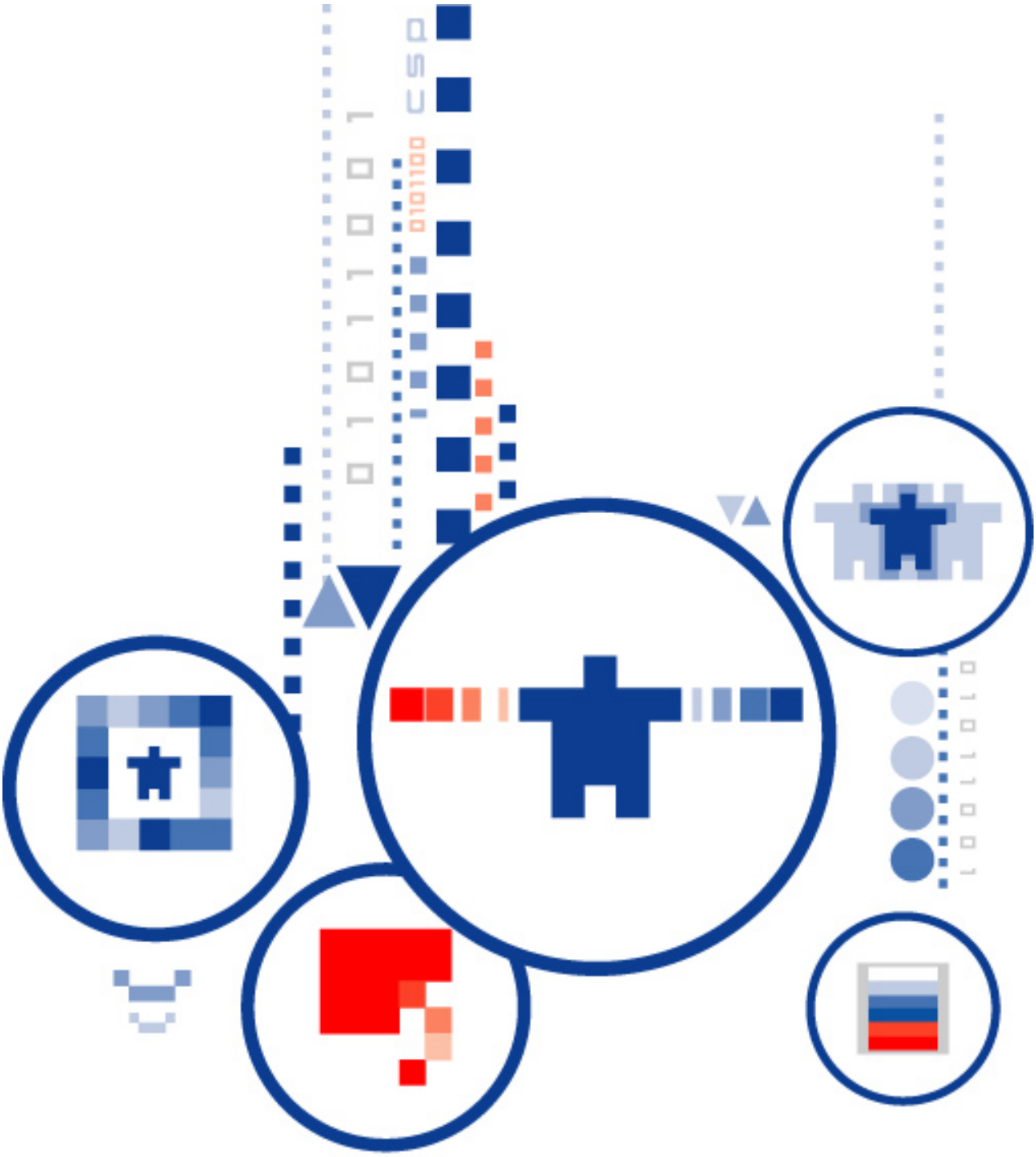
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 08-ЛУ

ЖТЯИ.00035-01 90 08



КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Программный комплекс разбора конфликтных ситуаций. Руководство по эксплуатации

Содержание

Содержание **2**

1. Аннотация **3**

2. Общие положения **4**

3. Требования для работы с приложением **5**

4. Состав программного обеспечения **6**

5. Назначение программного комплекса **7**

6. Порядок проведения разбора конфликтных ситуаций **8**

6.1. Порядок разбора конфликтной ситуации, связанной с проверкой ЭЦП уполномоченного лица УЦ 8

6.2. Порядок разбора конфликтной ситуации, связанной с проверкой ЭЦП электронного документа 9

6.2.1. Случаи невозможности проверки значения ЭЦП 10

7. Разбор конфликтной ситуации, связанной с проверкой ЭЦП уполномоченного лица УЦ 11

7.1. Стартовая страница мастера 11

7.2. Выбор режима 11

7.3. Выбор сертификата, изданного УЦ 12

7.4. Проверка цепочки сертификатов 15

7.5. Вывод результатов проверки подписи издателя 19

7.6. Результат работы мастера 20

8. Разбор конфликтной ситуации, связанной с проверкой ЭЦП электронного документа 21

8.1. Стартовая страница мастера 21

8.2. Выбор режима 21

8.3. Выбор электронного документа для проверки 21

8.4. Выбор сертификата подписчика 23

8.4.1. Подтверждение подлинности ЭЦП с использованием сертификата 24

8.4.2. Подтверждение подлинности ЭЦП с использованием только открытого ключа 31

8.5. Вывод результатов проверки подписи 32

8.6. Результат работы мастера 33

9. Удаление программного обеспечения АРМ разбора конфликтных ситуаций 35

10. Перечень рисунков **36**

11. Приложения **38**

11.1. Приложение 1. Пример протокола проверки ЭЦП в формате XML 38

11.2. Приложение 2. Пример протокола проверки ЭЦП в формате HTML 48

1. Аннотация

Данный документ содержит описание процесса эксплуатации программного комплекса (ПК) АРМ разбора конфликтных ситуаций (АРМ РКС), входящего в состав программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (КриптоПро УЦ).

Документ предназначен для администраторов безопасности как руководство по эксплуатации АРМ РКС.

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

127 018, Москва, улица Сущевский вал, 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

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, гарантирующих 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.

3. Требования для работы с приложением

Для установки и эксплуатации ПО АРМ разбора конфликтных ситуаций необходимо следующее программное обеспечение:

- Операционная система - Microsoft Windows Server 2000 с установленным пакетом обновлений SP4, Microsoft Windows Professional 2000 с установленным пакетом обновлений SP4, Microsoft Windows Server 2003 с установленным пакетом обновлений SP2, Microsoft Windows XP с установленным пакетом обновлений SP2. Операционные системы могут быть как английской версии, так и русской;
- Microsoft Internet Explorer 5.0 (и выше);
- Средство криптографической защиты информации (СКЗИ) КриптоПро CSP.

При использовании операционной системы Microsoft Windows 2000 или Microsoft Windows XP устанавливается СКЗИ «КриптоПро CSP» версии 2.0 (исполнение 4 для класса защиты КС2) или СКЗИ «КриптоПро CSP» версии 3.0 (исполнение 6 для класса защиты КС2).

При использовании операционной системы Microsoft Windows 2003 устанавливается СКЗИ «КриптоПро CSP» версии 3.0 (исполнение 6 для класса защиты КС2).

Установка СКЗИ «КриптоПро CSP» осуществляется в соответствии с эксплуатационной документацией.

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 владельца сертификата открытого ключа подписи, выполнившего ее формирование.

Также программный комплекс предназначен для выполнения процедуры подтверждения подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего Центра в выданных им сертификатах открытых ключей подписей.

6. Порядок проведения разбора конфликтных ситуаций

Программный комплекс АРМ РКС обеспечивает выполнение технических мероприятий при разборе следующих конфликтных ситуаций, связанных с практикой применения ЭЦП:

- конфликтные ситуации, связанные с удостоверением подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего Центра в выданных им в электронном виде сертификатах открытых ключей подписи;
- конфликтные ситуации, связанные с удостоверением подлинности электронных цифровых подписей владельцев ключей подписи в электронных документах, порожденных в автоматизированных системах.

6.1. Порядок разбора конфликтной ситуации, связанной с проверкой ЭЦП уполномоченного лица УЦ

Одной из целевых функций Удостоверяющего Центра является подтверждение подлинности электронных цифровых подписей уполномоченного лица Удостоверяющего Центра в выданных им сертификатах открытых ключей подписи.

Проверке сертификата открытого ключа подписи, изданного Удостоверяющим Центром, подлежит сертификат открытого ключа подписи, выданный владельцу в электронном виде.

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, если это определено соглашениями сторон.

Разбор конфликтной ситуации проводится на АРМ РКС (запуском программы Referee.EXE) для сертификата открытого ключа подписи, издание которого оспаривается.

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

Проверка изданного сертификата открытого ключа подписи включает в себя выполнение следующих действий:

- определение сертификата, необходимого для проверки ЭЦП издателя;
- проверка ЭЦП издателя сертификата открытого ключа, путем построения цепочки сертификатов до сертификата корневого Удостоверяющего центра;
- проверка действительности сертификатов на текущий момент времени;
- проверка отсутствия сертификатов в списке отозванных сертификатов (COC, CRL).

При проверке ЭЦП издателя, верификации цепочки сертификатов, отсутствии сертификата в CRL, авторство издателя считается установленным.

Несовпадение даты выпуска сертификата и сроков действия сертификата издателя и/или сроков действия секретного ключа не влияют на определение авторства издания сертификата. На их основе можно сделать предположение о несоблюдении

уполномоченным лицом регламента в части сроков действия ключей и сертификатов уполномоченного лица Удостоверяющего центра.

6.2. Порядок разбора конфликтной ситуации, связанной с проверкой ЭЦП электронного документа

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, если это определено соглашениями сторон.

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 списке отозванных сертификатов (COC, 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 автоматизированной системы, 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.

6.2.1. Случаи невозможности проверки значения ЭЦП

При отсутствии 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, связанной с проверкой ЭЦП уполномоченного лица УЦ

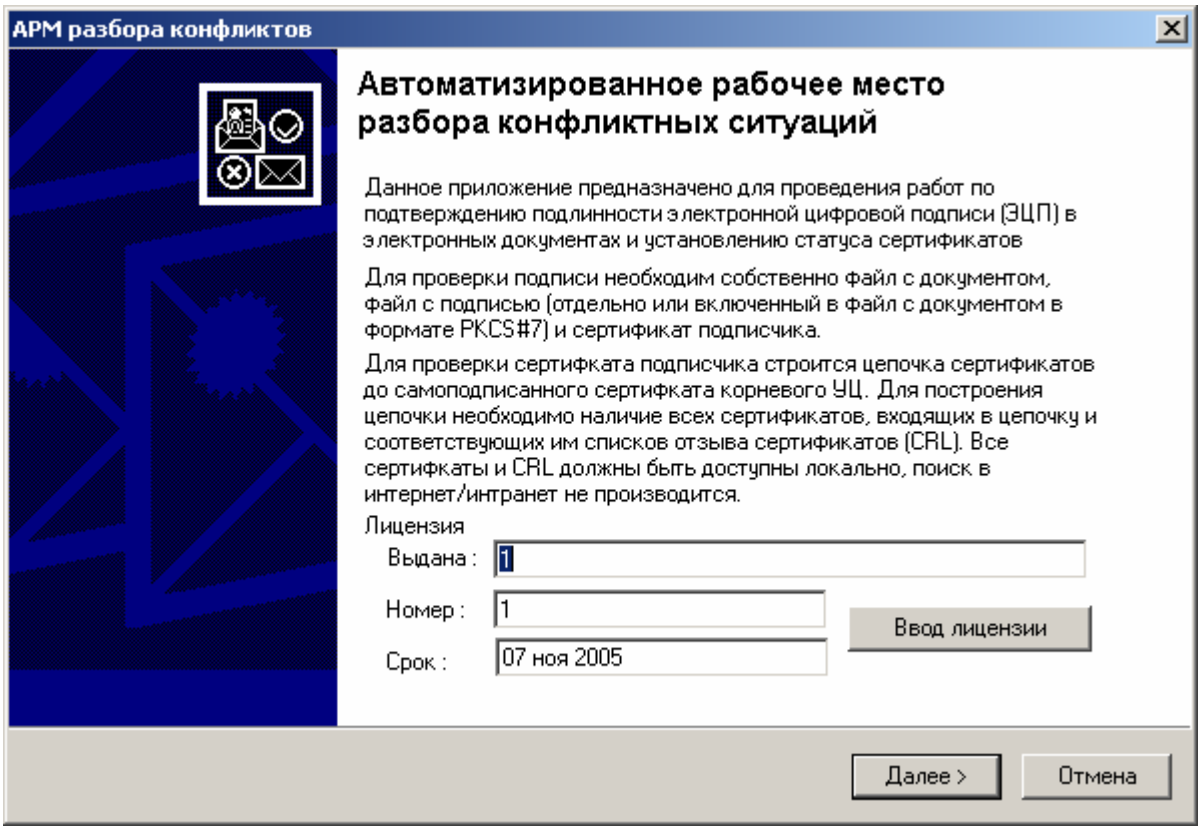
Для запуска процедуры разбора конфликтной ситуации необходимо запустить исполняемый файл Referee.EXE.

АРМ РКС позволяет проверять подпись издателя в сертификате открытого ключа, изданного в форме электронного документа в соответствии с рекомендациями X.509.

7.1. Стартовая страница мастера

При запуске программы выводится страница, содержащая краткую информацию о программе, а также информацию о владельце лицензии на право пользования данным ПО с указанием срока его действия. Нажатие кнопки **Ввод лицензии** обеспечит ввод серийного номера лицензии в случае продления срока действия лицензии (если лицензия была выдана на ограниченный срок), либо в случае, если серийный номер лицензии не был введен при установке программного обеспечения.

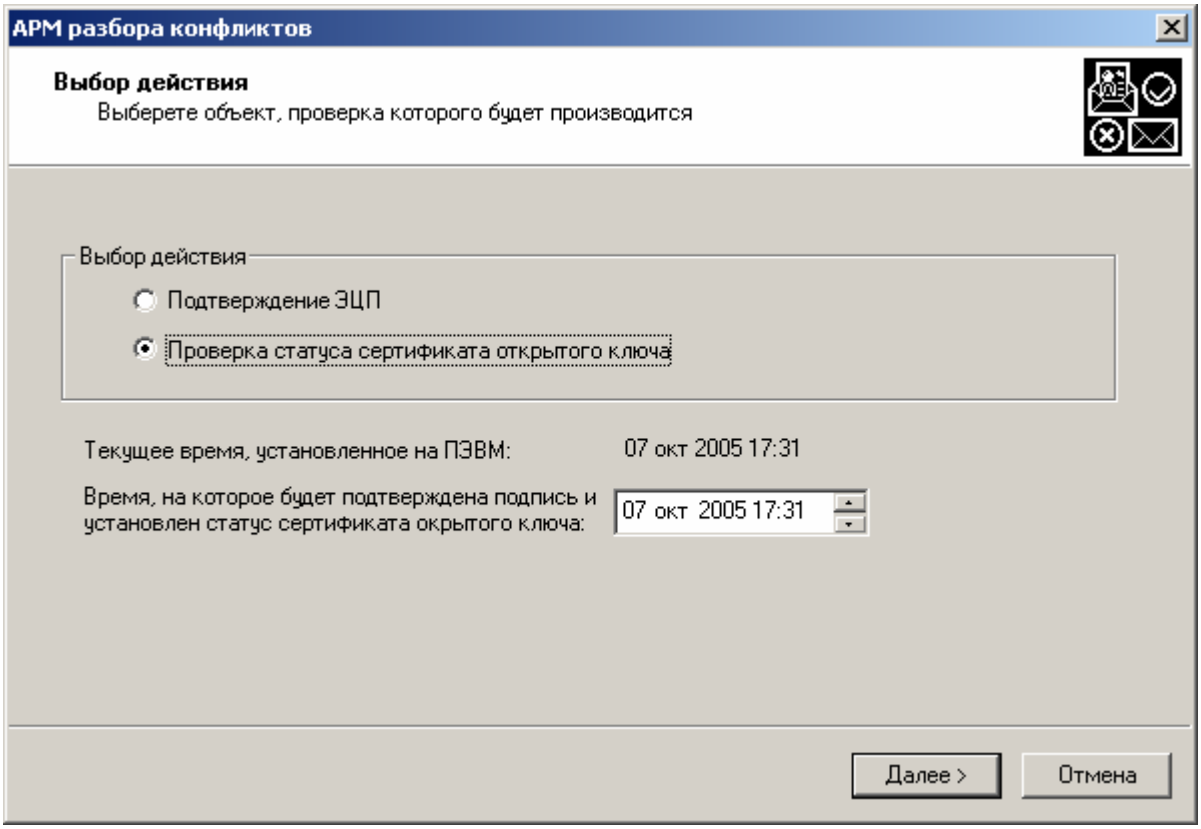
Рисунок 1. Стартовая страница



7.2. Выбор режима

В следующем окне выберите в качестве действия **Проверка статуса сертификата открытого ключа** и задайте время, на момент наступления которого требуется установить статус сертификата.

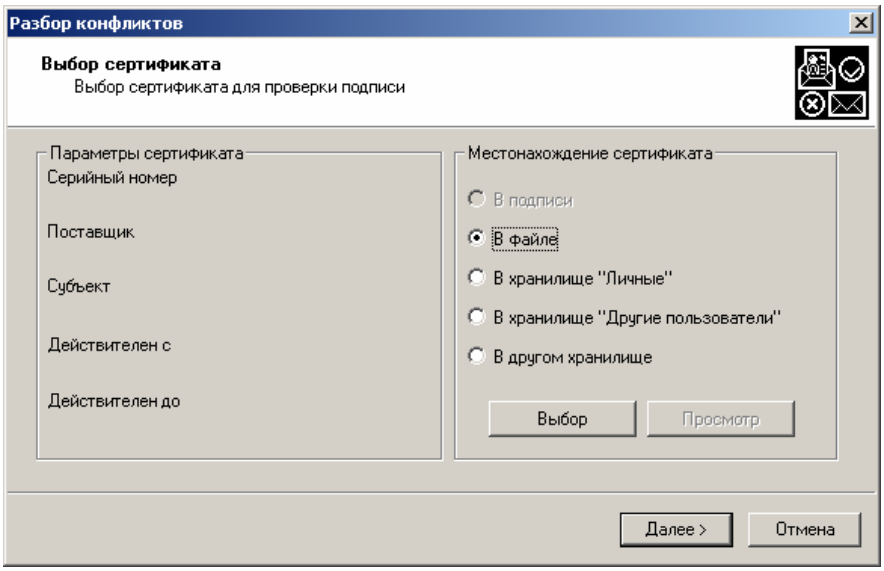
Рисунок 2. Выбор действия



7.3. Выбор сертификата, изданного УЦ

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

Рисунок 3. Выбор сертификата для проверки подписи



Сертификат может находиться

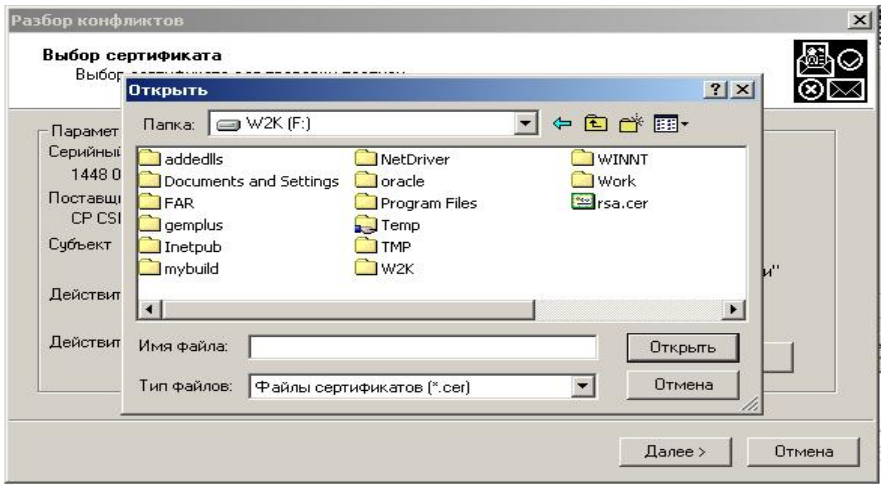
- В файле (кодировка DER или Base-64 без заголовка)
- В хранилище «Личные» (MY)

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

После выбора местонахождения сертификата необходимо его открыть кнопкой «**Выбор**».

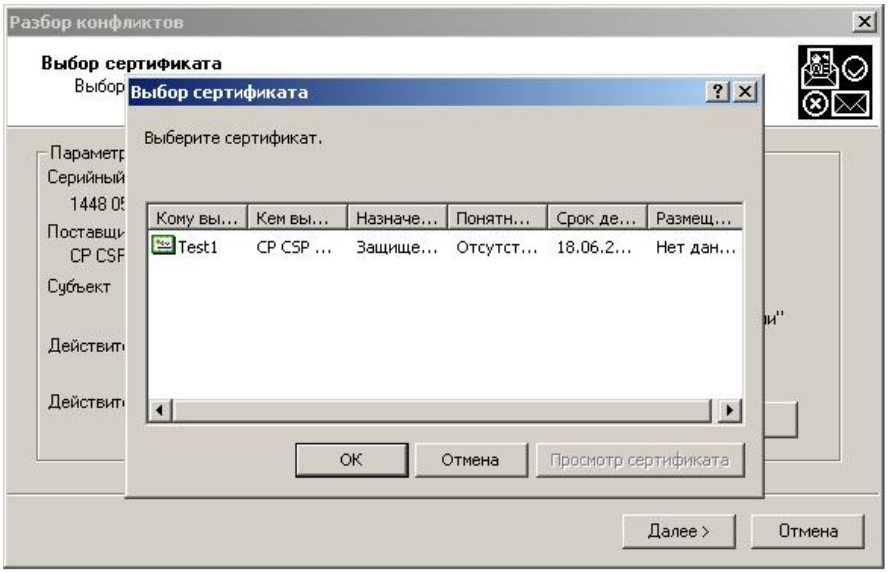
При выборе пункта «*В файле*» появится диалог открытия файла.

Рисунок 4. Выбор сертификата для проверки из файла



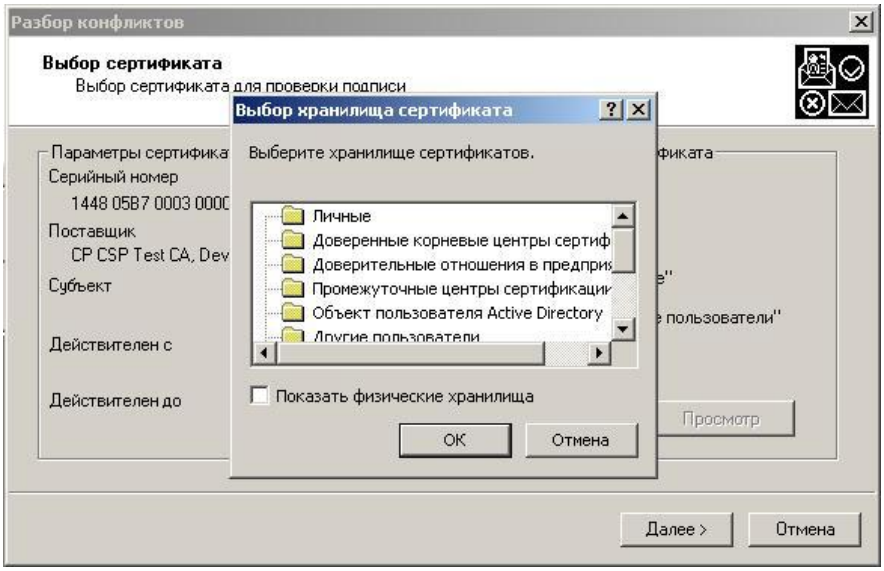
Если выбраны пункты «*В хранилище «Личные»* или «*В хранилище «Другие пользователи»*, то при нажатии кнопки «**Выбор**» появится окно диалога выбора файла из соответствующего хранилища.

Рисунок 5. Выбор сертификат для проверки из хранилища



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

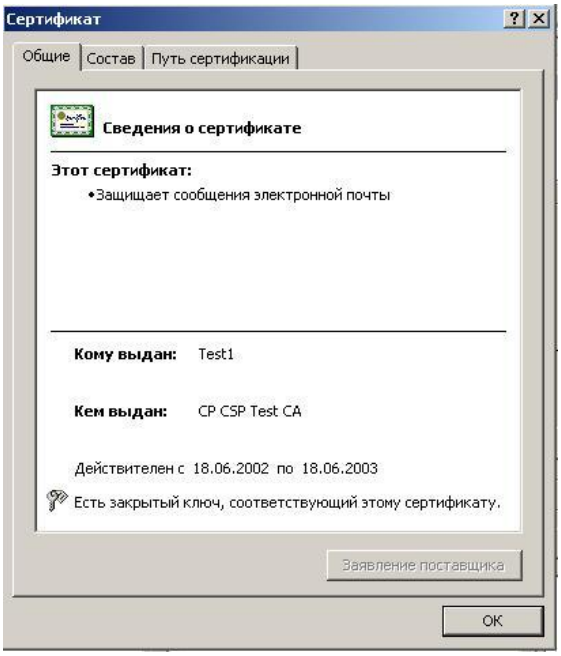
Рисунок 6. Выбор хранилища, где находится сертификат для проверки



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

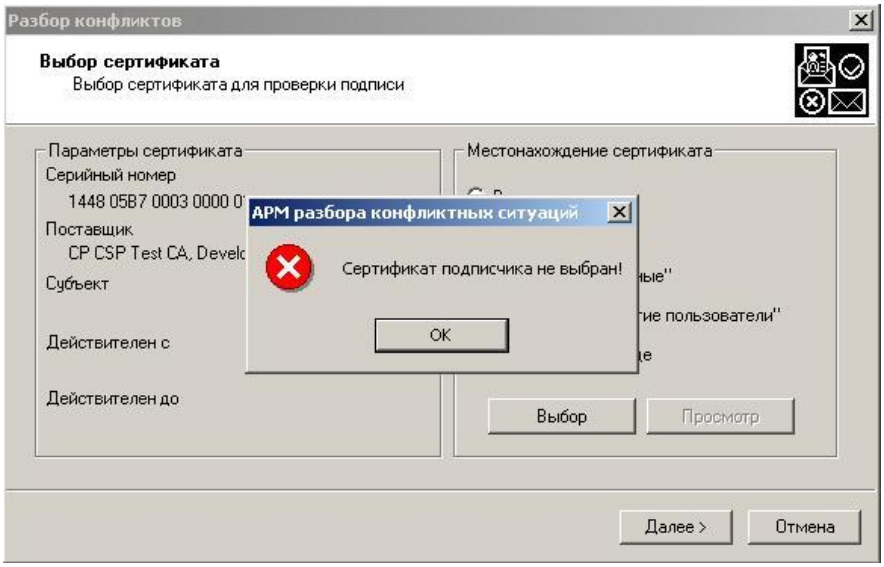
Кнопка «**Просмотр**» выводит окно просмотра выбранного сертификата.

Рисунок 7. 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!

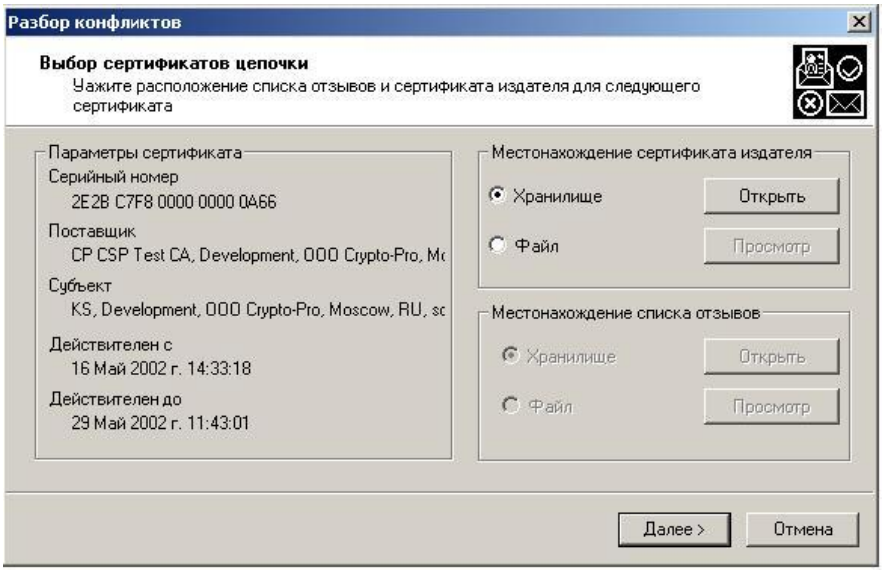
Рисунок 8. Сообщение об ошибке при выборе сертификата для проверки



7.4. Проверка цепочки сертификатов

На следующем шаге мастера выбираются сертификаты и списки отзыва, при помощи которых строится цепочка и проверяется ЭЦП издателя сертификата открытого ключа подписи.

Рисунок 9. Диалог выбора сертификатов для построения цепочки для проверки ЭЦП издателя сертификата открытого ключа подписи

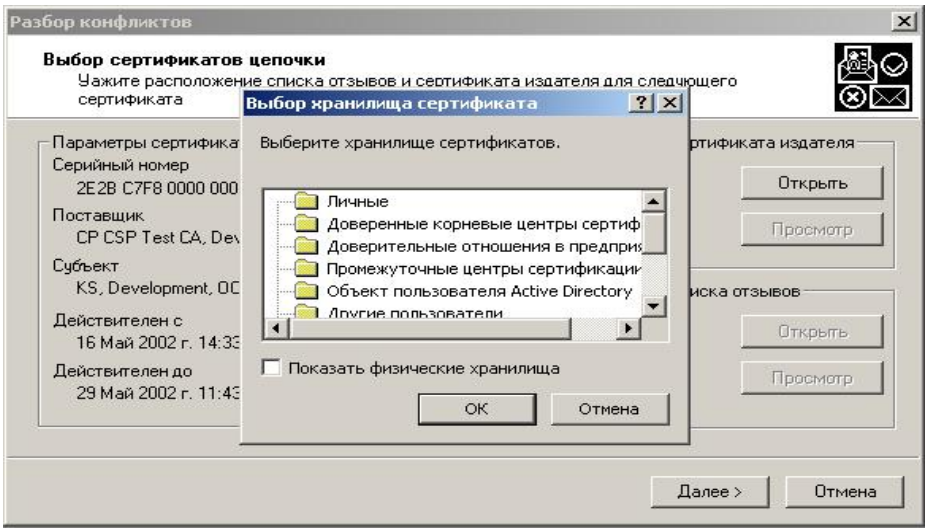


Сертификаты в цепочке перебираются последовательно, от того, которым было подписано, до корневого. Для каждого сертификата (кроме корневого) требуется указать соответствующий ему сертификат издателя и список отзыва сертификатов (CRL).

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

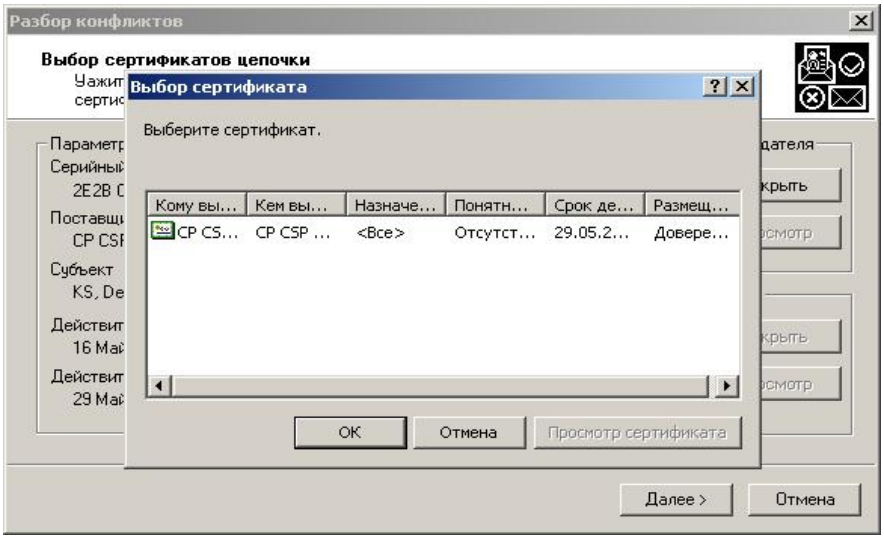
При выбранном пункте «*Хранилище*» при нажатии кнопки «**Открыть**» вначале появляется диалог выбора хранилища из всех хранилищ текущего пользователя.

Рисунок 10. Диалог выбора хранилища, где находится сертификат из цепочки



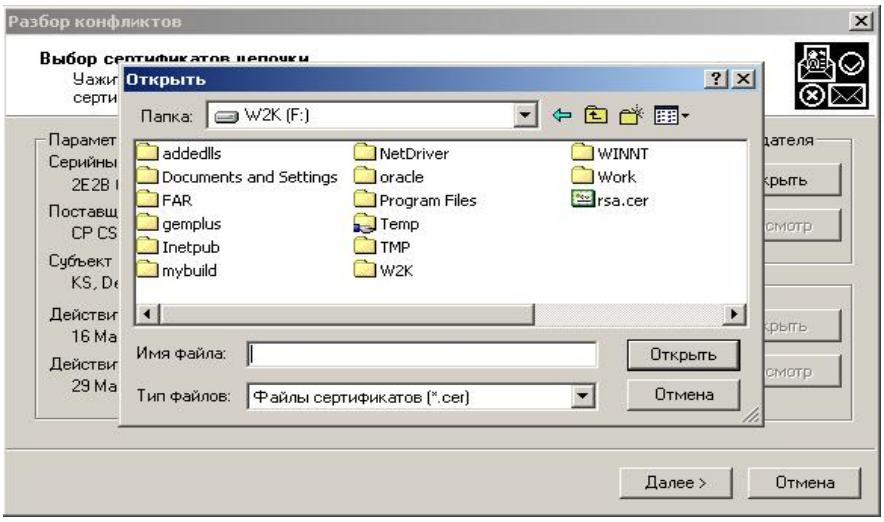
После выбора хранилища появляется диалог выбора сертификата из хранилища.

Рисунок 11. Диалог выбора сертификата для построения цепочки



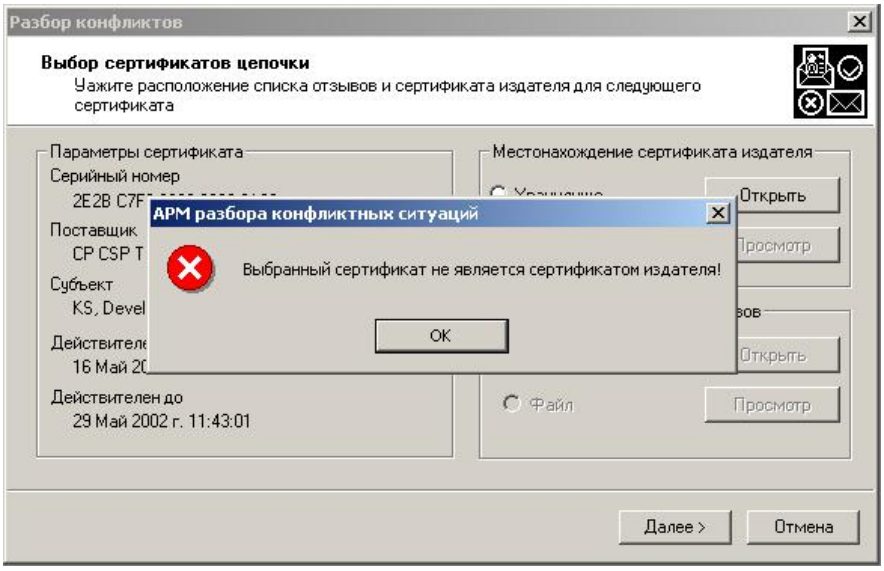
При выбранном пункте «*Файл*» появляется диалог открытия сертификата из файла.

Рисунок 12. Диалог открытия файла сертификата для построения цепочки



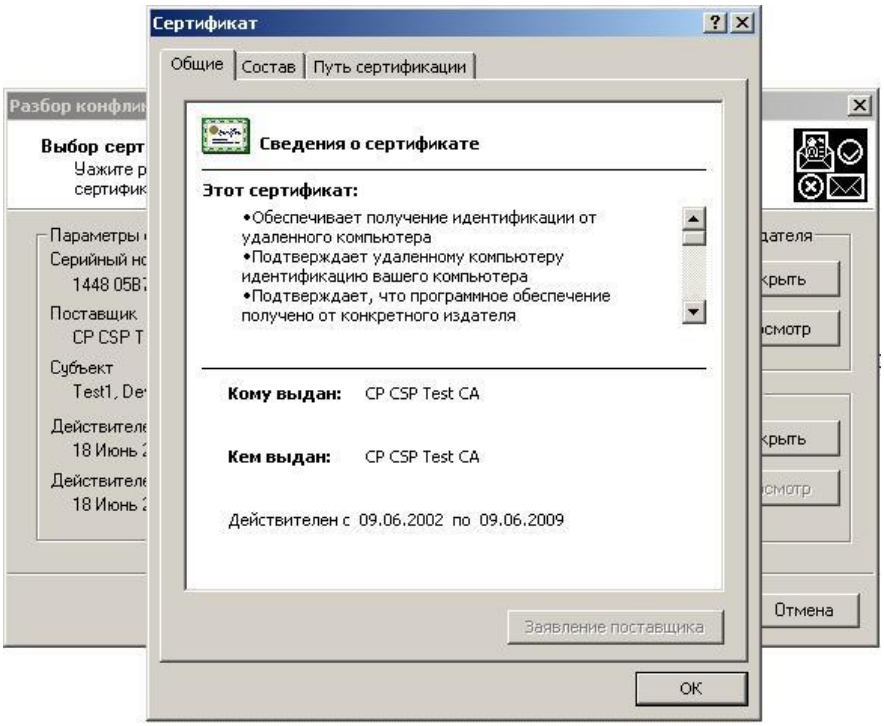
Если сертификат не является сертификатом издателя, то выводится сообщение об ошибке

Рисунок 13. Ошибка при чтении сертификата цепочки из файла



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

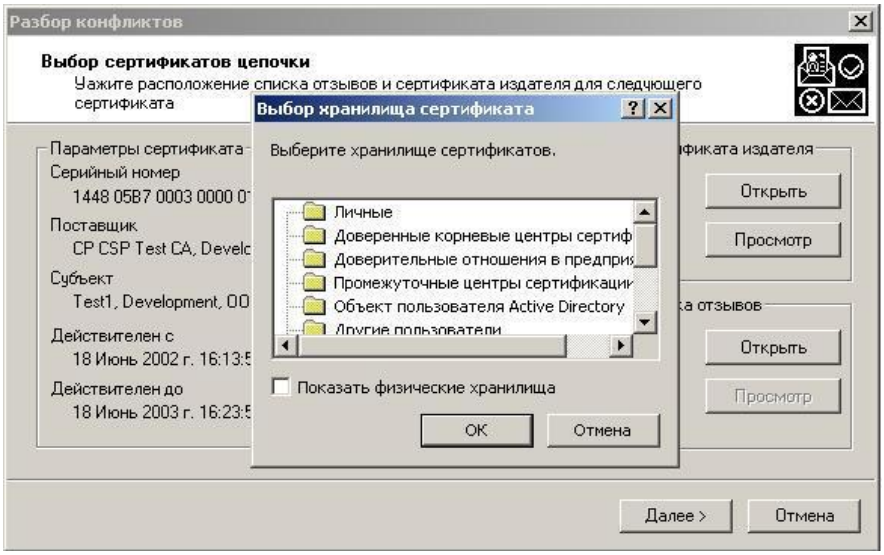
Рисунок 14. Окно просмотра выбранного сертификата для построения цепочки



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

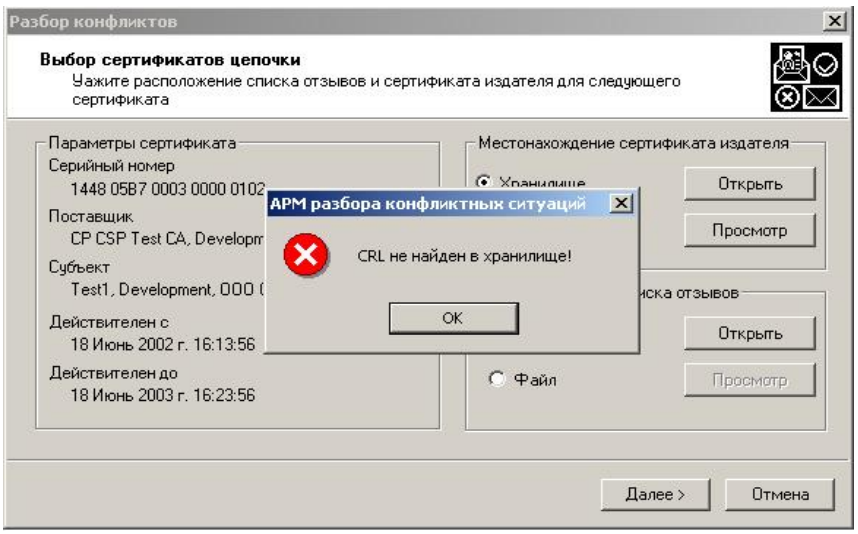
При выборе пункта «*Хранилище*» при нажатии кнопки «**Открыть**» появляется диалог выбора хранилища из всех хранилищ текущего пользователя.

Рисунок 15. Диалог выбора хранилища, где находится CRL



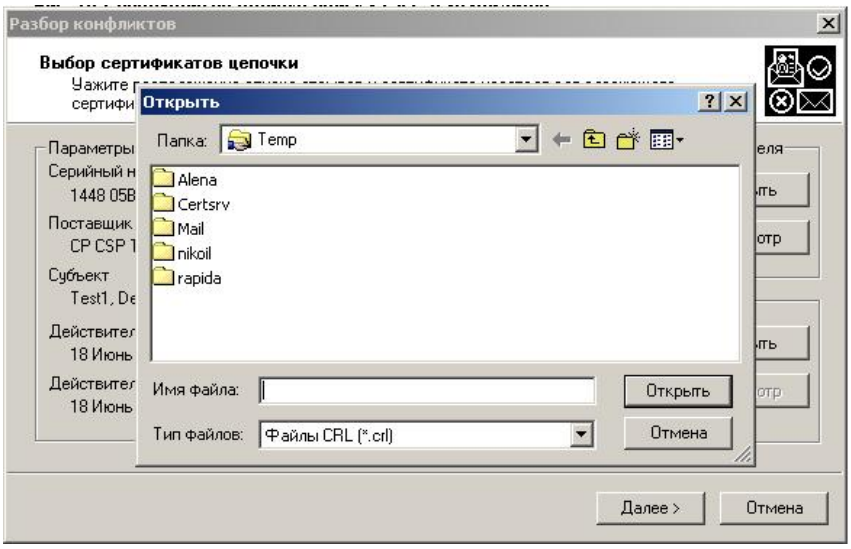
После выбора хранилища происходит автоматический поиск подходящего CRL в хранилище. Если таковой не найден, то выводится сообщение об ошибке.

Рисунок 16. Сообщение об ошибке поиска CRL в хранилище



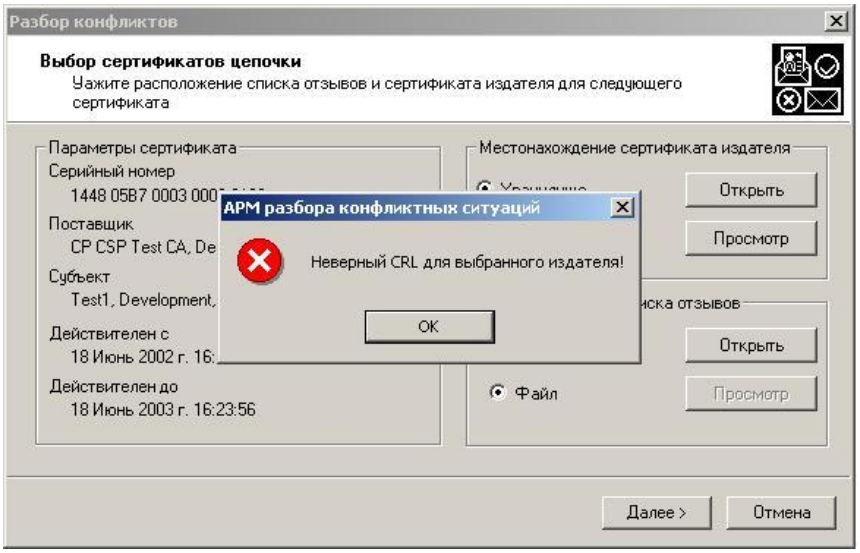
При выборе пункта «*Файл*» появляется диалог выбора файла, содержащего CRL.

Рисунок 17. Диалог открытия CRL из файла



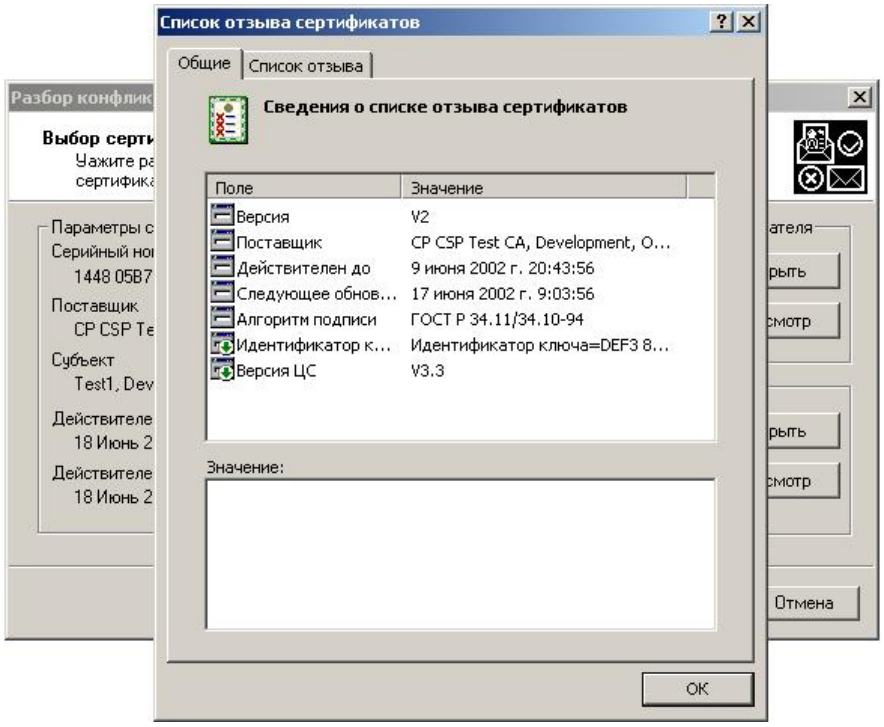
Если был выбран файл CRL, который не был издан выбранным центром, то возникнет сообщение об ошибке.

Рисунок 18. Ошибка несоответствия выбранного CRL



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

Рисунок 19. Окно просмотра выбранного CRL

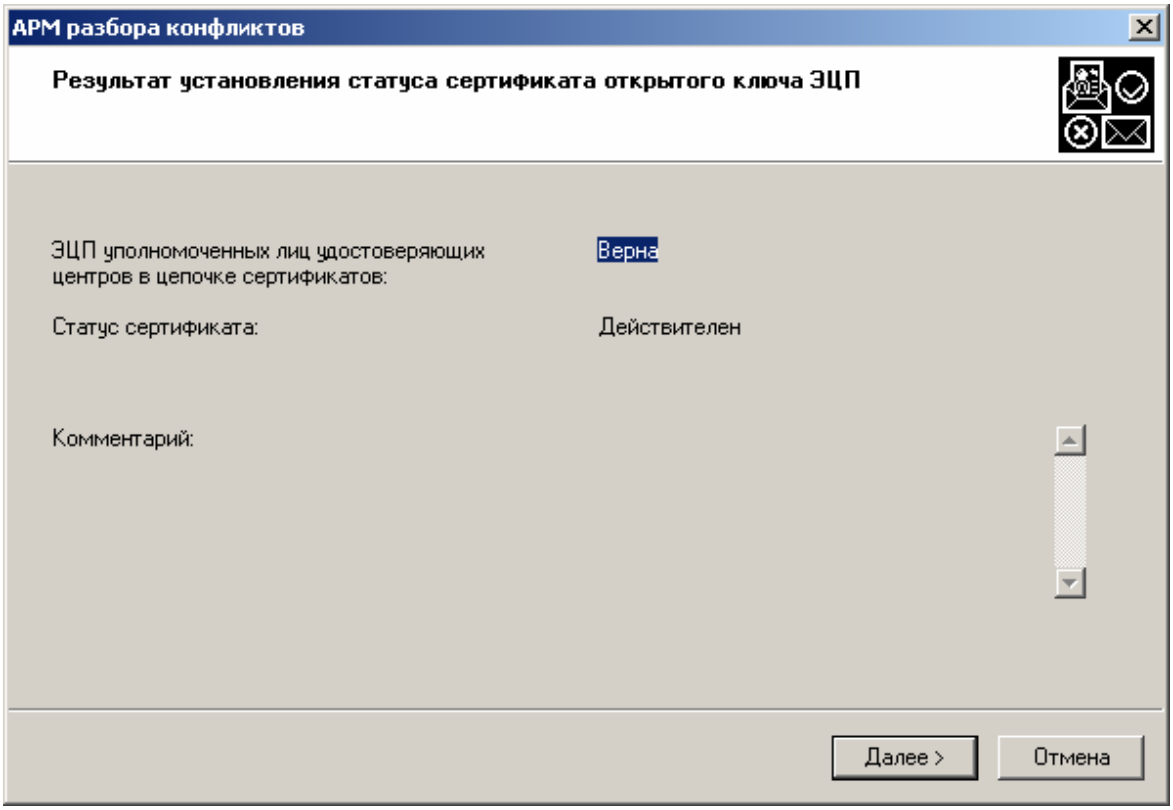


После нажатия кнопки «**Далее**» происходит переход к выбору сертификатов для проверки следующего сертификата в цепочке, либо, если в качестве сертификата издателя был указан сертификат корневого центра, переход к странице вывода результатов проверки ЭЦП издателя сертификата.

7.5. Вывод результатов проверки подписи издателя

На этой странице отображаются результаты проверки ЭЦП издателя сертификата открытого ключа. Выводится порядковый номер подписи, равный 1, результат подтверждения подлинности ЭЦП уполномоченных лиц в цепочке сертификатов и информация о статусе сертификата. В поле «*Комментарий*» выводятся все ошибки, возникшие при проверке сертификата.

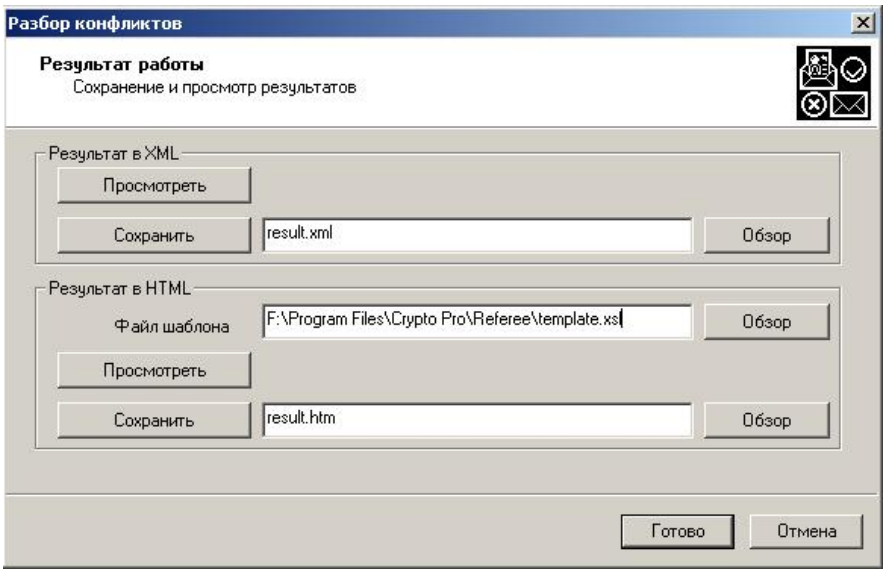
Рисунок 20. Страница вывода результатов проверки подписи издателя



После нажатия кнопки «**Далее**» происходит переход к странице выдачи результатов работы.

7.6. Результат работы мастера

Рисунок 21. 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.

8. Разбор конфликтной ситуации, связанной с проверкой ЭЦП электронного документа

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.

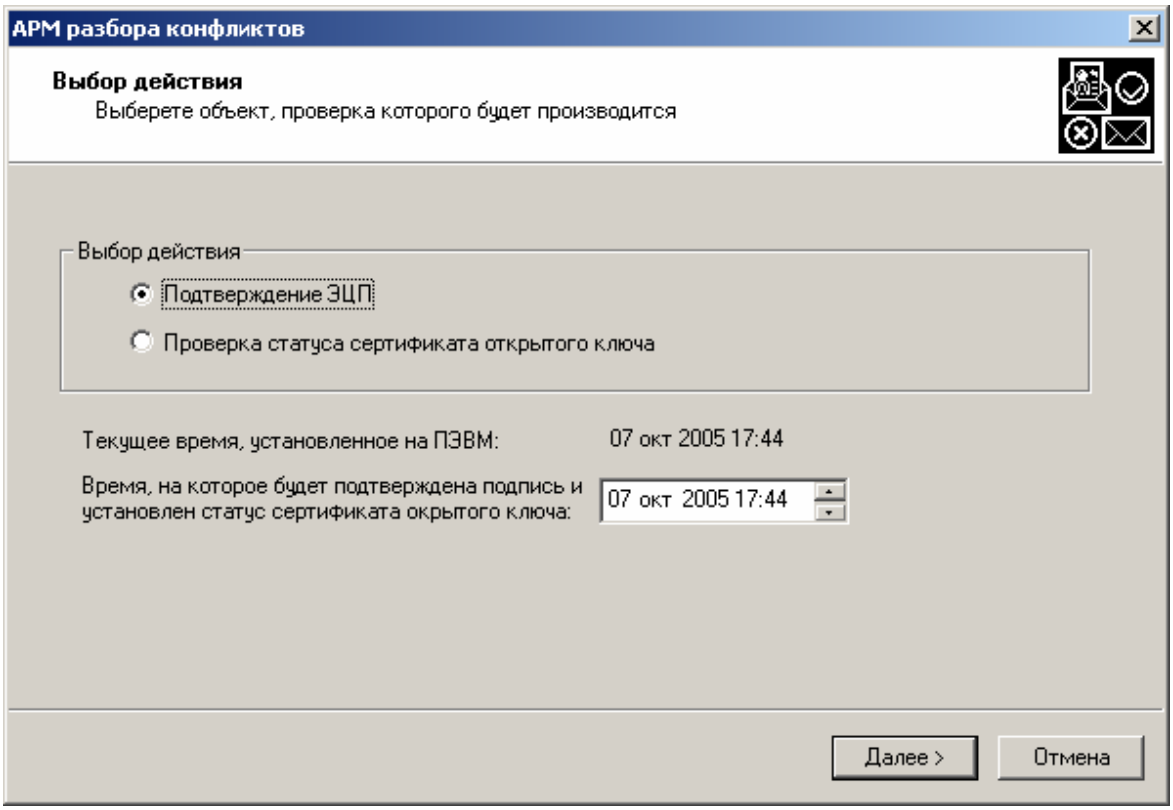
8.1. Стартовая страница мастера

При запуске программы выводится страница, содержащая краткую информацию о программе (см. Рисунок 1).

8.2. Выбор режима

В следующем окне выберите в качестве действия **Подтверждение ЭЦП** и задайте время, на момент наступления которого требуется подтвердить подлинность ЭЦП в электронном документе.

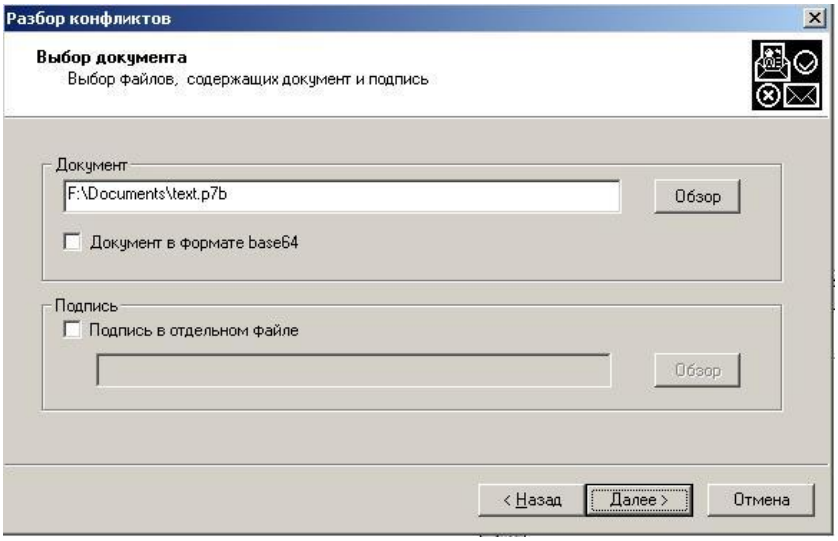
Рисунок 22. Выбор действия



8.3. Выбор электронного документа для проверки

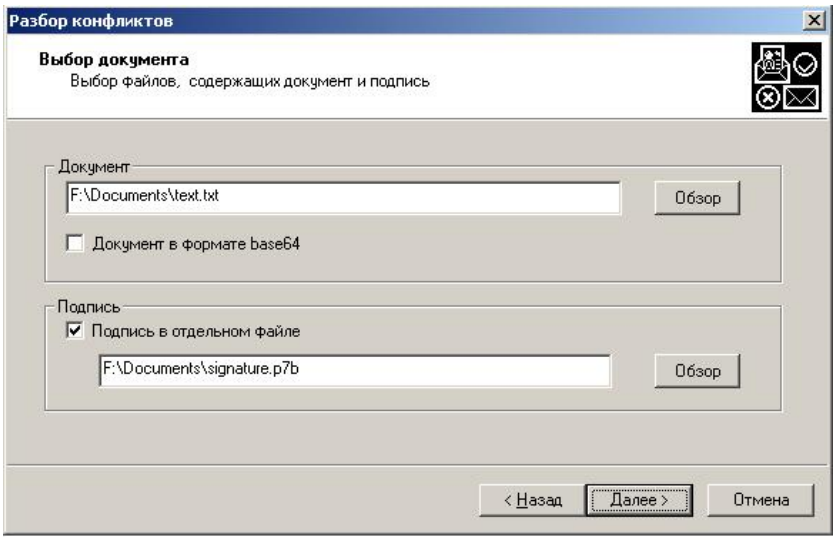
Для выполнения проверки ЭЦП необходимо выбрать файл, который содержит данные и ЭЦП этих данных в формате, определенном стандартом PKCS#7,

Рисунок 23. Диалог выбора файла данных



или два файла, один из которых содержит исходные данные, подписанные ЭЦП, а другой электронную цифровую подпись данных в формате, определенном стандартом PKCS#7 .

Рисунок 24. Диалог выбора файла данных и файла подписи

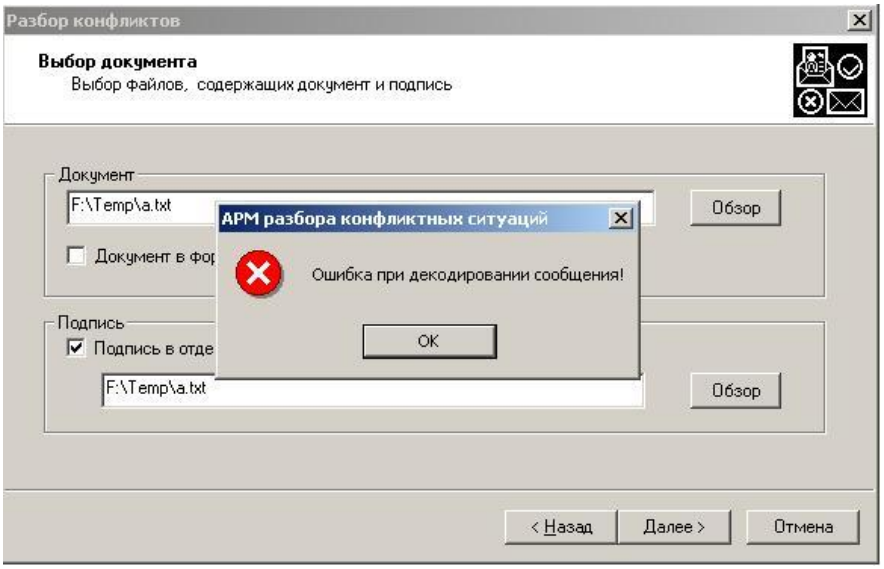


Документ может быть как в бинарном виде(DER), так и в кодировке base64. Для чтения документов в base64 необходимо установить соответствующий флаг.

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

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

Рисунок 25. Ошибка при выборе файла данных

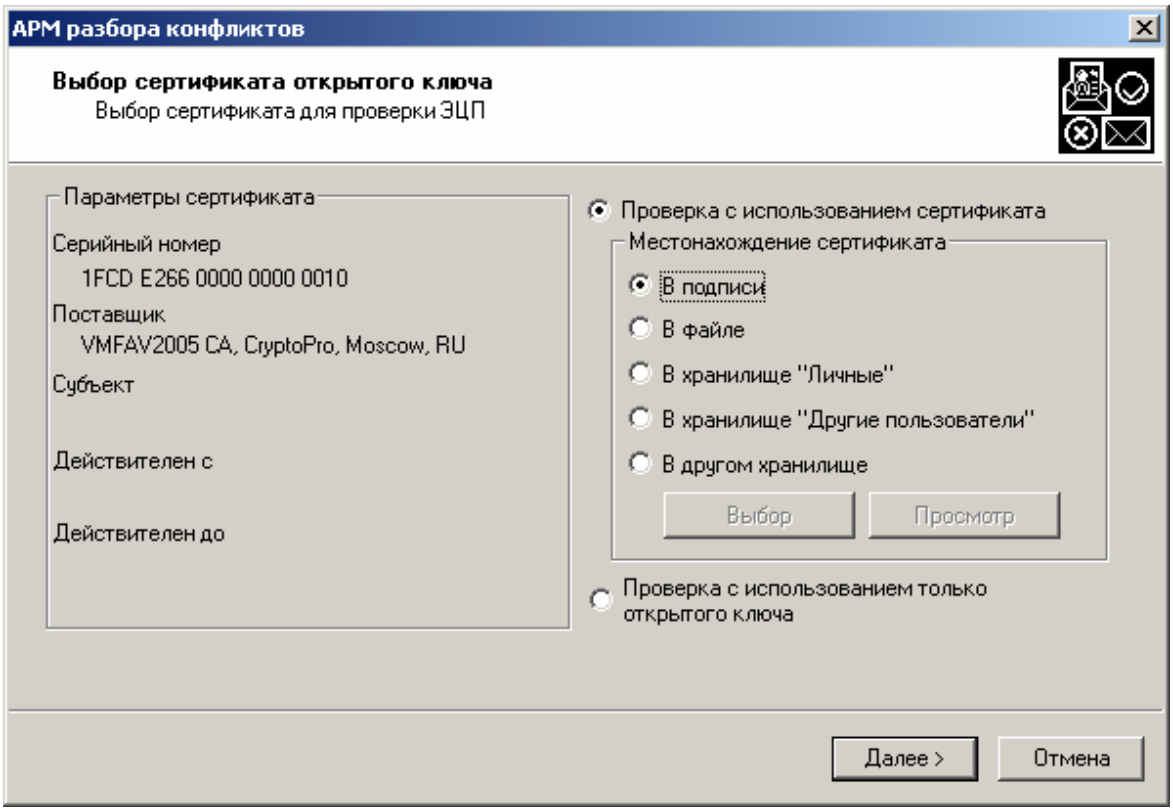


После этого начинается последовательная проверка подписей, которыми был подписан документ.

8.4. Выбор сертификата подписчика

Для криптографической проверки подписи необходимо выбрать сертификат, на котором будет проверяться подпись – переключатель **Проверка с использованием сертификата**, либо ввести открытый ключ, соответствующий сертификату подписавшего электронный документ лица, и указать параметры этого открытого ключа – переключатель **Проверка с использованием только открытого ключа**:

Рисунок 26. Выбор сертификата для проверки подписи



8.4.1. Подтверждение подлинности ЭЦП с использованием сертификата

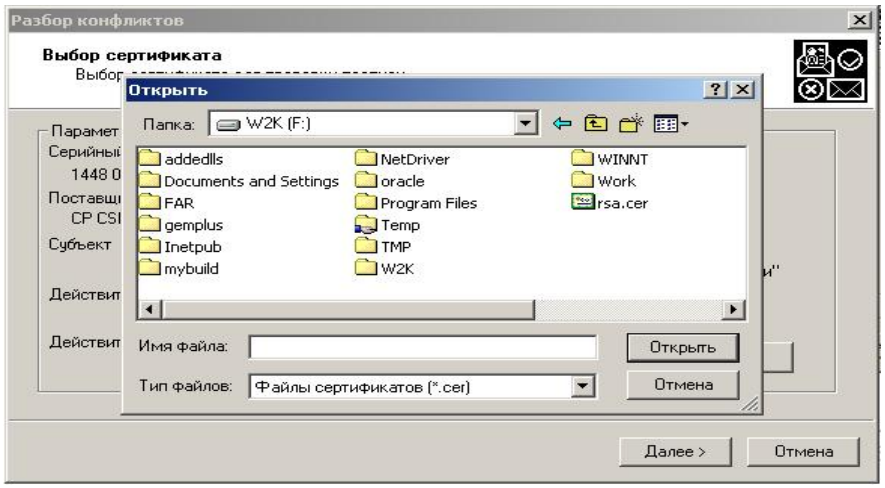
При подтверждении подлинности ЭЦП с использованием сертификата необходимо выбрать местонахождение сертификата:

- 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**».

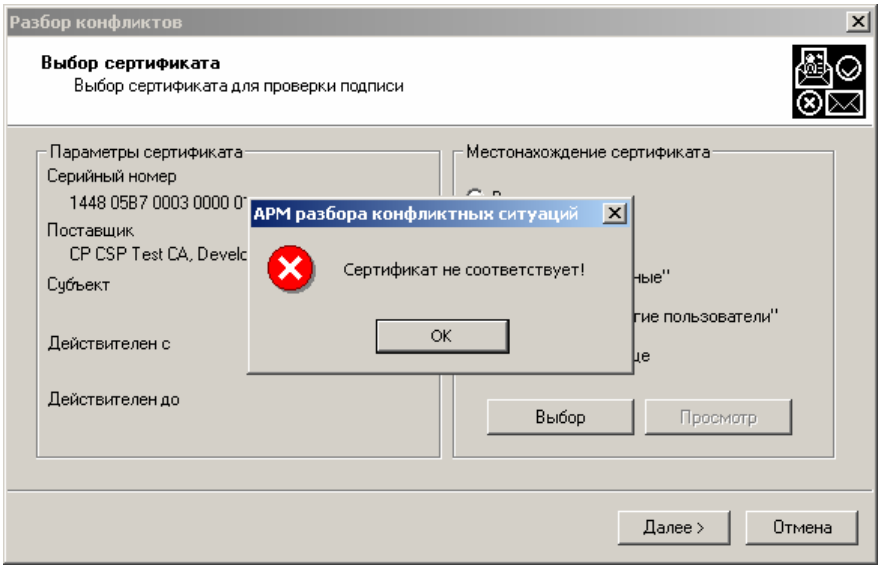
При выборе пункта «*В файле*» появится диалог открытия файла.

Рисунок 27. Выбор сертификата для проверки из файла



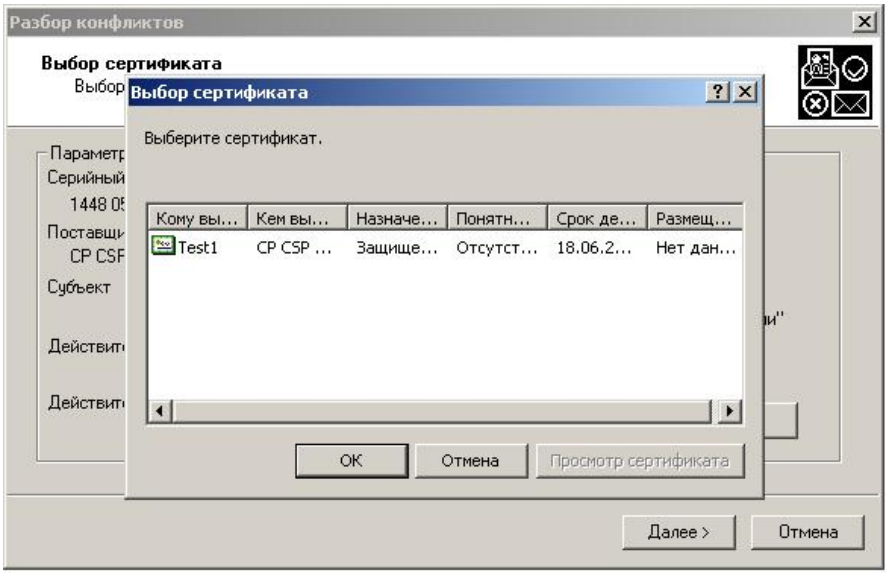
Если выбран файл с сертификатом, не соответствующим тому, которым было подписано сообщение (несовпадение серийного номера или издателя), то появится сообщение об ошибке.

Рисунок 28. Ошибка при выборе сертификата для проверки



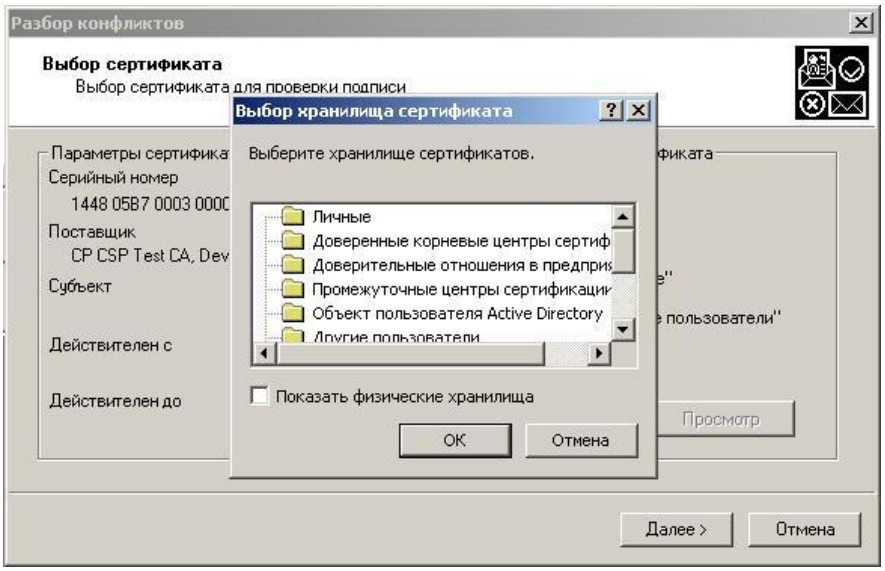
Если выбраны пункты «*В хранилище «Личные»* или «*В хранилище «Другие пользователи»*, то при нажатии кнопки «**Выбор**» появится окно диалога выбора файла из соответствующего хранилища.

Рисунок 29. Выбор сертификат для проверки из хранилища



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

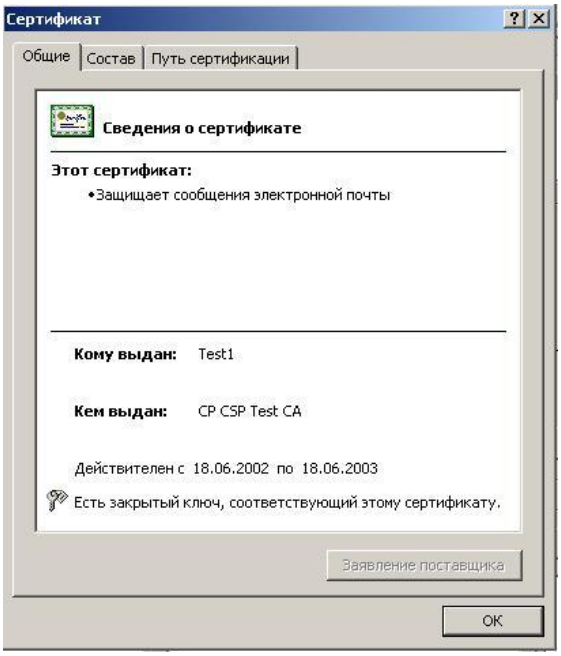
Рисунок 30. Выбор хранилища, где находится сертификат для проверки



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

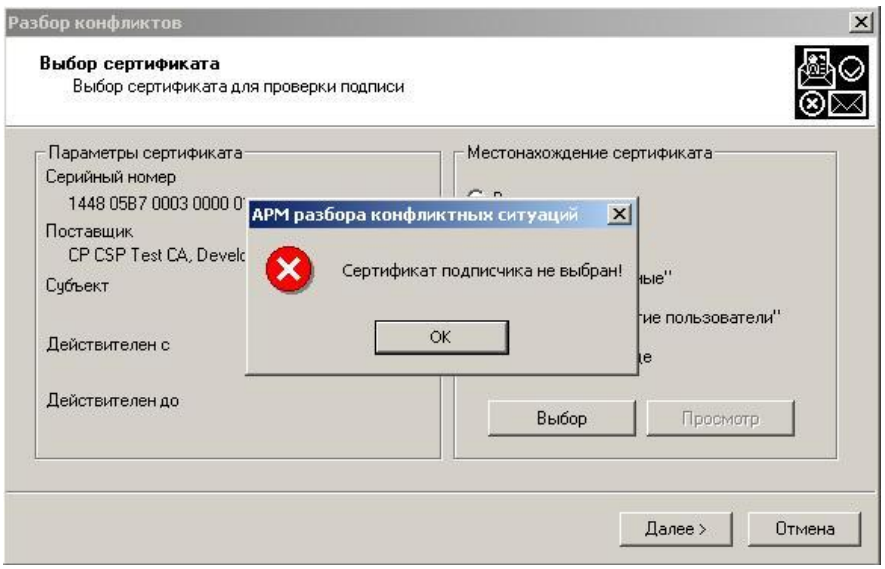
Кнопка «**Просмотр**» выводит окно просмотра выбранного сертификата.

Рисунок 31. Просмотр сертификата для проверки



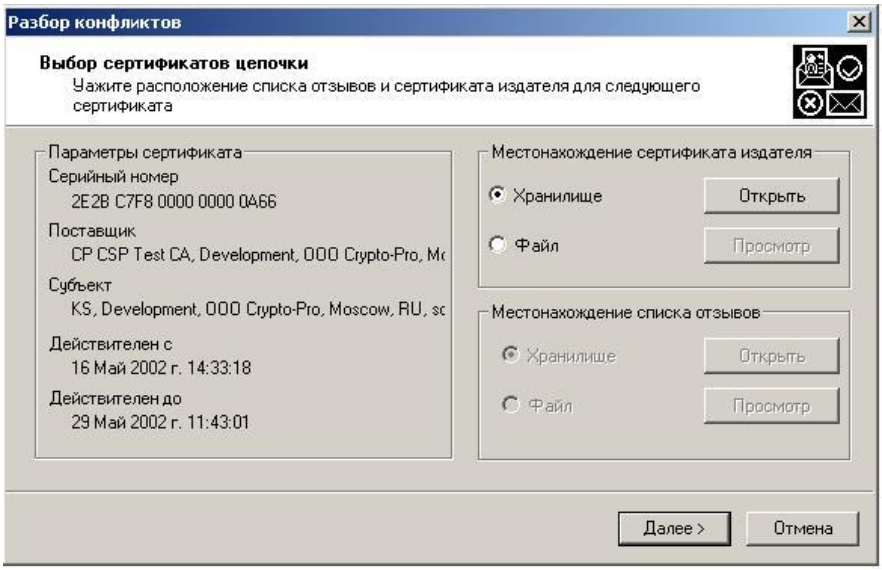
Если на данном шаге мастера по какой-то причине сертификат не был выбран, то переход к следующему шагу невозможен – возникнет сообщение об ошибке!

Рисунок 32. Сообщение об ошибке при выборе сертификата для проверки



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

Рисунок 33. Диалог выбора сертификатов для построения цепочки для проверки сертификата подписи

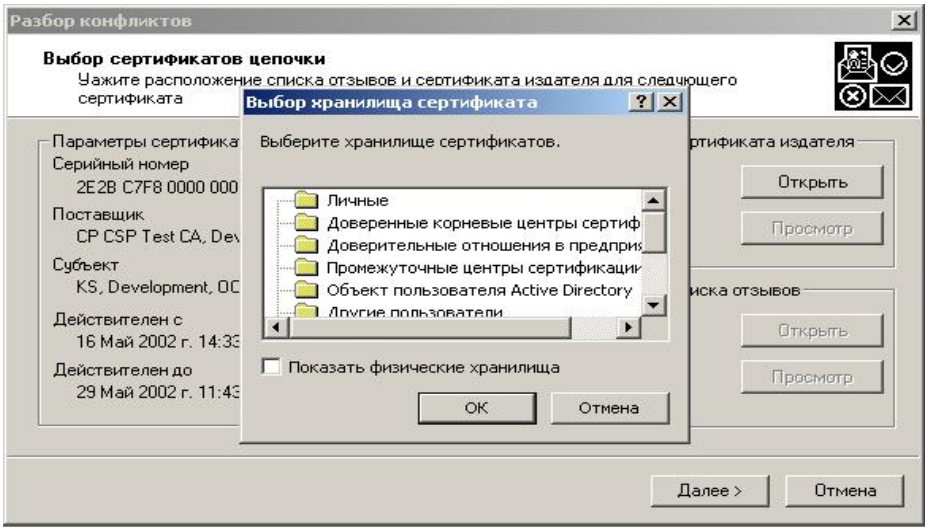


Сертификаты в цепочке перебираются последовательно, от того, которым было подписано, до корневого. Для каждого сертификата (кроме корневого) требуется указать соответствующий ему сертификат издателя и список отзыва сертификатов (CRL).

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

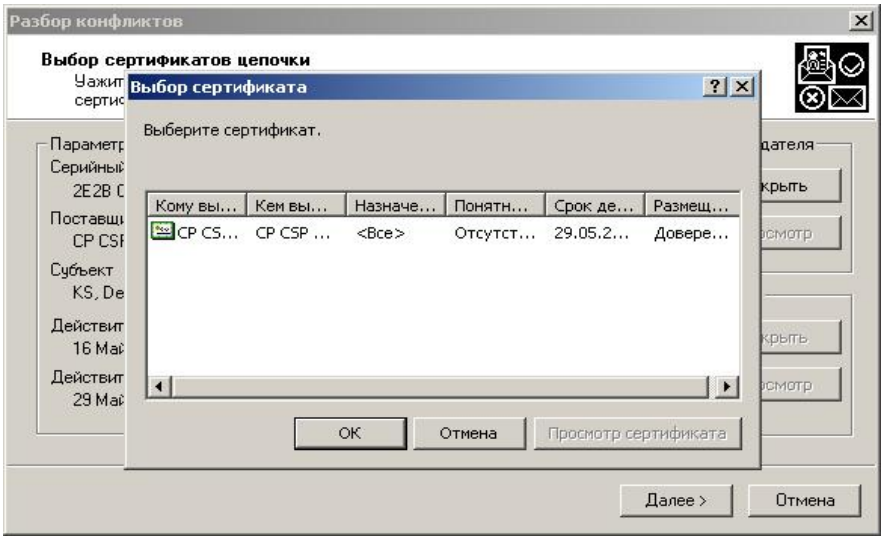
При выбранном пункте «*Хранилище*» при нажатии кнопки «**Открыть**» вначале появляется диалог выбора хранилища из всех хранилищ текущего пользователя.

Рисунок 34. Диалог выбора хранилища, где находится сертификат из цепочки



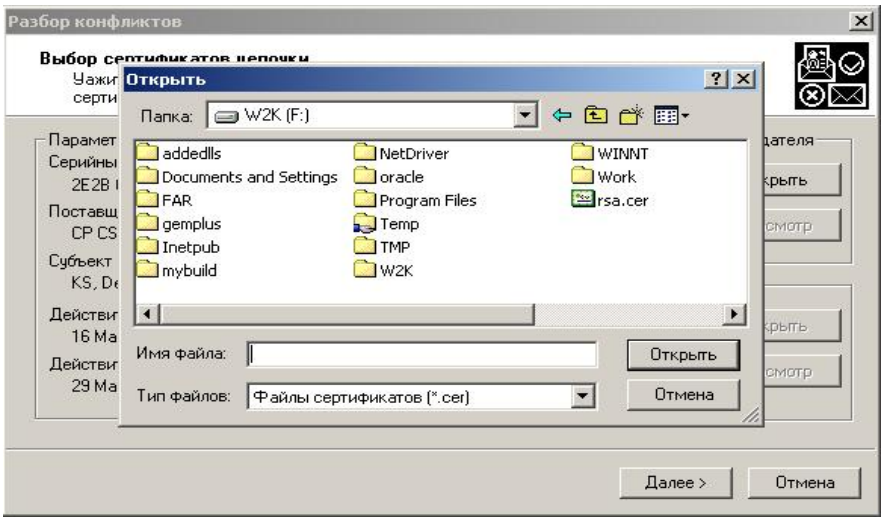
После выбора хранилища появляется диалог выбора сертификата из хранилища.

Рисунок 35. Диалог выбора сертификата для построения цепочки



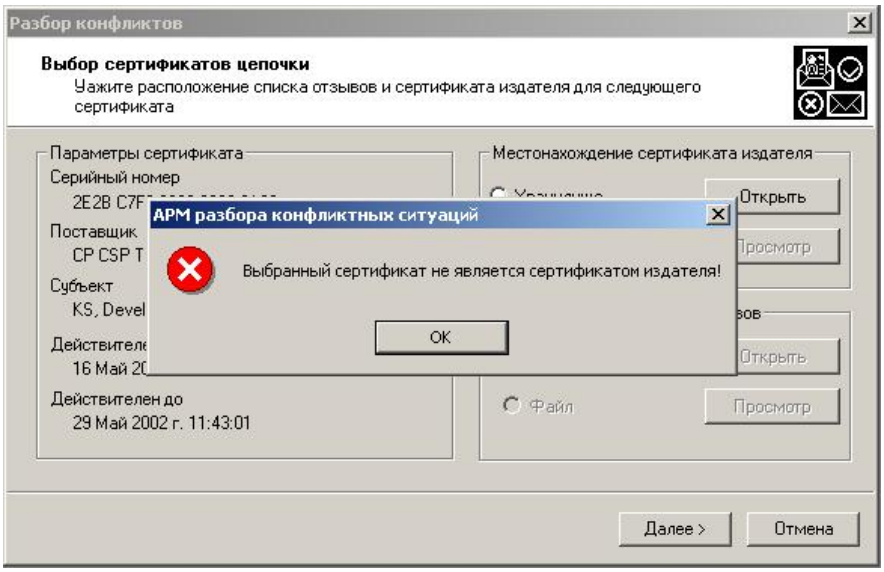
При выбранном пункте «*Файл*» появляется диалог открытия сертификата из файла.

Рисунок 36. Диалог открытия файла сертификата для построения цепочки



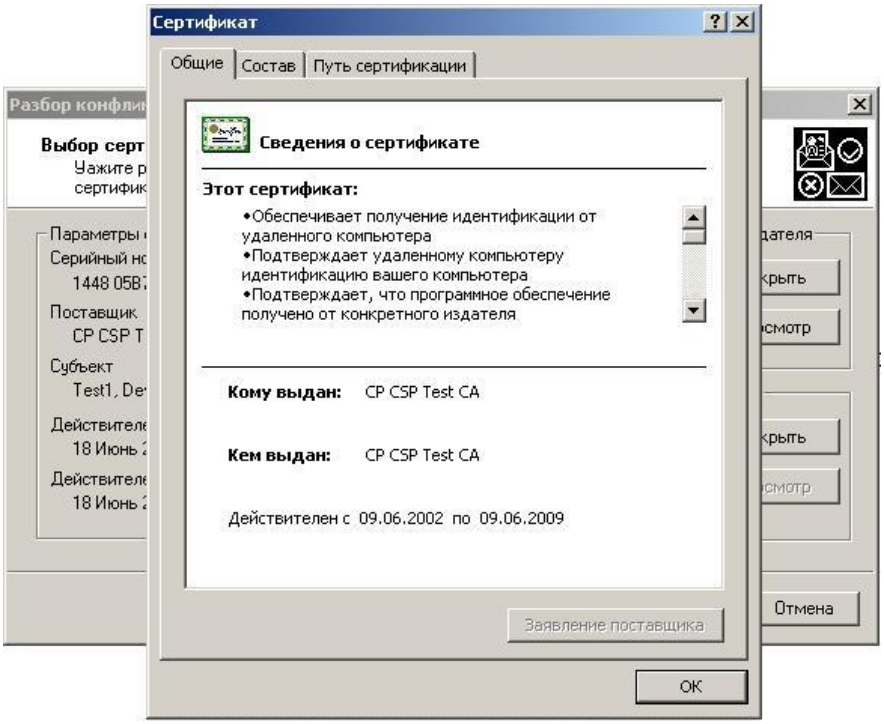
Если сертификат не является сертификатом издателя, то выводится сообщение об ошибке

Рисунок 37. Ошибка при чтении сертификата цепочки из файла



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

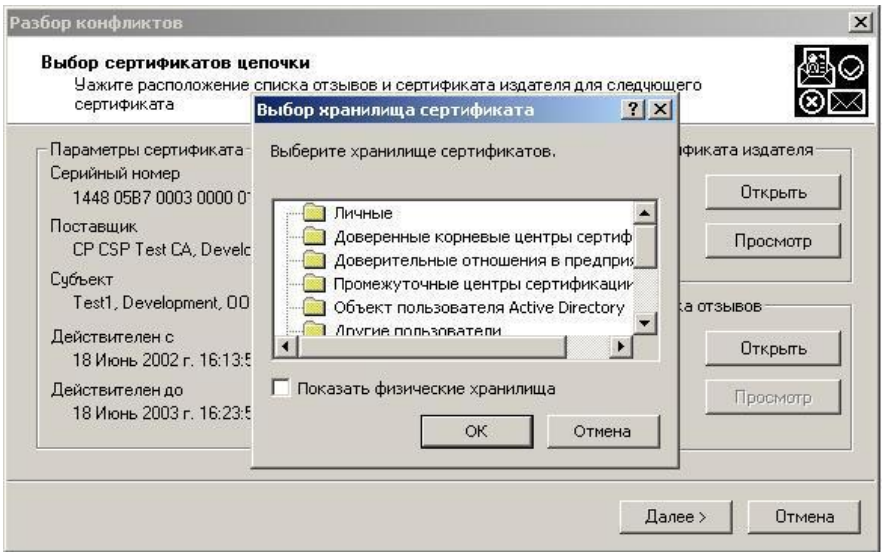
Рисунок 38. Окно просмотра выбранного сертификата для построения цепочки



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

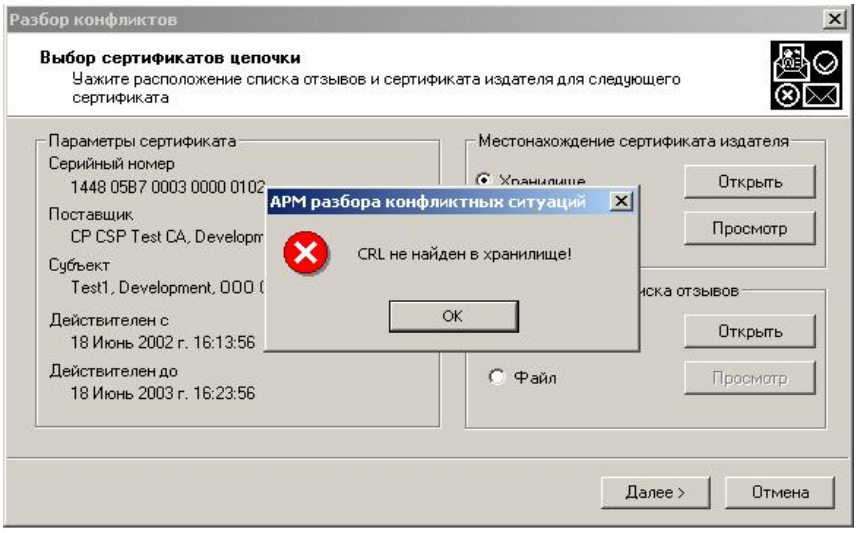
При выборе пункта «*Хранилище*» при нажатии кнопки «**Открыть**» появляется диалог выбора хранилища из всех хранилищ текущего пользователя.

Рисунок 39. Диалог выбора хранилища, где находится CRL



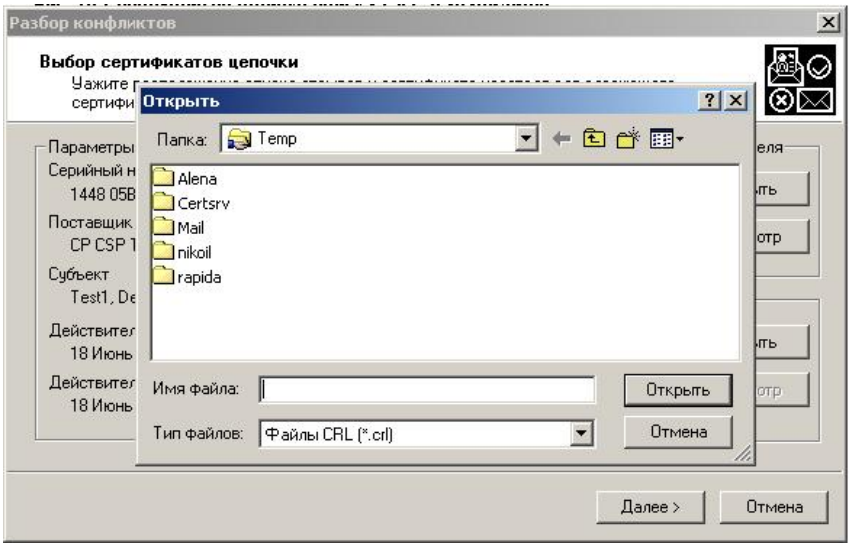
После выбора хранилища происходит автоматический поиск подходящего CRL в хранилище. Если таковой не найден, то выводится сообщение об ошибке

Рисунок 40. Сообщение об ошибке поиска CRL в хранилище



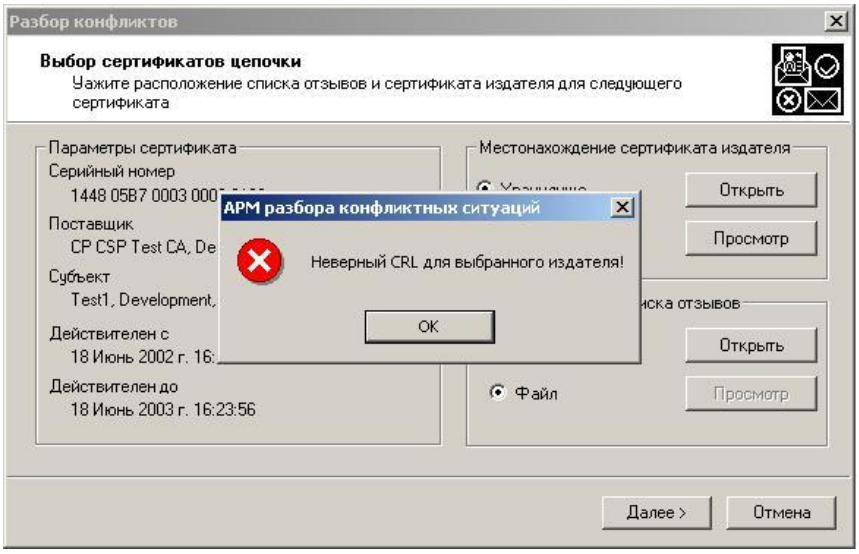
При выборе пункта «*Файл*» появляется диалог выбора файла, содержащего CRL.

Рисунок 41. Диалог открытия CRL из файла



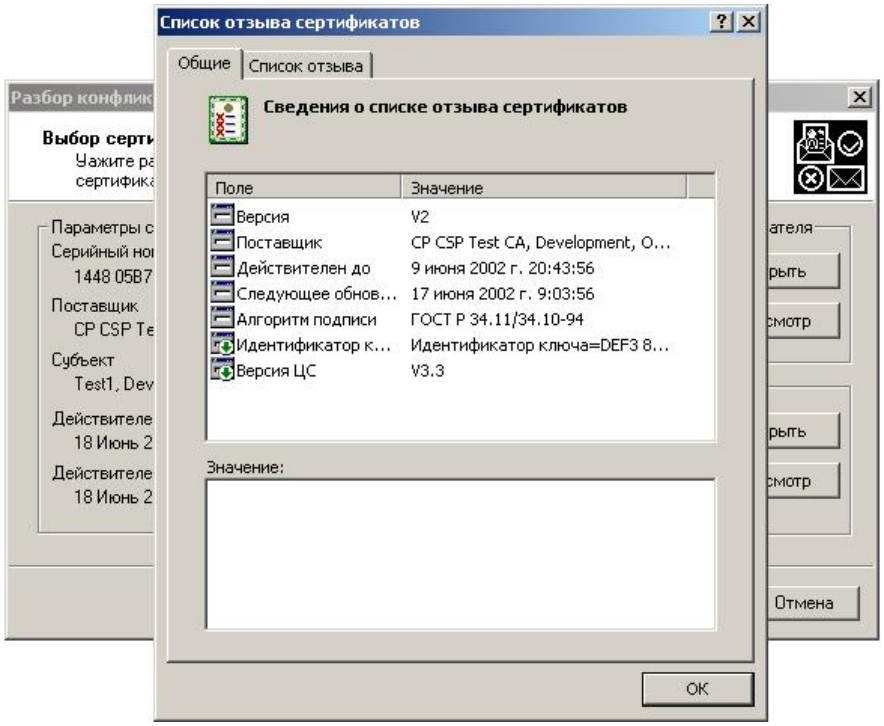
Если был выбран файл CRL, который не был издан выбранным центром, то возникнет сообщение об ошибке.

Рисунок 42. Ошибка несоответствия выбранного CRL



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

Рисунок 43. Окно просмотра выбранного CRL



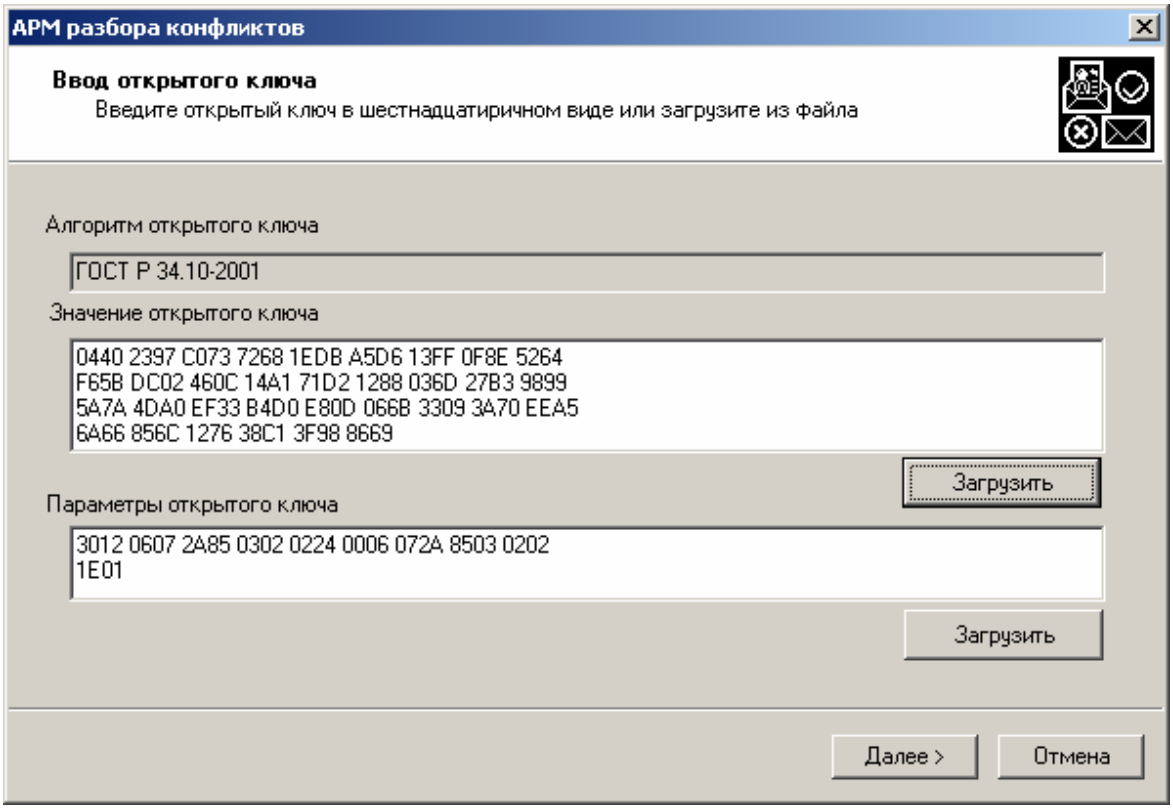
После нажатия кнопки «**Далее**» происходит переход к выбору сертификатов для проверки следующего сертификата в цепочке, либо, если в качестве сертификата издателя был указан сертификат корневого центра, переход к странице вывода результатов проверки подписи и сертификата.

8.4.2. Подтверждение подлинности ЭЦП с использованием только открытого ключа

При проверке с использованием только открытого ключа необходимо указать значение открытого ключа и параметры открытого ключа. Загрузка данных параметров может быть выполнена вручную из сертификата на бумажном носителе, либо посредством нажатия кнопок **Загрузить** из соответствующих файлов.

После установки необходимых параметров нажмите кнопку **Далее** для просмотра результата проверки ЭЦП.

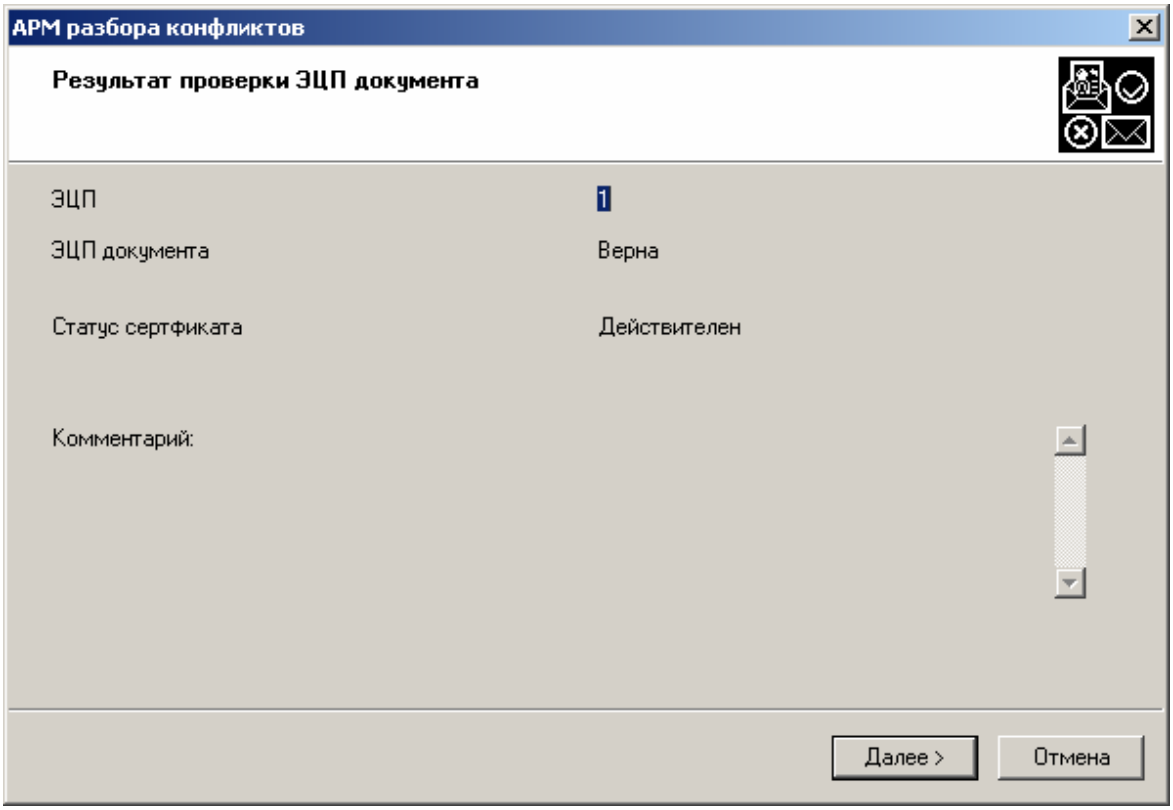
Рисунок 44. Окно ввода открытого ключа для подтверждения подлинности ЭЦП



8.5. 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.

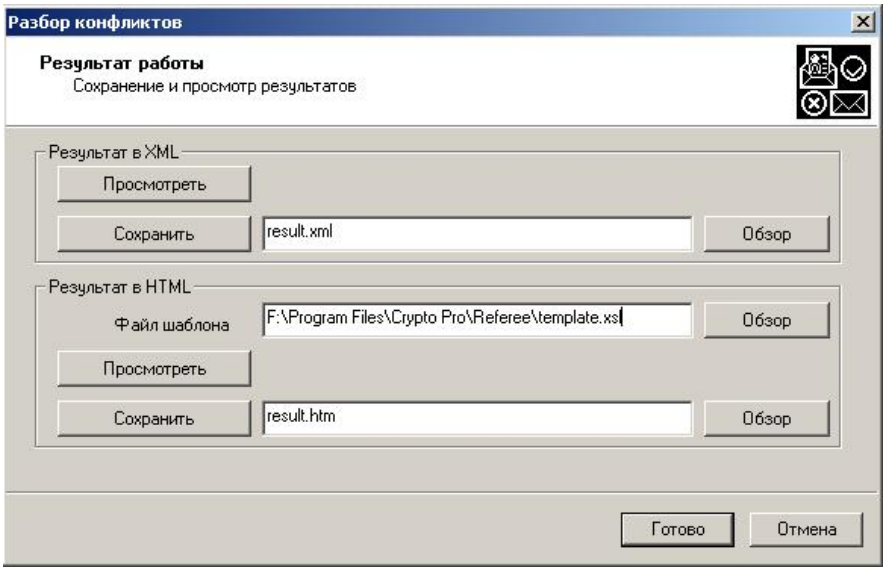
Рисунок 45. Страница вывода результатов проверки подписи



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.

8.6. Результат работы мастера

Рисунок 46. 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.

9. Удаление программного обеспечения АРМ разбора конфликтных ситуаций

Удаление программного обеспечения АРМ разбора конфликтных ситуаций осуществляется в следующем порядке:

1. Удаление компоненты «КриптоПро УЦ – АРМ разбора конфликтных ситуаций»;
2. Удаление сертификата Центра сертификации (уполномоченного лица удостоверяющего центра) из соответствующего хранилища доверенных сертификатов центров сертификации – выполняется в том случае, если в дальнейшем нет необходимости применения данного сертификата для построения цепочки сертификатов пользователей удостоверяющего центра на компьютере АРМ разбора конфликтных ситуаций.
3. Удаление СКЗИ КриптоПро CSP – выполняется в том случае, если в дальнейшем на компьютере АРМ разбора конфликтных ситуаций отсутствует необходимость использования СКЗИ.

Удаление компоненты «КриптоПро УЦ – АРМ разбора конфликтных ситуаций» и СКЗИ «КриптоПро CSP» осуществляется с использованием сервиса **Установка и удаления программ**, запускающегося из **Панели управления компьютера**. Для удаления необходимой компоненты, выделите ее левой кнопкой мыши и нажмите на кнопку **Удалить**.

Удаление сертификата Центра сертификации (уполномоченного лица удостоверяющего центра) из хранилища сертификатов **Локальный компьютер/Доверенные корневые центры сертификации** (если удостоверяющий центр – корневой), либо **Локальный компьютер/Промежуточные центры сертификации** (если удостоверяющий центр – подчиненный) осуществляется с использованием интерфейса консоли **mmc** и изолированной оснастки **Сертификаты**.

10. Перечень рисунков

Рисунок 1. Стартовая страница 11
Рисунок 2. Выбор действия 12
Рисунок 3. Выбор сертификата для проверки подписи 12
Рисунок 4. Выбор сертификата для проверки из файла 13
Рисунок 5. Выбор сертификат для проверки из хранилища 13
Рисунок 6. Выбор хранилища, где находится сертификат для проверки 14
Рисунок 7. Просмотр сертификата для проверки 14
Рисунок 8. Сообщение об ошибке при выборе сертификата для проверки 15
Рисунок 9. Диалог выбора сертификатов для построения цепочки для проверки ЭЦП издателя сертификата открытого ключа подписи 15
Рисунок 10. Диалог выбора хранилища, где находится сертификат из цепочки 16
Рисунок 11. Диалог выбора сертификата для построения цепочки 16
Рисунок 12. Диалог открытия файла сертификата для построения цепочки 16
Рисунок 13. Ошибка при чтении сертификата цепочки из файла 17
Рисунок 14. Окно просмотра выбранного сертификата для построения цепочки 17
Рисунок 15. Диалог выбора хранилища, где находится CRL 18
Рисунок 16. Сообщение об ошибке поиска CRL в хранилище 18
Рисунок 17. Диалог открытия CRL из файла 18
Рисунок 18. Ошибка несоответствия выбранного CRL 19
Рисунок 19. Окно просмотра выбранного CRL 19
Рисунок 20. Страница вывода результатов проверки подписи издателя 20
Рисунок 21. Страница просмотра и сохранения результатов работы мастера 20
Рисунок 22. Выбор действия 21
Рисунок 23. Диалог выбора файла данных 22
Рисунок 24. Диалог выбора файла данных и файла подписи 22
Рисунок 25. Ошибка при выборе файла данных 23
Рисунок 26. Выбор сертификата для проверки подписи 23
Рисунок 27. Выбор сертификата для проверки из файла 24
Рисунок 28. Ошибка при выборе сертификата для проверки 24
Рисунок 29. Выбор сертификат для проверки из хранилища 25
Рисунок 30. Выбор хранилища, где находится сертификат для проверки 25
Рисунок 31. Просмотр сертификата для проверки 26
Рисунок 32. Сообщение об ошибке при выборе сертификата для проверки 26
Рисунок 33. Диалог выбора сертификатов для построения цепочки для проверки сертификата подписи 27
Рисунок 34. Диалог выбора хранилища, где находится сертификат из цепочки 27
Рисунок 35. Диалог выбора сертификата для построения цепочки 28
Рисунок 36. Диалог открытия файла сертификата для построения цепочки 28

Рисунок 37. Ошибка при чтении сертификата цепочки из файла 28
Рисунок 38. Окно просмотра выбранного сертификата для построения цепочки 29
Рисунок 39. Диалог выбора хранилища, где находится CRL 29
Рисунок 40. Сообщение об ошибке поиска CRL в хранилище..... 30
Рисунок 41. Диалог открытия CRL из файла..... 30
Рисунок 42. Ошибка несоответствия выбранного CRL 30
Рисунок 43. Окно просмотра выбранного CRL 31
Рисунок 44. Окно ввода открытого ключа для подтверждения подлинности ЭЦП 32
Рисунок 45. Страница вывода результатов проверки подписи 33
Рисунок 46. Страница просмотра и сохранения результатов работы мастера 33

11. Приложения

11.1. Приложение 1. 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>
```

11.2. Приложение 2. Пример протокола проверки ЭЦП в формате HTML

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