Средство
Криптографической
Защиты
Информации

КриптоПро CSP (версия 2.0)

Содержание

Введение

Данный документ является кратким руководством по установке и регистрации средства криптографической защиты информации (СКЗИ) КриптоПро CSP. Полная информация по установке и работе с КриптоПро CSP находится на CD-ROM "КриптоПро CSP" (директория "**\DOC**").

Полный комплект эксплуатационной документации и описание использования КриптоПро CSP в различных системах Microsoft можно найти на сервере http://www.cryptopro.ru/CryptoPro/product6.html.

Краткое описание

КриптоПро CSP разработано в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

КриптоПро CSP реализует российские криптографические алгоритмы:

- ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования".
- ГОСТ Р 34.10-94 "Информационная технология. Криптографическая защита информации. Система электронной цифровой подписи на базе асимметричного криптографического алгоритма".
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".
- ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".

Требования к системе

Программное обеспечение СКЗИ КриптоПро CSP предназначено для использования в операционных системах Windows 95/98/ME/NT 4.0/2000/XP и Solaris.

Приведенная в данном документе информация относится только к платформе Windows.

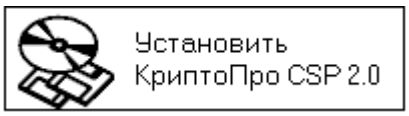
Установка дистрибутива ПО СКЗИ КриптоПро CSP

Установка дистрибутива должна производится пользователем, имеющим права администратора. Перед установкой дистрибутива КриптоПро CSP, удалите все ранее существующие версии устанавливаемого программного обеспечения. Если модуль криптографической поддержки не удален, новая версия не будет установлена. Для этого используете пункты основного меню Windows **Пуск, Настройка, Панель управления, Установка и удаление программ**.

Для установки программного обеспечения вставьте компакт-диск в привод считывателя. Программа установки запуститься автоматически (см. Рисунок 1). Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** с компакт-диска.

Рисунок 1. Содержание диска КриптоПро CSP

Для дальнейшей установки КриптоПро CSP, выберите значок **Установить КриптоПро CSP 2.0**.



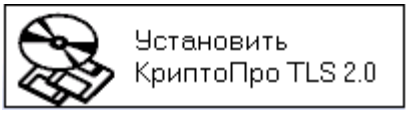
Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Установка КриптоПро TLS

Кроме СКЗИ КриптоПро CSP на компакт-диске содержится дистрибутив программного обеспечения, реализующего протокол TLS (Transport Layer Security). Протокол TLS (RFC 2246) является дальнейшим развитием протокола SSL (Secure Socket Layer) и широко используется в сети Internet для защиты соединений в клиент-серверных технологиях.

Программное обеспечение КриптоПро TLS является реализацией протокола TLS и использует криптографические функции КриптоПро CSP для обеспечения процесса аутентификации и шифрования трафика между клиентом и сервером.

Для установки программного обеспечения КриптоПро TLS с компакт-диска (см. Рисунок 1) выберите значок **Установить КриптоПро TLS 2.0**

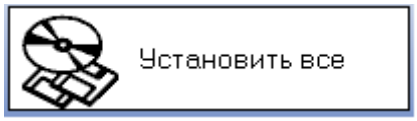


Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Установка СКЗИ КриптоПро CSP и КриптоПро TLS

Программа установки обеспечивает дополнительный режим установки, так называемый режим **установить все**. Это режим позволяет обеспечить последовательную установку ПО СКЗИ КриптоПро CSP и КриптоПро TLS без перезагрузок компьютера после установки каждой компоненты.

Для установки программного обеспечения СКЗИ КриптоПро CSP и КриптоПро TLS с компакт-диска (см. Рисунок 1) выберите значок **Установить все**

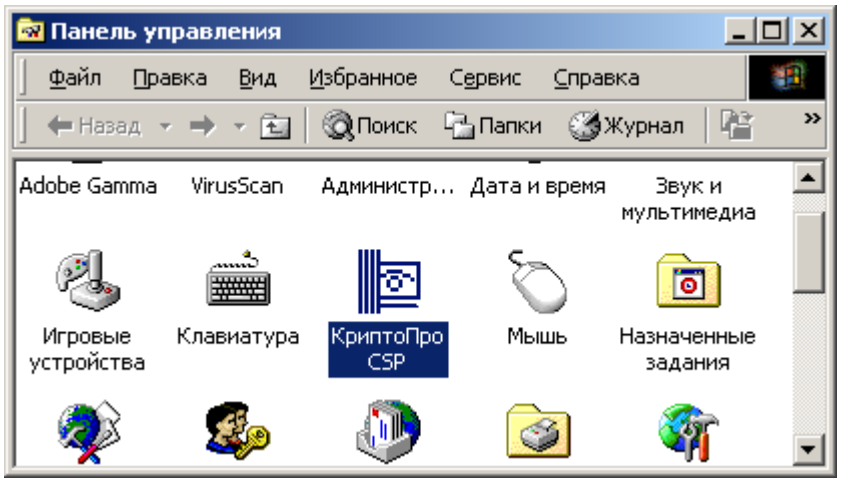


Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Изменение набора устройств хранения ключевой информации

Программа установки по умолчанию устанавливает все модули, обеспечивающие работу с различными поддерживаемыми устройствами хранения ключевой информации, но при этом настойки КриптоПро CSP допускают использовать в качестве ключевого носителя только дискету 3,5". Если для работы с КриптоПро CSP необходимы дополнительные типы устройств работы с ключевыми носителями, выберите режим изменения их состава.

Рисунок 2. Панель управления



Для этого откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления (см. Рисунок 2) выберите значок **КриптоПро CSP**. В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 3) выберите закладку **Оборудование** и, нажав кнопку **Настроить считыватели/Configure carriers**, добавьте (или удалите) из списка те устройства, которые будут использованы в качестве считывателей ключевой информации (см. Рисунок 4).

Рисунок 3. Панель настройки

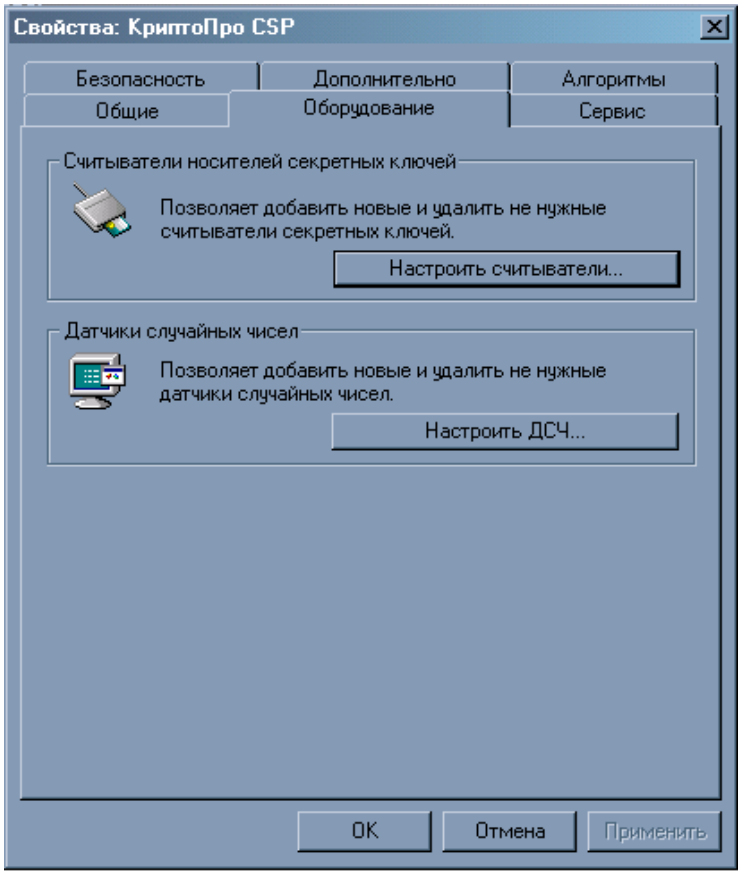
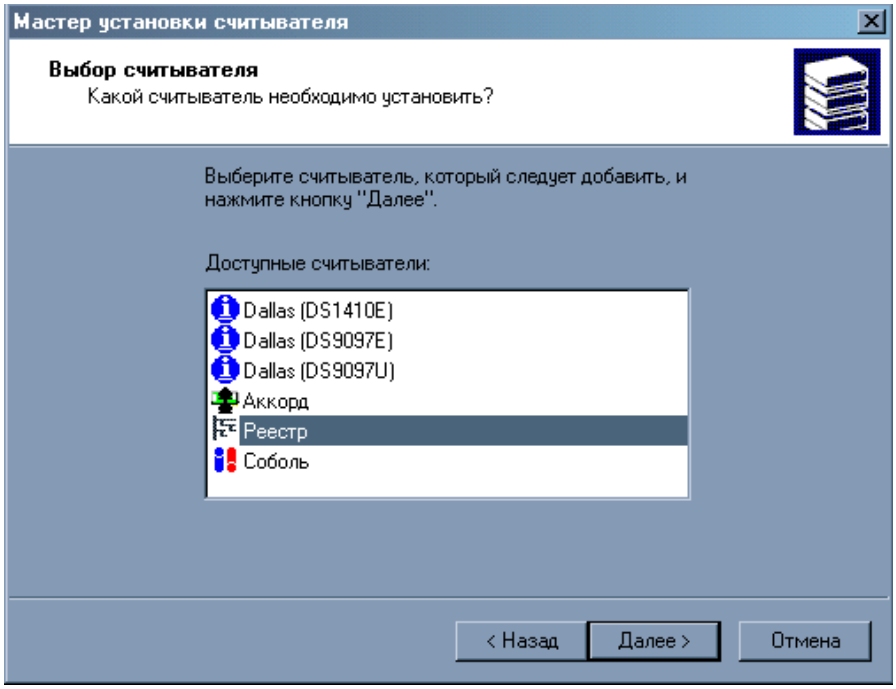


Рисунок 4. Добавление устройства хранения ключей



В состав дистрибутива СКЗИ КриптоПро CSP не входят драйвера и другие модули третьих производителей, обеспечивающие взаимодействие КриптоПро CSP с аппаратной частью. Для их установки нужно воспользоваться программой установки, поставляемой производителями таких устройств, либо получить их с сервера разработчика по адресу http://www.cryptopro.ru/CryptoPro/moduls.html. Например, если КриптоПро CSP уже установлено и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

Лицензия и регистрация ПО СКЗИ

Программное обеспечение КриптоПро CSP распространяется с ограниченным использованием по времени – 30 дней. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер и код активации с Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (Дилера).

Для этого откройте панель управления компьютером, используя пункты меню **Пуск, Настройка**, **Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 5) выберите пункт **Ввод лицензии** и введите **серийный номер** и **ключ активации** с бланка **Лицензии** (см. Рисунок 6).

Рисунок 5. Панель настройки

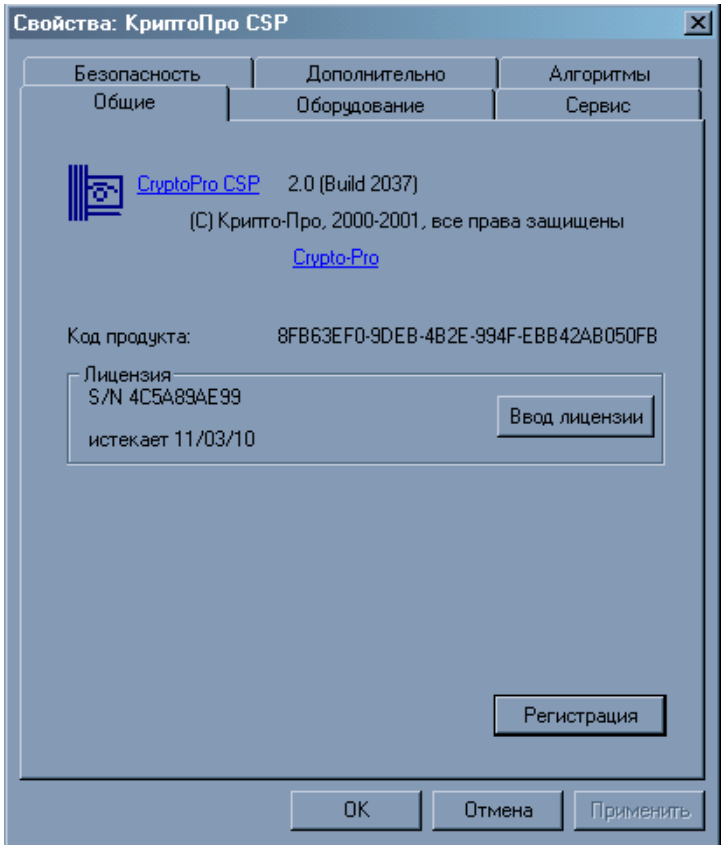
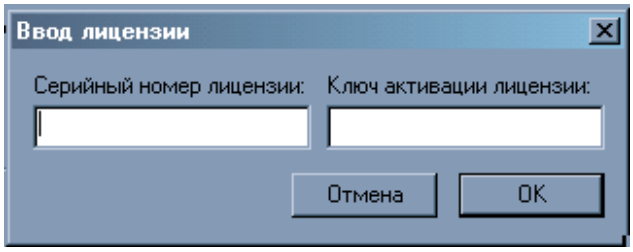


Рисунок 6. Ввод данных лицензии



После завершения программы установки рекомендуется зарегистрировать установленное программное обеспечение КриптоПро CSP у организации-разработчика. Для этого откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**.

В панели настройки СКЗИ КриптоПро CSP (см. Рисунок 5) выберите пункт **Регистрация**, и выполните регистрацию.

Настойка КриптоПро CSP

КриптоПро CSP может функционировать и хранить ключевую информацию в двух режимах:

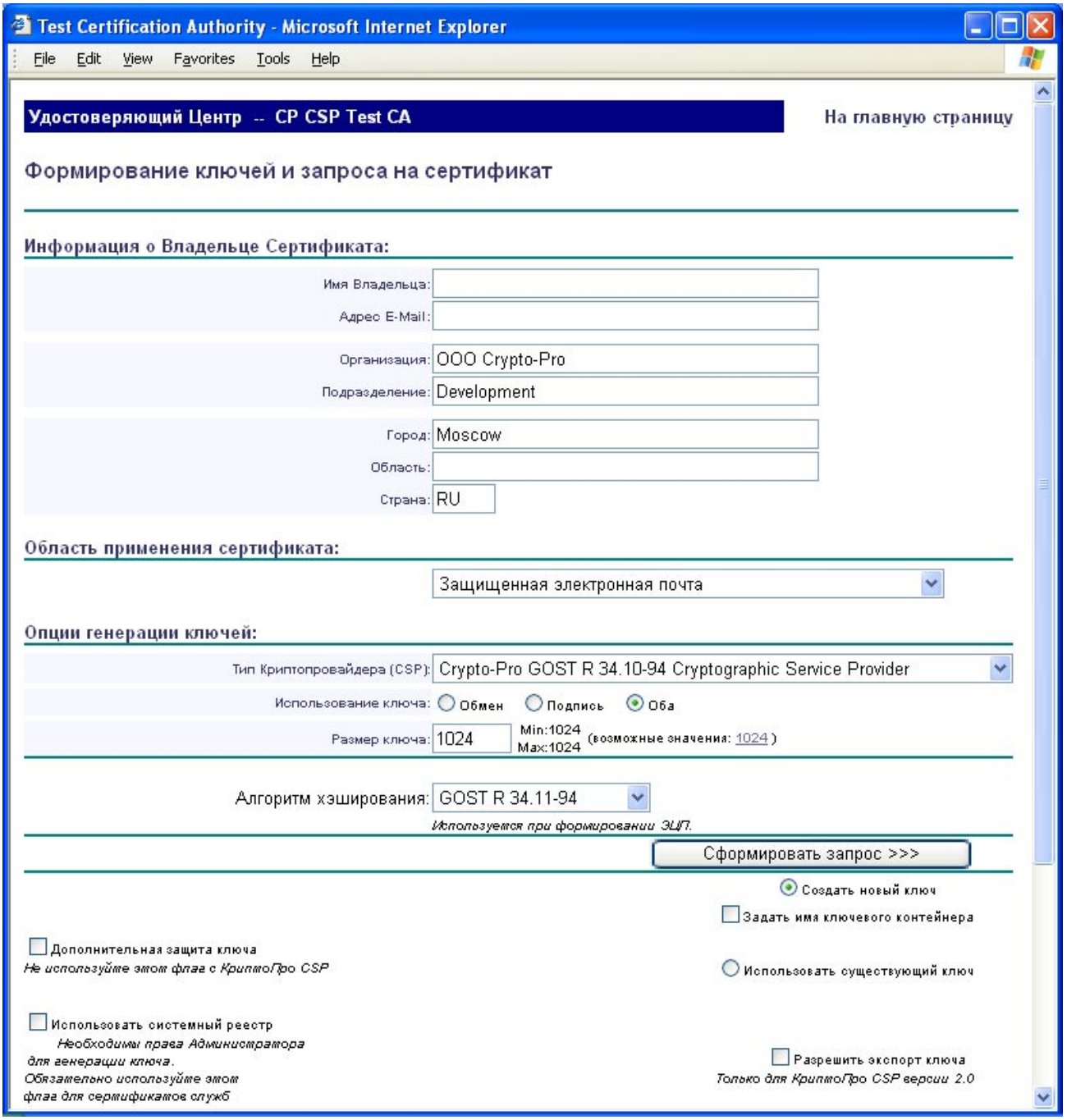
- В памяти приложения.
- В "Службе хранения ключей", которая реализована в виде системного сервиса.

Функционирование КриптоПро CSP в "Службе хранения ключей" обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на компьютере, но может незначительно снизить производительность. Для изменения режима функционирования СКЗИ откройте панель настроек КриптоПро CSP как описано в предыдущем пункте и выберите необходимый режим.

Генерация ключей и получение сертификата

Для формирования личных ключей и получения сертификатов можно воспользоваться тестовым Центром Сертификации http://www.CryptoPro.ru/CertSrv.

Рисунок 7. Генерация ключа



В диалоге создания ключа и формирования запроса на сертификат (см. Рисунок 7) задайте "Имя Владельца" сертификата и введите свой адрес электронной почты "Адрес E-Mail".

Если запрашиваемый сертификат предполагается использовать в электронной почте, выберите **Защищенная электронная почта** в разделе **Область применения ключа**.

Если запрашиваемый сертификат предполагается использовать в протоколе TLS, выберите **Сертификат аутентификации клиента** в разделе **Область применения ключа**.

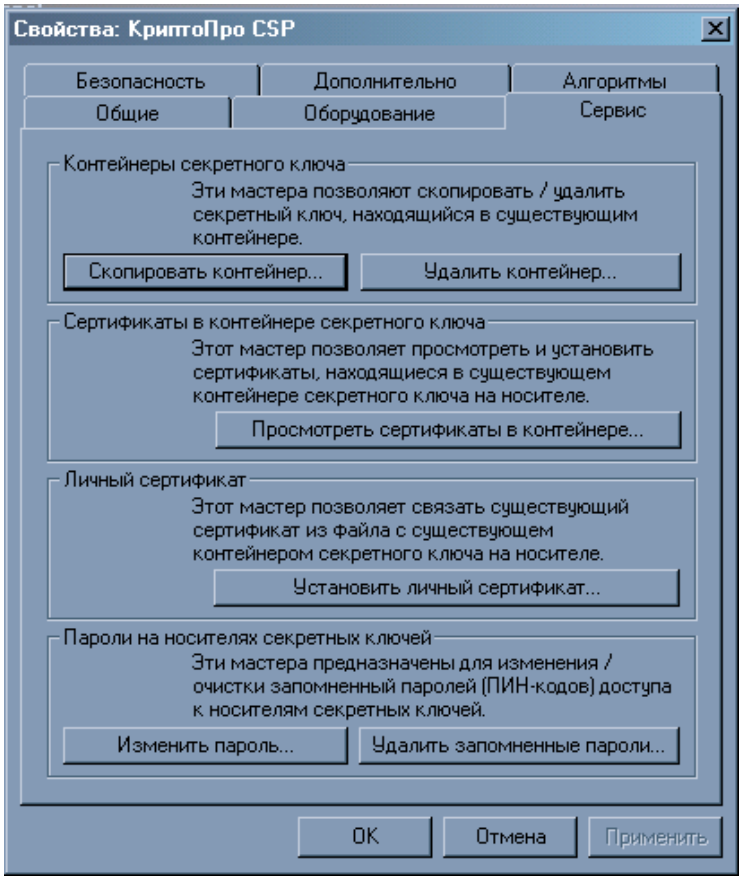
Если введенный адрес почты не совпадает с зарегистрированным адресом в Outlook Express (Outlook), использовать криптографические функции в электронной почте будет невозможно.

Использование ключей и сертификатов на другом компьютере

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а так же вместе с личными ключами пользователя на ключевом носителе (при условии, что ключевой носитель имеет достаточный объем памяти для записи сертификата). Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места.

Для того чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере необходимо на этом компьютере установить пользовательский сертификат в локальных справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

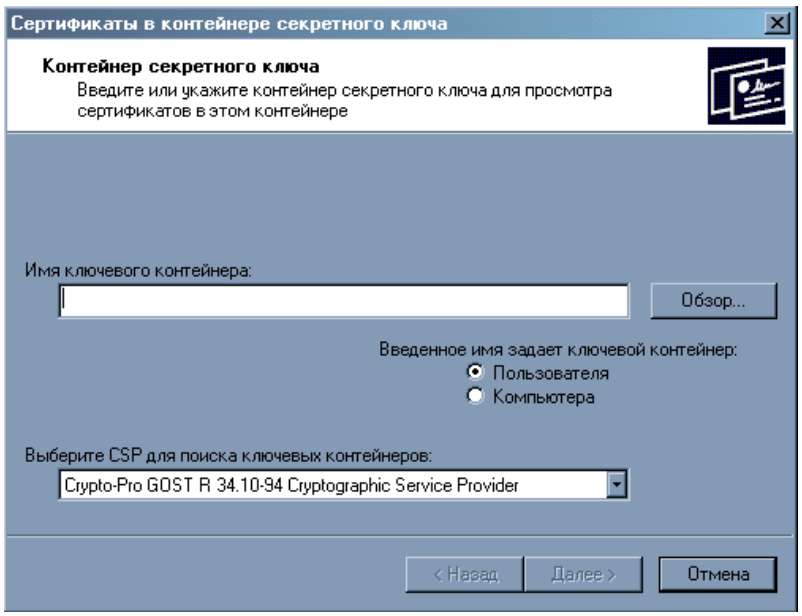
Рисунок 8. Установка сертификата



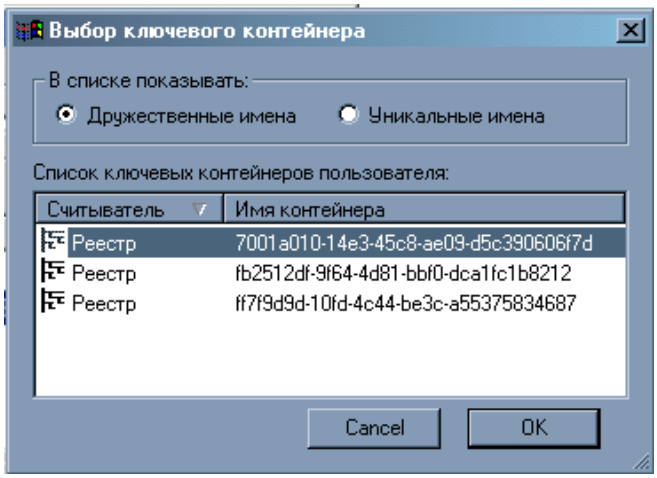
Для этого, используя пункты меню **Пуск, Настройка, Панель управления** в окне панели управления выберите значок **КриптоПро CSP** (см. Рисунок 5). В отображаемом окне диалога выберите закладку **Сервис/Service** и нажмите кнопку **Просмотр сертификатов в контейнере/View certificates in container** (см. Рисунок 8).

Ключевой носитель, содержащий личный ключ и сертификат, при этом должен быть вставлен в соответствующее устройство считывания.

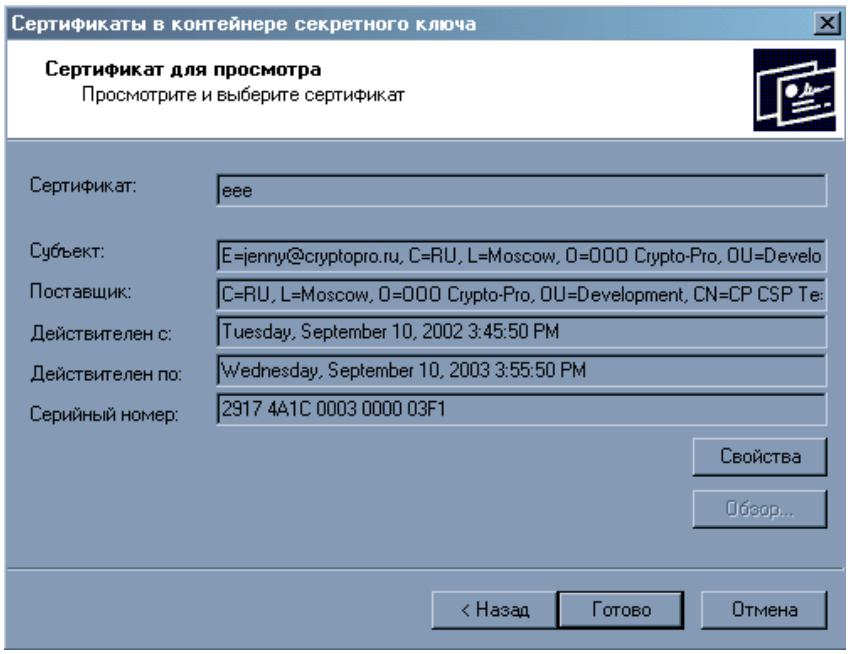
В появившемся окне необходимо выбрать ключевой контейнер, из которого будет устанавливаться сертификат. Для выбора ключевого контейнера нажмите кнопку **Обзор/Browse**. Перед этим можно установить параметры просмотра ключевых контейнеров. Выбирая ключевые контейнеры пользователя или локального компьютера, а также тип CSP можно значительно сузить перечень ключевых контейнеров доступных для установки сертификата.



После нажатия кнопки **Обзор** выберите из списка ключевой контейнер.

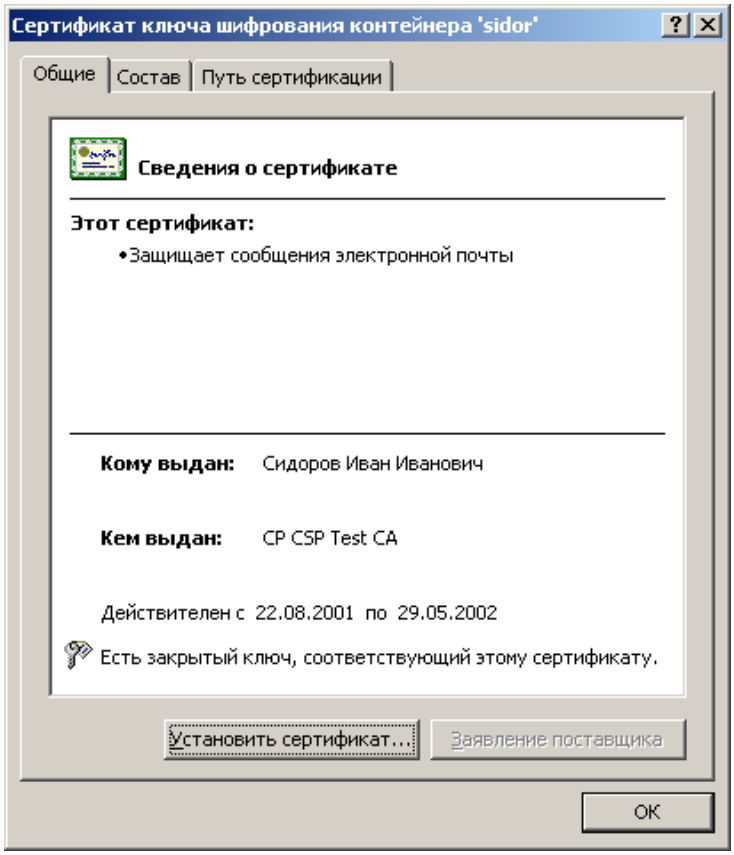


Выбрав ключевой контейнер, и нажав кнопку Дальше/Next, осуществляется переход на окно отображения информации о сертификате, расположенном в ключевом контейнере. В случае, если в ключевом контейнере нет сертификата, об этом будет выведено диагностическое сообщение. Требуется выбрать новый ключевой контейнер для просмотра.



При нажатии на кнопку **Свойства/Properties** содержание его будет отображено в стандартном окне просмотра сертификатов. Нажмите кнопку **Установить сертификат** для его переноса с ключевого носителя в локальный справочник (см. Рисунок 9).

Рисунок 9. Отображение сертификата



Использование КриптоПро CSP

Программное обеспечение КриптоПро CSP позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей X.509 со следующим программным обеспечением:

- Центр Сертификации - Microsoft Certification Authority, входящий в состав OS Windows 2000 Server, Advanced Server (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/2000cert.asp);
- Электронная почта - Microsoft Outlook 98, 2000, XP (http://www.microsoft.com/technet/security/outlksec.asp) (подробнее см. информационный документ "Защита информации в корпоративной электронной почте" в файле "**\DOC\smime.pdf**").
- Электронная почта - Microsoft Outlook Express, входящая в состав Internet Explorer версии 5.0 или выше (http://www.microsoft.com/TechNet/win2000/pubkeyox.asp) (подробнее см. информационный документ "Защита информации в корпоративной электронной почте" в файле "**\DOC\smime.pdf**").
- Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode (http://www.microsoft.com/TechNet/security/authtech.asp)
- Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – Web сервер IIS 5.0 (4.0) (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/maintain/featusability/c06iis.asp). Для использования протокола TLS совместно с КриптоПро CSP, установите дистрибутива программного обеспечения КриптоПро TLS с компакт-диска.

Информационный документ **Инфраструктура Открытых Ключей операционной системы Microsoft Windows 2000** (http://www.cryptopro.ru/CryptoPro/doc/w2k_PKI.doc) приводит описание интегрированных набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими.

На сервере Крипто-Про работают центры сертификации (http://www.cryptopro.ru/certsrv, http://ca.cryptopro.ru) с помощью которых можно сформировать личные ключи и получить сертификаты для их применения в различных приложениях.

Встраивание КриптоПро CSP

Иерархическая архитектура криптографических функций в операционной системе Windows позволяет использовать российские криптографические алгоритмы, реализованные в КриптоПро CSP на самых различных уровнях.

Встраивание на уровне CryptoAPI 2.0.

КриптоПро CSP может быть использовано в прикладном программном обеспечении (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс CryptoAPI 2.0, подробное описание которого приведено в программной документацией MSDN (Microsoft Developer Network) http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncapi/html/msdn_cryptapi.asp. В этом случае способ выбора криптографического алгоритма в прикладном ПО может определятся идентификатором алгоритма открытого ключа отправителя/получателя, содержащегося в сертификате X.509.

Встраивание на уровне CryptoAPI 2.0 позволяет воспользоваться большим набором функций, решающих большинство проблем связанных с представлением (форматами) различных криптографических сообщений (подписанных, зашифрованных), способами представления открытых ключей в виде цифровых сертификатов, способами хранения и поиска сертификатов в различных справочниках, включая LDAP.

Функции CryptoAPI 2.0 позволяют полностью реализовать представление и обмен данными в соответствии с международными рекомендациями и Инфраструктурой Открытых Ключей (Public Key Infrastructure).

Встраивание на уровне CSP

КриптоПро CSP может быть непосредственно использовано в прикладном программном обеспечении путем загрузки модуля с использованием функции LoadLibrary(). Для этих целей в комплект поставки включается **Руководство программиста**, описывающее состав функций и тестовое ПО. При такой реализации прикладному ПО доступен лишь ограниченный набор низкоуровневых криптографических функций, соответствующий интерфейсу Microsoft CSP.

Использование COM интерфейсов

КриптоПро CSP может быть использовано из COM интерфейсов, разработанных Microsoft.

- CAPICOM 2.0
- Certificate Services
- Certificate Enrollment Control

Certificate Enrollment Control

COM интерфейс Certificate Enrollment Control (реализованный в файле xenroll.dll) предназначен для использования ограниченного количества функций CryptoAPI 2.0, связанных с генерацией ключей, запросов на сертификаты и обработкой сертификатов, полученных от Центра Сертификации с использованием языков программирования Visual Basic, C++, JavaScript, VBScript и среды разработки Delphi.

Именно этот интерфейс используют различные публичные Центры Сертификации (Verisign, Thawte и т. д.) при формировании сертификатов пользователей на платформе Windows.

CAPICOM 2.0

CAPICOM (реализованный в файле capicom.dll) предоставляет COM интерфейс, использующий основные функции CryptoAPI 2.0. Этот компонент является добавлением к уже существующему COM интерфейсу Certificate Enrollment Control (xenroll.dll), который реализуют клиентские функции генерации ключей, запросов на сертификаты и обмена с центром сертификации.

С выпуском данного компонента стало возможным использование функций формирования и проверки электронной цифровой подписи, построения и проверки цепочек сертификатов, взаимодействия с различными справочниками сертификатов (включая Active Directory) с использованием Visual Basic, C++, JavaScript, VBScript и среды разработки Delphi. Использование CAPICOM позволяет реализовать функциональность "тонкого" клиента в интерфейсе броузера Internet Explorer.

Компонент CAPICOM является свободно распространяемым и поставляется в составе Redistributable инструментария разработчика Microsoft Platform SDK.

Подробную информацию об интерфейсе CAPICOM можно получить на сервере http://www.cryptopro.ru/CryptoPro/capicom.html. Дистрибутив интерфейса и примеры использования находятся на компакт-диске в директории "**\REDISTR\CAPICOM 2.0**".

Certificate Services

Certificate Services включает в себя несколько COM интерфейсов, позволяющих изменить функциональность Центра Сертификации, входящего в состав ОС Windows 2000 Server. При помощи данных интерфейсов возможно:

- обрабатывать поступающие от пользователей запросы на сертификаты;
- изменить состав данных (в том числе дополнений X.509), записываемых в издаваемые центром сертификаты;
- определить дополнительный способ публикации (хранения) изданных центром сертификатов.

Использование протокола TLS в прикладном программном обеспечении

Кроме использования протокола TLS в интерфейсе Internet Explorer, прикладное программное обеспечение может использовать протокол TLS с КриптоПро CSP для аутентификации и защиты данных, передаваемых по собственным протоколам на основе TCP/IP и HTTPS.

Для встраивания протокола TLS в комплект примеров, поставляемых с Platform SDK, входят примеры WebClient и WebServer.

Примеры использования средств криптографической защиты

КриптоПро CSP поставляется с тестовым ПО, содержащим примеры вызовов основных функций CryptoAPI 2.0. Примеры находятся в директории ("**\SAMPLES\csptest**") Большое количество

примеров использования функций CryptoAPI 2.0, CAPICOM, Certificate Services входит в документацию MSDN и в инструментарий разработчика Platform SDK.

На сервере Крипто-Про (http://www.cryptopro.ru/CryptoPro/forum.html) ведется конференция по вопросам использования криптографических функций и сертификатов открытых ключей. Соответствующие конференции по отдельным темам ведутся на сервере Microsoft:

- http://discuss.microsoft.com/archives/cryptoapi.html - вопросы использования CryptoAPI;
- http://discuss.microsoft.com/archives/capicom.html - вопросы использования технологии Authenticode;
- http://discuss.microsoft.com/archives/authenticode.html - вопросы использования CAPICOM.

В этих конференциях зарегистрировано около 1500 пользователей и разработчиков.

Заключение

КриптоПро CSP позволяет использовать стойкие сертифицированные средства криптографической защиты информации в составе обширного инструментария и программного обеспечения корпорации Microsoft, для реализации различных защищенных систем документооборота и электронной коммерции, на основе Инфраструктуры Открытых Ключей (Public Key Infrastructure), соответствующей международным рекомендациям X.509, RFC 2459.