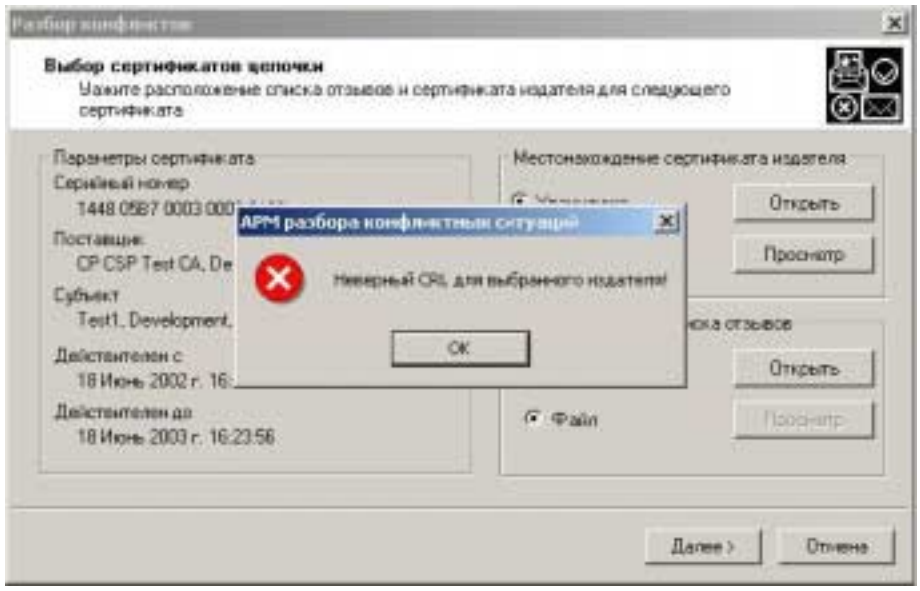

Рис. 21 Ошибка несоответствия выбранного CRL

После выбора CRL его можно просмотреть нажатием кнопки «**Просмотр**».

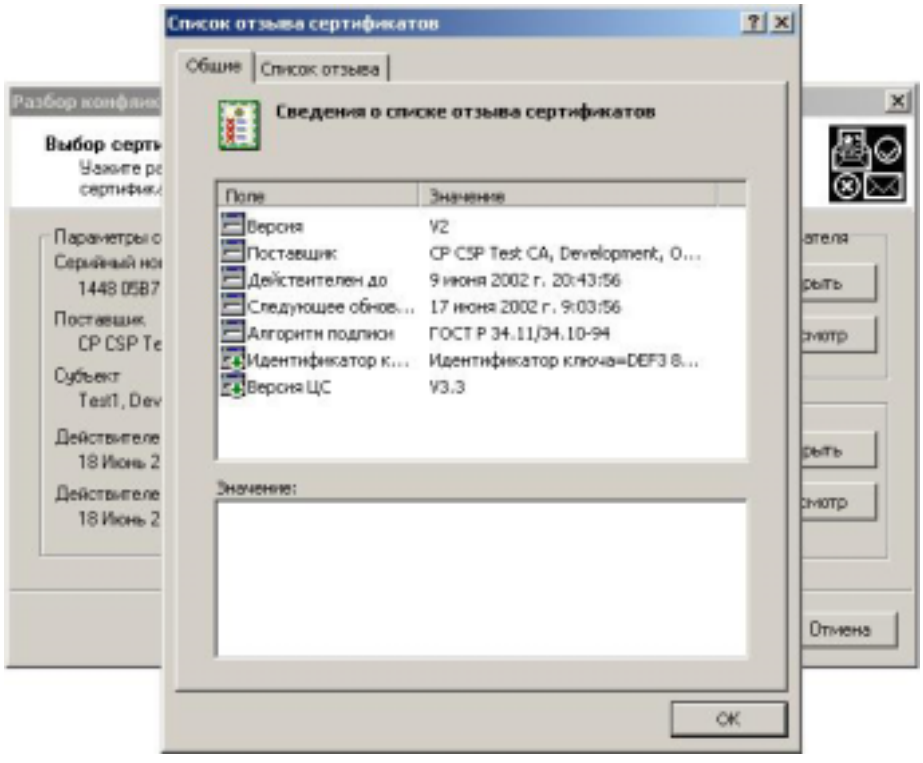

Рис. 22 Окно просмотра выбранного CRL

После нажатия кнопки «**Далее**» происходит переход к выбору сертификатов для проверки следующего сертификата в цепочке, либо, если в качестве сертификата издателя был указан сертификат корневого центра, переход к странице вывода результатов проверки подписи и сертификата.

7.5. Вывод результатов проверки подписи

На этой странице отображаются результаты проверки подписи и сертификата подписчика. Выводится порядковый номер подписи из всех присутствующих, результат криптографической проверки и результат проверки сертификата. В поле «*Комментарий*» выводятся все ошибки, возникшие при проверке сертификата.

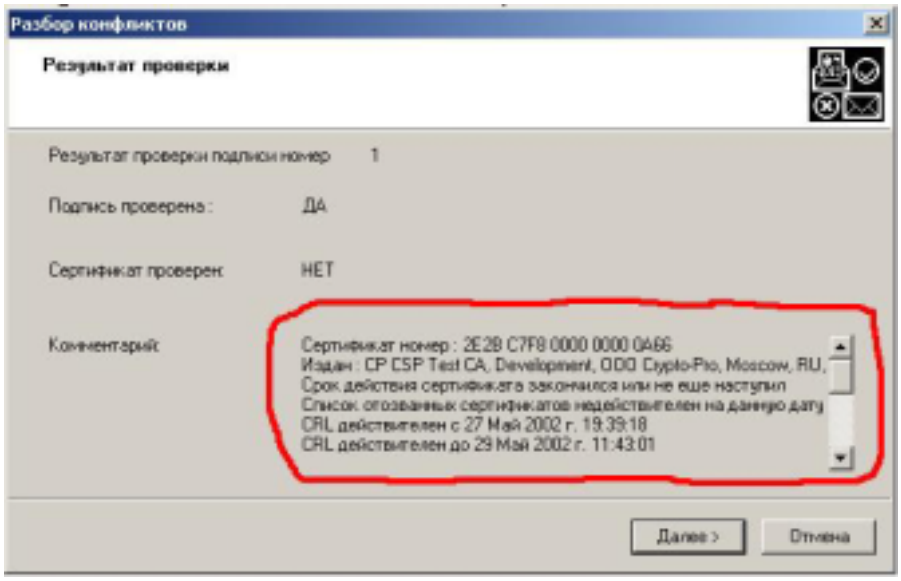

Рис. 23 Страница вывода результатов проверки подписи

После нажатия кнопки «**Далее**» происходит переход к проверке следующей подписи, если таковая существует. Если следующая подпись отсутствует, то происходит переход к странице выдачи результатов работы.

7.6. Результат работы мастера

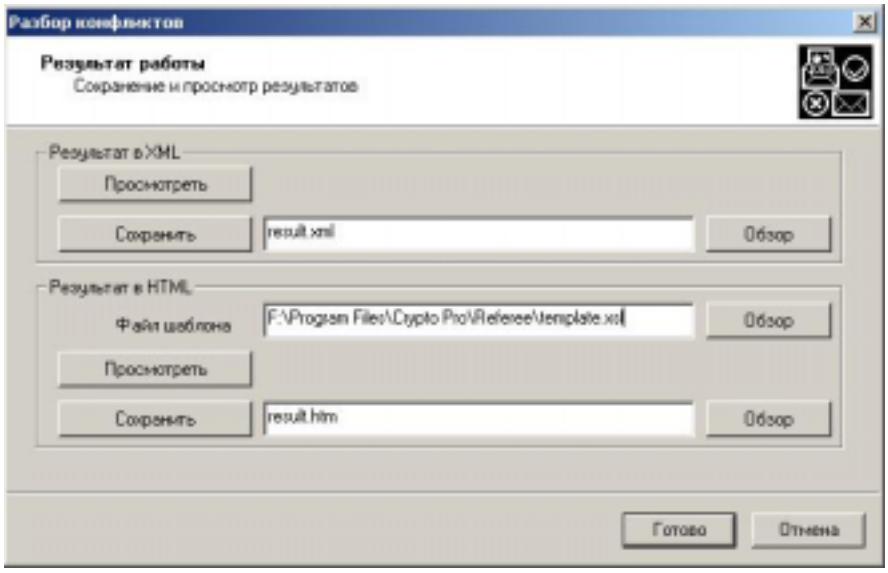

Рис. 24 Страница просмотра и сохранения результатов работы мастера

Данная страница позволяет просмотреть и сохранить отчет о результатах работы мастера. Отчет может быть представлен как в формате XML, так и в формате HTML. Просмотр осуществляется в окне браузера, использующегося системой по умолчанию для открытия XML и HTML файлов. Для создания отчета в виде HTML документа необходимо указать

месторасположение шаблона, с помощью которого XML преобразовывается в HTML. По умолчанию файл шаблона располагается в той же папке, где и модуль Referee.EXE.

Приложение 1. Протокол проверки ЭЦП в формате XML

Ниже приведён пример протокола проверки ЭЦП в формате XML:


```
<?xml version="1.0" encoding="windows-1251" ?>
- <pki:report xmlns:pki="http://www.cryptopro.ru/2001/Schema/WD1-PKI" xml:lang="ru" pki:report_time="27 Ноябрь 2002 г. 13:50:46">
  <pki:datafilename xml:lang="ru" pki:value="D:\temp\a.txt" />
  <pki:datafiletime xml:lang="ru" pki:value="04 Март 2002 г. 13:16:37" />
  <pki:sgnfilename xml:lang="ru" pki:value="D:\temp\a.sgn" />
  <pki:sgnfiletime xml:lang="ru" pki:value="27 Ноябрь 2002 г. 13:19:07" />
- <pki:signatures pki:count="1">
- <pki:signature pki:signature_order="1">
  <pki:signature_result xml:lang="ru" pki:value="ПРОВЕРЕНА" />
  <pki:signature_time xml:lang="ru" pki:value="27 Ноябрь 2002 г. 13:19:07" />
  <pki:cert_serial pki:value="1165 7779 0000 0000 0025" />
  <pki:cert_subject xml:lang="ru" pki:value="exp, Dev, CryptoPro, Moscow, RU" />
  <pki:cert_result xml:lang="ru" pki:value="ПРОВЕРЕН" />
  <pki:chain_status />
- <pki:certificates>
- <pki:used_cert pki:cert_order="1">
- <pki:certificate xmlns:pki="http://www.cryptopro.ru/2001/Schema/WD1-PKI">
  <pki:version pki:value="2">3</pki:version>
  <pki:serial-number>1165 7779 0000 0000 0025</pki:serial-number>
- <pki:signature>
- <pki:algorithm pki:id="1.2.643.2.2.3">
  <pki:name xml:lang="ru">ГОСТ Р 34.11/34.10-2001</pki:name>
    </pki:algorithm>
  - <pki:parameters>
  - <![CDATA[
  0500
```

```
]]>
</pki:parameters>
</pki:signature>
- <pki:issuer pki:count="6">
- <pki:rdn pki:order="6" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.3">
<pki:name xml:lang="ru">CN</pki:name>
<pki:value xml:lang="ru">BUG</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="5" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.11">
<pki:name xml:lang="ru">OU</pki:name>
<pki:value xml:lang="ru">Dev</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="4" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.10">
<pki:name xml:lang="ru">O</pki:name>
<pki:value xml:lang="ru">CryptoPro</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="3" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.7">
<pki:name xml:lang="ru">L</pki:name>
<pki:value xml:lang="ru">Moscow</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="2" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.6">
<pki:name xml:lang="ru">C</pki:name>
<pki:value xml:lang="ru">RU</pki:value>
```

```
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="1" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="7" pki:type-name="ia5-string" pki:id="1.2.840.113549.1.9.1">
<pki:name xml:lang="ru">E</pki:name>
<pki:value xml:lang="ru">sobolev@cryptopro.ru</pki:value>
</pki:rdn-attr>
</pki:rdn>
</pki:issuer>
- <pki:validity>
<pki:notBefore>6 ноября 2002 г. 15:09:00 UTC</pki:notBefore>
<pki:notAfter>6 ноября 2003 г. 15:18:00 UTC</pki:notAfter>
</pki:validity>
- <pki:subject pki:count="5">
- <pki:rdn pki:order="5" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.3">
<pki:name xml:lang="ru">CN</pki:name>
<pki:value xml:lang="ru">exp</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="4" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.11">
<pki:name xml:lang="ru">OU</pki:name>
<pki:value xml:lang="ru">Dev</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="3" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.10">
<pki:name xml:lang="ru">O</pki:name>
<pki:value xml:lang="ru">CryptoPro</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="2" pki:count="1">
```

- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.7">
<pki:name xml:lang="ru">L</pki:name>
<pki:value xml:lang="ru">Moscow</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="1" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.6">
<pki:name xml:lang="ru">C</pki:name>
<pki:value xml:lang="ru">RU</pki:value>
</pki:rdn-attr>
</pki:rdn>
</pki:subject>
- <pki:subject-public-key-info>
- <pki:public-key-algorithm>
- <pki:algorithm pki:id="1.2.643.2.2.20">
<pki:name xml:lang="ru">ГОСТ Р 34.10-94</pki:name>
</pki:algorithm>
- <pki:parameters>
- <![CDATA[
3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
]]>
</pki:parameters>
</pki:public-key-algorithm>
- <pki:subject-public-key>
- <pki:value pki:unused-bits="0">
- <![CDATA[
0481 8005 4E51 34D6 6163 EF19 3270 31CF
162B 7381 D510 C65D D6C4 1C8A 7A5D 6DD1
E30D DE0E BE4D C26A 8A10 8E63 2254 A557
22C5 A8FD 2806 5958 66D4 A229 61FA AB5A
FC3F 69AF 95C5 FFFA 2742 9231 6150 6408
FD93 8102 F5C6 F81B C956 CA58 D8F5 D083
A2A3 B1DC 1297 3164 3A4E 70A3 E09E 8E6D
0DDB C678 9870 6E63 F85B 71C1 BB43 579A
1395 32

]]>
</pki:value>
</pki:subject-public-key>
</pki:subject-public-key-info>
- <pki:extensions pki:count="4">
- <pki:extension pki:order="1" pki:critical="yes" pki:id="2.5.29.15">
<pki:name xml:lang="ru">Использование ключа</pki:name>
- <pki:value xml:lang="ru">
- <![CDATA[
Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
]]>
</pki:value>
</pki:extension>
- <pki:extension pki:order="2" pki:critical="no" pki:id="2.5.29.37">
<pki:name xml:lang="ru">Улучшенный ключ</pki:name>
- <pki:value xml:lang="ru">
- <![CDATA[
Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
]]>
</pki:value>
</pki:extension>
- <pki:extension pki:order="3" pki:critical="no" pki:id="2.5.29.14">
<pki:name xml:lang="ru">Идентификатор ключа субъекта</pki:name>
- <pki:value xml:lang="ru">
- <![CDATA[
4A30 7BB4 B5F8 7C5A CEBE DDCD C20A 0D50 8F86 E470
]]>
</pki:value>
</pki:extension>
- <pki:extension pki:order="4" pki:critical="no" pki:id="2.5.29.35">
<pki:name xml:lang="ru">Идентификатор ключа центра сертификатов</pki:name>
- <pki:value xml:lang="ru">
- <![CDATA[
Идентификатор ключа=38CB A568 4475 0E72 9FAA 2ED7 DC57 C494 77FB 546C
Поставщик сертификата:
Адрес каталога:
CN=BUG
OU=Dev
O=CryptoPro
L=Moscow

```
            C=RU
            E=sobolev@cryptopro.ru
        Серийный номер сертификата=05AA 649C 84EE 82B4 4B39 A85F A0F7 956E
    ]]>
    </pki:value>
    </pki:extension>
    </pki:extensions>
- <pki:signed-content>
- <pki:signature-algorithm>
- <pki:algorithm pki:id="1.2.643.2.2.3">
  <pki:name xml:lang="ru">ГОСТ Р 34.11/34.10-2001</pki:name>
    </pki:algorithm>
  - <pki:parameters>
  - <![CDATA[
  0500
    ]]>
    </pki:parameters>
    </pki:signature-algorithm>
- <pki:signature-value>
  - <pki:value pki:unused-bits="0">
      - <![CDATA[
      5161 4565 CF79 FA04 D45D CF7C 0779 8B73
      5E86 5537 11EE EBAD 1D5E 482D 1FD5 63DE
      24AC BA10 4334 1D51 07AB 18AC FE40 5495
      5673 40E6 D832 E30D 0E09 28FB 9D46 5776
```

```
]]>
</pki:value>
</pki:signature-value>
</pki:signed-content>
</pki:certificate>
</pki:used_cert>
- <pki:used_cert pki:cert_order="2">
- <pki:certificate xmlns:pki="http://www.cryptopro.ru/2001/Schema/WD1-PKI">
  <pki:version pki:value="2">3</pki:version>
  <pki:serial-number>05AA 649C 84EE 82B4 4B39 A85F A0F7 956E</pki:serial-number>
- <pki:signature>
- <pki:algorithm pki:id="1.2.643.2.2.3">
  <pki:name xml:lang="ru">ГОСТ Р 34.11/34.10-2001</pki:name>
    </pki:algorithm>
  - <pki:parameters>
  - <![CDATA[
  0500
```

```
]]>
</pki:parameters>
</pki:signature>
- <pki:issuer pki:count="6">
- <pki:rdn pki:order="6" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.3">
<pki:name xml:lang="ru">CN</pki:name>
<pki:value xml:lang="ru">BUG</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="5" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.11">
<pki:name xml:lang="ru">OU</pki:name>
<pki:value xml:lang="ru">Dev</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="4" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.10">
<pki:name xml:lang="ru">O</pki:name>
<pki:value xml:lang="ru">CryptoPro</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="3" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.7">
<pki:name xml:lang="ru">L</pki:name>
<pki:value xml:lang="ru">Moscow</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="2" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.6">
<pki:name xml:lang="ru">C</pki:name>
<pki:value xml:lang="ru">RU</pki:value>
```

```
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="1" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="7" pki:type-name="ia5-string" pki:id="1.2.840.113549.1.9.1">
<pki:name xml:lang="ru">E</pki:name>
<pki:value xml:lang="ru">sobolev@cryptopro.ru</pki:value>
</pki:rdn-attr>
</pki:rdn>
</pki:issuer>
- <pki:validity>
<pki:notBefore>1 ноября 2002 г. 11:33:28 UTC</pki:notBefore>
<pki:notAfter>1 ноября 2007 г. 11:33:28 UTC</pki:notAfter>
</pki:validity>
- <pki:subject pki:count="6">
- <pki:rdn pki:order="6" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.3">
<pki:name xml:lang="ru">CN</pki:name>
<pki:value xml:lang="ru">BUG</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="5" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.11">
<pki:name xml:lang="ru">OU</pki:name>
<pki:value xml:lang="ru">Dev</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="4" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.10">
<pki:name xml:lang="ru">O</pki:name>
<pki:value xml:lang="ru">CryptoPro</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="3" pki:count="1">
```

- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.7">
<pki:name xml:lang="ru">L</pki:name>
<pki:value xml:lang="ru">Moscow</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="2" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="4" pki:type-name="printable-string" pki:id="2.5.4.6">
<pki:name xml:lang="ru">C</pki:name>
<pki:value xml:lang="ru">RU</pki:value>
</pki:rdn-attr>
</pki:rdn>
- <pki:rdn pki:order="1" pki:count="1">
- <pki:rdn-attr pki:order="1" pki:type="7" pki:type-name="ia5-string" pki:id="1.2.840.113549.1.9.1">
<pki:name xml:lang="ru">E</pki:name>
<pki:value xml:lang="ru">sobolev@cryptopro.ru</pki:value>
</pki:rdn-attr>
</pki:rdn>
</pki:subject>
- <pki:subject-public-key-info>
- <pki:public-key-algorithm>
- <pki:algorithm pki:id="1.2.643.2.2.19">
<pki:name xml:lang="ru">ГОСТ Р 34.10-2001</pki:name>
</pki:algorithm>
- <pki:parameters>
- <![CDATA[
3012 0607 2A85 0302 0223 0106 072A 8503 0202 1E01
]]>
</pki:parameters>
</pki:public-key-algorithm>
- <pki:subject-public-key>
- <pki:value pki:unused-bits="0">
- <![CDATA[
0440 DB12 7CF0 18E7 ECB8 34AA 9AFE 6989
E879 FF73 E934 639B E448 2B80 AA0F A858
E158 98E3 6A9F 43E8 F446 709C 44E9 C319

C49B D408 969B 65EB 5AAB BA1F E47E F0E7
17C0
]]>
</pki:value>
</pki:subject-public-key>
</pki:subject-public-key-info>
- <pki:extensions pki:count="**6**">
- <pki:extension pki:order="**1**" pki:critical="**no**" pki:id="**1.3.6.1.4.1.311.20.2**">
<pki:name xml:lang="**ru**">**Шаблон сертификата**</pki:name>
- <pki:value xml:lang="**ru**">
- <![CDATA[
CA
]]>
</pki:value>
</pki:extension>
- <pki:extension pki:order="**2**" pki:critical="**no**" pki:id="**2.5.29.15**">
<pki:name xml:lang="**ru**">**Использование ключа**</pki:name>
- <pki:value xml:lang="**ru**">
- <![CDATA[
Неотрекаемость , Подписывание сертификатов , Автономное подписание списка отзыва (CRL) , Подписание списка отзыва (CRL)(46)
]]>
</pki:value>
</pki:extension>
- <pki:extension pki:order="**3**" pki:critical="**yes**" pki:id="**2.5.29.19**">
<pki:name xml:lang="**ru**">**Основные ограничения**</pki:name>
- <pki:value xml:lang="**ru**">
- <![CDATA[
Тип субъекта=ЦС
Ограничение на длину пути=Отсутствует
]]>
</pki:value>
</pki:extension>
- <pki:extension pki:order="**4**" pki:critical="**no**" pki:id="**2.5.29.14**">
<pki:name xml:lang="**ru**">**Идентификатор ключа субъекта**</pki:name>
- <pki:value xml:lang="**ru**">
- <![CDATA[
38CB A568 4475 0E72 9FAA 2ED7 DC57 C494 77FB 546C

]]>

</pki:value>

</pki:extension>

- <pki:extension pki:order="**5**" pki:critical="**no**" pki:id="**2.5.29.31**">

<pki:name xml:lang="**ru**">**Точки распространения списков отзыва (CRL)**</pki:name>

- <pki:value xml:lang="**ru**">

- <![CDATA[

[1]Точка распределения списка отзыва (CRL)
Имя точки распространения:
Полное имя:
URL=http://bug2k.cp.ru/CertEnroll/BUG.crl
[2]Точка распределения списка отзыва (CRL)
Имя точки распространения:
Полное имя:
URL=file://\\BUG2K.cp.ru\CertEnroll\BUG.crl

]]>

</pki:value>

</pki:extension>

- <pki:extension pki:order="**6**" pki:critical="**no**" pki:id="**1.3.6.1.4.1.311.21.1**">

<pki:name xml:lang="**ru**">**Версия ЦС**</pki:name>

- <pki:value xml:lang="**ru**">

- <![CDATA[

V0.0

]]>

</pki:value>

</pki:extension>

</pki:extensions>

- <pki:signed-content>

- <pki:signature-algorithm>

- <pki:algorithm pki:id="**1.2.643.2.2.3**">

<pki:name xml:lang="**ru**">**ГОСТ Р 34.11/34.10-2001**</pki:name>

</pki:algorithm>

- <pki:parameters>

- <![CDATA[

0500

```
]]>
</pki:parameters>
</pki:signature-algorithm>
- <pki:signature-value>
  - <pki:value pki:unused-bits="0">
      - <![CDATA[
      36FF 92F1 7C9C 5B41 280E 170D 3354 D9A0
      3A30 1440 13C7 CF9F A5F6 CD5A E421 8B1B
      B6BF E62C 66C2 EE8B 396F 6B0D 851A A44A
      B1AA 31EF C94F 4495 62F1 6C52 E491 CEB5
    ]]>
    </pki:value>
    </pki:signature-value>
    </pki:signed-content>
    </pki:certificate>
    </pki:used_cert>
    </pki:certificates>
    </pki:signature>
    </pki:signatures>
    </pki:report>
```


Приложение 2. Протокол проверки ЭЦП в формате HTML

Ниже приведён пример протокола проверки ЭЦП в формате HTML, выведенный в окне браузера Internet Explorer 6.0:

Отчет
Время отчета: 27 Ноябрь 2002 г. 13:51:11
Проверен файл: D:\temp\a.txt
Созданный: 04 Март 2002 г. 13:16:37
Подпись содержится в файле: D:\temp\a.sgn
Созданном: 27 Ноябрь 2002 г. 13:19:07
Количество проверенных подписей: 1
Алгоритм подписи:
Подпись - ПРОВЕРЕНА
Подпись была создана: 27 Ноябрь 2002 г. 13:19:07
Серийный номер: 1165 7779 0000 0000 0025
Субьект: exp, Dev, CryptoPro, Moscow, RU
Сертификат, которым подписано - ПРОВЕРЕН
Результат проверки цепочки сертификатов
Сертификаты, использованные при проверке подписи
Сертификат X.509:
Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Кому выдан:
exp
Кем выдан:
BUG

Действителен с 6 ноября 2002 г. 15:09:00 UTC по 6 ноября 2003 г. 15:18:00 UTC
Версия: 3 (0x2)
Серийный номер:
1165 7779 0000 0000 0025
Алгоритм подписи:
Название:
ГОСТ Р 34.11/34.10-2001
Идентификатор:
1.2.643.2.2.3
Параметры:
0500
Издатель:
CN = BUG
OU = Dev
O = CryptoPro
L = Moscow
C = RU
E = sobolev@cryptopro.ru
Срок действия:
Действителен с:
6 ноября 2002 г. 15:09:00 UTC
Действителен по:
6 ноября 2003 г. 15:18:00 UTC
Субъект:
CN = exp
OU = Dev
O = CryptoPro
L = Moscow
C = RU
Открытый ключ:
Алгоритм открытого ключа:
Название:
ГОСТ Р 34.10-94
Идентификатор:
1.2.643.2.2.20
Параметры:
3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01
Значение:
0481 8005 4E51 34D6 6163 EF19 3270 31CF
162B 7381 D510 C65D D6C4 1C8A 7A5D 6DD1
E30D DE0E BE4D C26A 8A10 8E63 2254 A557
22C5 A8FD 2806 5958 66D4 A229 61FA AB5A
FC3F 69AF 95C5 FFFA 2742 9231 6150 6408
FD93 8102 F5C6 F81B C956 CA58 D8F5 D083
A2A3 B1DC 1297 3164 3A4E 70A3 E09E 8E6D
0DDB C678 9870 6E63 F85B 71C1 BB43 579A
1395 32
Расширения X.509
1. Расширение 2.5.29.15 (критическое)
Название:
Использование ключа
Значение:
Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
Название:
Улучшенный ключ
Значение:
Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название:

Идентификатор ключа субъекта
Значение:
4A30 7BB4 B5F8 7C5A CEBE DDCD C20A 0D50 8F86 E470
4. Расширение 2.5.29.35
Название:
Идентификатор ключа центра сертификатов
Значение:
Идентификатор ключа=38CB A568 4475 0E72 9FAA 2ED7 DC57 C494 77FB 546C
Поставщик сертификата:
Адрес каталога:
CN=BUG
OU=Dev
O=CryptoPro
L=Moscow
C=RU
E=sobolev@cryptopro.ru
Серийный номер сертификата=05AA 649C 84EE 82B4 4B39 A85F A0F7 956E
Подпись:
Алгоритм подписи:
Название:
ГОСТ Р 34.11/34.10-2001
Идентификатор:
1.2.643.2.2.3
Параметры:
0500
Значение:
5161 4565 CF79 FA04 D45D CF7C 0779 8B73
5E86 5537 11EE EBAD 1D5E 482D 1FD5 63DE
24AC BA10 4334 1D51 07AB 18AC FE40 5495
5673 40E6 D832 E30D 0E09 28FB 9D46 5776
Сертификат X.509:
Сведения о сертификате:
Этот сертификат:
Кому выдан:
BUG
Кем выдан:
BUG
Действителен с 1 ноября 2002 г. 11:33:28 UTC по 1 ноября 2007 г. 11:33:28 UTC
Версия: 3 (0x2)
Серийный номер:
05AA 649C 84EE 82B4 4B39 A85F A0F7 956E
Алгоритм подписи:
Название:
ГОСТ Р 34.11/34.10-2001
Идентификатор:
1.2.643.2.2.3
Параметры:
0500
Издатель:
CN = BUG
OU = Dev
O = CryptoPro
L = Moscow
C = RU
E = sobolev@cryptopro.ru
Срок действия:
Действителен с:
1 ноября 2002 г. 11:33:28 UTC
Действителен по:
1 ноября 2007 г. 11:33:28 UTC

Субъект:
CN = BUG
OU = Dev
O = CryptoPro
L = Moscow
C = RU
E = sobolev@cryptopro.ru
Открытый ключ:
Алгоритм открытого ключа:
Название:
ГОСТ Р 34.10-2001
Идентификатор:
1.2.643.2.2.19
Параметры:
3012 0607 2A85 0302 0223 0106 072A 8503 0202 1E01
Значение:
0440 DB12 7CF0 18E7 ECB8 34AA 9AFE 6989
E879 FF73 E934 639B E448 2B80 AA0F A858
E158 98E3 6A9F 43E8 F446 709C 44E9 C319
C49B D408 969B 65EB 5AAB BA1F E47E F0E7
17C0
Расширения X.509
1. Расширение 1.3.6.1.4.1.311.20.2
Название:
Шаблон сертификата
Значение:
CA
2. Расширение 2.5.29.15
Название:
Использование ключа
Значение:
Неотрекаемость , Подписывание сертификатов , Автономное подписание списка отзыва (CRL) , Подписание списка отзыва (CRL)(46)
3. Расширение 2.5.29.19 (критическое)
Название:
Основные ограничения
Значение:
Тип субъекта=ЦС
Ограничение на длину пути=Отсутствует
4. Расширение 2.5.29.14
Название:
Идентификатор ключа субъекта
Значение:
38CB A568 4475 0E72 9FAA 2ED7 DC57 C494 77FB 546C
5. Расширение 2.5.29.31
Название:
Точки распространения списков отзыва (CRL)
Значение:
[1]Точка распределения списка отзыва (CRL)
    Имя точки распространения:
        Полное имя:
            URL=http://bug2k.cp.ru/CertEnroll/BUG.crl
[2]Точка распределения списка отзыва (CRL)
    Имя точки распространения:
        Полное имя:
            URL=file://\\BUG2K.cp.ru\CertEnroll\BUG.crl
6. Расширение 1.3.6.1.4.1.311.21.1
Название:
Версия ЦС
Значение:

V0.0
Подпись:
Алгоритм подписи:
Название:
ГОСТ Р 34.11/34.10-2001
Идентификатор:
1.2.643.2.2.3
Параметры:
0500
Значение:
36FF 92F1 7C9C 5B41 280E 170D 3354 D9A0
3A30 1440 13C7 CF9F A5F6 CD5A E421 8B1B
B6BF E62C 66C2 EE8B 396F 6B0D 851A A44A
B1AA 31EF C94F 4495 62F1 6C52 E491 CEB5