127 018, Москва, Сущевский Вал, д.18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 3.6.1

Руководство администратора безопасности

Использование СКЗИ под управлением ОС Windows

ЖТЯИ.00050-03 90 02-08
Листов 34

2013

Содержание

Аннотация

Настоящее Руководство дополняет документ «ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть» при использовании СКЗИ под управлением операционных систем Windows 2000/2003/Vista/2008/7/2008R2/8/2012.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро CSP, должны разрабатываться с учетом требований настоящего документа.

Список сокращений

АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
Сертификат	Электронный документ, подтверждающий принадлежность открытого *ключа* и определенных *атрибутов* конкретному абоненту
Сертификация	Процесс изготовления *сертификата* открытого ключа абонента в центре сертификации
СФК	Среда функционирования криптосредства
СКЗИ	Средство криптографической защиты информации

1. Основные технические данные и характеристики СКЗИ

1.1. Программно-аппаратные среды функционирования

СКЗИ ЖТЯИ.00050-03 функционирует под управлением ОС Windows в программно-аппаратных средах:

Windows 2000 (x86);

Windows 2003/Vista/2008/7/2008R2/8/2012 (x86, ia64, x64).

В ОС Windows 2000 при использовании СКЗИ должна быть произведена установка следующих пакетов обновлений:

1. Service Pack 4
2. Microsoft Security Bulletin MS02-050. Certificate Validation Flaw Could Enable Identity Spoofing (Q328145). September 09, 2002.
   Доступ по адресу:
   http://www.microsoft.com/technet/security/bulletin/MS02-050.mspx

В ОС Windows 2003 должна быть произведена установка пакета обновлений Service Pack 1.

Со сроками эксплуатации операционных систем, в среде которых функционирует СКЗИ, можно ознакомиться по ссылке: http://support.microsoft.com/gp/lifeselect.

1.2. Исполнения СКЗИ

СКЗИ в программно-аппаратных средах п.1.1 выпускается в пяти вариантах исполнения:

Исполнение 1 класса защиты КС1 в составе криптопровайдера, криптодрайвера, модуля сетевой аутентификации (TLS), модуля аутентификации пользователя в домене Windows, модуля протоколов КриптоПро IKE, КриптоПро ESP, модуля шифрующей файловой системы КриптоПро EFS, модуля командной строки, модуля поддержки интерфейса Microsoft CNG, модуля поддержки интерфейса Mozilla NSS, сервисных модулей (cpverify, wipefile, stunnel); функционирует в программно-аппаратных средах п.1.1.

Исполнение 2 класса защиты КС2 в составе исполнения 1 с добавлением утилиты выработки внешней гаммы; функционирует в программно-аппаратных средах п.1.1.

Исполнение 3 класса защиты КС3 в составе криптодрайвера, криптосервиса, модуля сетевой аутентификации (TLS), модуля шифрующей файловой системы КриптоПро EFS, модуля командной строки, утилиты выработки внешней гаммы, сервисных программ; функционирует в программно-аппаратных средах Windows 2003 (платформа x86, x64) с пакетом Secure Pack Rus версии 3.0.

Описание данного исполнения и рекомендации по использованию содержатся в документе ЖТЯИ.00050-03 90 02-01. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ класса защиты КС3 под управлением ОС Windows.

Исполнение 4 класса защиты КС3 выполнено в составе криптодрайвера,

Криптосервиса, модуля сетевой аутентификации (TLS), модуля аутентификации пользователя в домене Windows, модуля КриптоПро IPSec, модуля шифрующей файловой системы КриптоПро EFS (ОС Windows), модуля командной строки, сервисных программ, утилиты выработки внешней гаммы; и функционирует в программно-аппаратных средах Windows 2003/Vista/2008/7/2008R2 (x86, x64) с пакетом Secure Pack Rus версии 3.0.

Описание данного исполнения и рекомендации по использованию содержатся в документе ЖТЯИ.00050-03 90 02-01. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ класса защиты КС3 под управлением ОС Windows.

Исполнение 5 класса защиты КС3 выполнено в составе

криптодрайвера, криптосервиса, модуля сетевой аутентификации (TLS),

модуля шифрующей файловой системы КриптоПро EFS (ОС Windows), сервисных программ и функционирует в программно-аппаратных средах Windows 2000/2003 (платформа ia32), Windows 2003 (платформа x64) с программным обеспечением СЗИ Secret Net 6.

Описание данного исполнения и рекомендации по использованию содержатся в документе ЖТЯИ.00050-03 90 02-01. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ класса защиты КС3 под управлением ОС Windows.

1.3. Ключевые носители

В качестве ключевых носителей используются:

- ГМД 3,5’’;
- USB диски
- электронный ключ с интерфейсом USB (e-Token);
- Смарткарты РИК, Оскар, Магистра
- идентификаторы Touch-Memory DS1995 – DS1996 ПАК защиты от НСД (Аккорд-АМДЗ, электронный замок "Соболь);
- Rutoken;
- Раздел HDD ПЭВМ (в ОС Windows – реестр).

Использование ключевых носителей в зависимости от программно-аппаратной платформы см. документ "ЖТЯИ.00050-03 30 01. СКЗИ "КриптоПро CSP". Формуляр, п.п. 3.8, 3.9.

Примечание 1. В состав дистрибутива СКЗИ ЖТЯИ.00050-03 входят библиотеки поддержки всех перечисленных носителей, но не входят драйвера для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

Примечание 2. Допускается хранение закрытых ключей в реестре ОС Windows и в разделе HDD (в случае других ОС) при условии распространения на HDD или ПЭВМ с HDD требований по обращению с ключевыми носителями, в том числе и после удаления ключей из реестра.

2. Установка дистрибутивов ПО СКЗИ

Установка дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права администратора.

СКЗИ КриптоПро CSP требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

Для исполнений 1,2 модуль IPsec поставляется в виде библиотек в SDK и не требует установки через setup.

Для установки программного обеспечения вставьте компакт-диск в привод считывателя. Из предлагаемых дистрибутивов выберите дистрибутив,

пдходящий для Вашей операционной системы, имеющий нужный Вам класс защиты и удобный для Вас язык установки. Запустите выполнение установки.

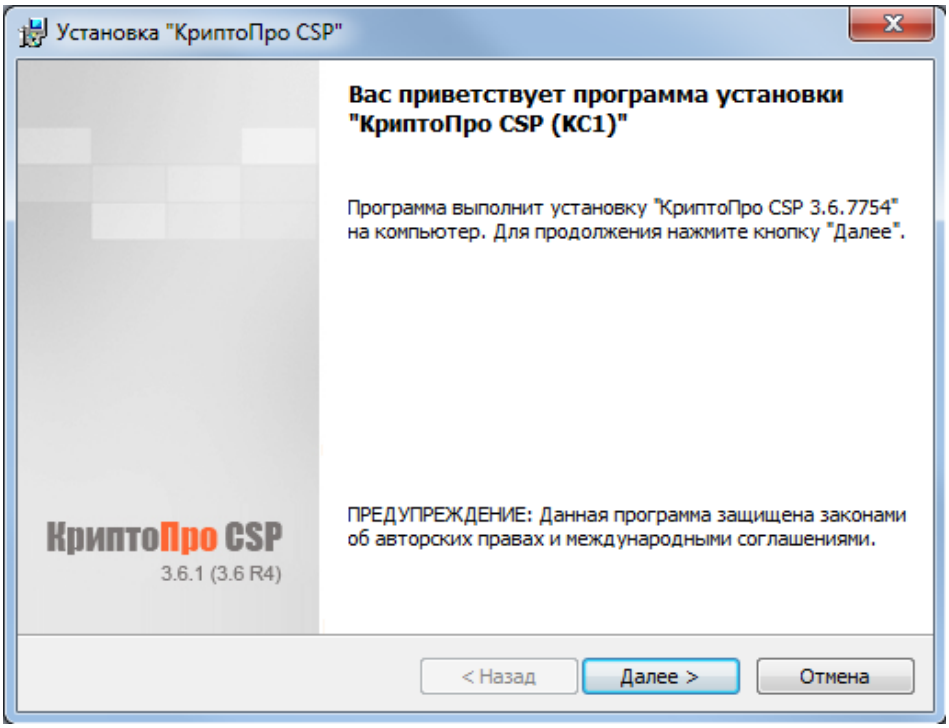


Рис. 2. Приветственное окно мастера установки.

Если мастер установки обнаружит на машине более раннюю версию КриптоПро CSP, то в этом окне появится информация о замещаемых продуктах:

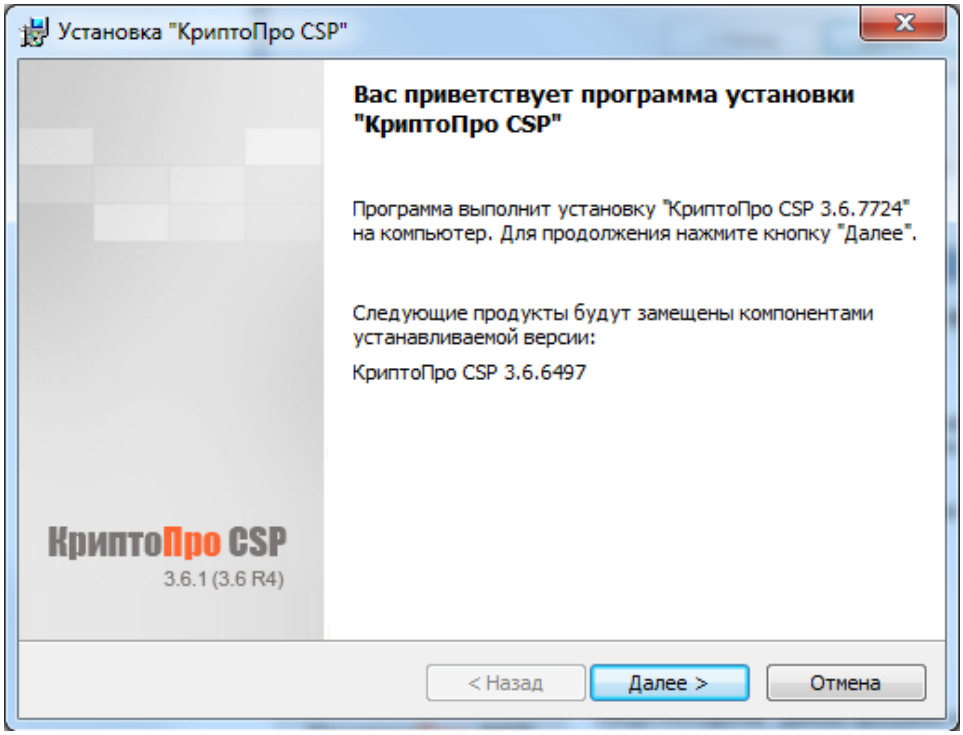


Рис. 3. Установка с замещением компонент.

Для дальнейшей установки КриптоПро CSP нажмите **Далее**.

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации,

дополнительные датчики случайных чисел (для класса КС2) или настроить криптопровайдер на использование службы хранения ключей (для класса КС1). Все эти настройки можно произвести как в момент установки криптопровайдера, так и в любой момент после завершения установки через панель свойств.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

2.1. Параметры установки КриптоПро CSP.

При установке КриптоПро CSP можно использовать различные параметры командной строки, влияющие на устанавливаемые компоненты, начальную настройку продукта и т.д.

Для их использования необходимо запускать установку следующим образом:

msiexec /i <полный или относительный путь к .msi-файлу> <параметры>

2.1.1. Справочник параметров установки

Следующие опции позволяют не устанавливать соответствующие библиотеки поддержки:

NOACCORD=1 - Аккорд

NOBIO=1 - Биологический ДСЧ

NODALLAS=1 - Носители Dallas

NODS=1 - Считыватели Dallas

NODSRF=1 - ДСЧ "Последовательность поставщика"

NOEMV=1 - Карта EMV

NOFLOPPY=1 - Считыватель дискет

NOJCARD=1 - Карты JCard

NOPCSC=1 - PC/SC

NOREGISTRY=1 - Считыватель "Реестр"

NORIC=1 - Карты RIC/OSCAR

NORUTOKEN=1 - Носитель Rutoken

NOSABLE=1 - Соболь

Следующие опции позволяют управлять регистрацией поддерживаемого оборудования во время установки КриптоПро CSP (значение 0 означает "отключить опцию"; звездочкой отмечены опции, включенные по умолчанию):

REGACCORDRDR=1 - Зарегистрировать считыватель "Аккорд"

REGACCORDRND=1 - Зарегистрировать ДСЧ "Аккорд"

REGBIO=1 - Зарегистрировать биологический ДСЧ *(только для КС1)

REGETOKEN=1 - Зарегистрировать все носители "Alladin eToken" * отдельные типы: REGETOKENJAVA10, REGETOKENJAVA10B, REGETOKENM420, REGETOKENM420B, REGETOKEN16, REGETOKEN32, REGETOKENR2

REGFLOPPY=буквы - Зарегистрировать считыватель "дискета" для букв, указанных через запятую

REGPNPFLOPPY=1- Зарегистрировать считыватель "Все съемные носители" *

REGDSRF=путь - Зарегистрировать ДСЧ "Последовательность поставщика" и задать путь (без "\" на конце) к папке с db1, db2

REGDS1410E=порты - Зарегистрировать считыватель "DS1410E" (список портов через запятую: LPT1,LPT2,...)

REGDS9097E=порты - Зарегистрировать считыватель "DS9097E" (список портов через запятую: COM1,COM2,...)

REGDS9097U=порты - Зарегистрировать считыватель "DS9097U" (список портов через запятую: COM1,COM2,...)

REGDS199X=1 - Зарегистрировать носитель "DS199x"

REGOSCAR=1 - Зарегистрировать носитель "Оскар"

REGOSCAR2=1 - Зарегистрировать носитель "Оскар2" *

REGTRUST=1 - Зарегистрировать носитель "Магистра" *

REGTRUSTS=1 - Зарегистрировать носитель "Магистра Сбербанк/BGS" *

REGTRUSTD=1 - Зарегистрировать носитель "Магистра Debug" *

REGPNPPCSC=1 - Зарегистрировать считыватель "Все считыватели смарткарт" *

REGALLPCSC=1 - Зарегистрировать подключенные считыватели смарткарт

REGREGISTRY=1 - Зарегистрировать считыватель "Реестр"

REGRIC=1 - Зарегистрировать носитель "РИК"

REGRUTOKEN=1 - Зарегистрировать носитель "Rutoken" *

REGSABLERDR=1 - Зарегистрировать считыватель "Соболь"

REGSABLERND=1 - Зарегистрировать ДСЧ "Соболь"

NOETOKENWL=1 - Не регистрировать носители "Alladin eToken" для Winlogon

NOOSCAR2WL=1 - Не регистрировать носитель "Оскар2" для Winlogon

NOTRUSTWL=1 - Не регистрировать носитель "Магистра" для Winlogon

NOTRUSTSWL=1 - Не регистрировать носитель "Магистра Сбербанк/BGS" для Winlogon

NOTRUSTDWL=1 - Не регистрировать носитель "Магистра Debug" для Winlogon

NORUTOKENWL=1 - Не регистрировать носитель "Rutoken" для Winlogon *

Управление режимами работы:

CPCSPR=1 - Для версии КС1 позволяет выбрать режим службы хранения ключей (только при установке)

MEDIACSPS=1 - Регистрировать в системе отдельный провайдер для каждого типа ключевых носителей (только при установке)

CACHED=N - Настройка кэширования ключей. Если N=0, то выключено, если N>0, то задает размер кэша (только при установке и только для режима службы хранения ключей)

CSPDELETEKEYS=1 - При удалении продукта удалит так же все настройки и все ключевые контейнеры из реестра

Указание серийных номеров лицензий:

PIDKEY= - Использовать указанный серийный номер CSP

WLPIDKEY= - Использовать указанный серийный номер Winlogon

RPPIDKEY= - Использовать указанный серийный номер Revocation Provider

OCSPAPIPIDKEY= - Использовать указанный серийный номер OCSP Client

TSPAPIPIDKEY= - Использовать указанный серийный номер TSP Client

Стандартные параметры Windows Installer (подробнее – см. документацию: http://msdn.microsoft.com/en-us/library/aa367988.aspx):

INSTALLDIR=... - Путь установки

INSTALLDIR64=... - Путь установки для 64-компонент (x64, Itanium)

REBOOT=R - Не перезагружать компьютер после установки

ADDLOCAL=модули - Задает список дополнительных модулей, которые следует установить (список через зяпятую).

Существующие дополнительные модули: reprov, driver, compat.

REMOVE=модули- ДЛЯ УЖЕ УСТАНОВЛЕННОГО ПРОДУКТА удаляет указанные модули

/qb - установка без мастера

/qn - установка без окон

/L*v файл - создание журнала установки

Для удаления КриптоПро CSP:

msiexec /x {54A08450-B343-40B0-924E-68F031450996}

Примеры:

msiexec /i "d:\КриптоПро CSP 3.6\csp-win32-kc1-rus.msi" INSTALLDIR="d:\csp" /L*v "c:\temp\csp.log" /qb

3. Обновление СКЗИ КриптоПро CSP

Для обновления КриптоПро CSP на ОС Windows необходимо:

запомнить текущую конфигурацию CSP (установленные ДСЧ, считыватели, носители, параметры алгоритмов по умолчанию и т.п.)

удалить штатными средствами ОС дистрибутив КриптоПро CSP

установить аналогичный новый дистрибутив КриптоПро CSP

при необходимости внести изменения в настройки

ключи и сертификаты сохраняются автоматически.

4. Варианты встраивания КриптоПро CSP и КриптоПро TLS в прикладное ПО

4.1. 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, описание которого приведено в программной документации MSDN (Microsoft Developer Network): http://msdn.microsoft.com/en-us/library/windows/desktop/aa380239.aspx. В этом случае способ выбора криптографического алгоритма в прикладном ПО может определяться идентификатором алгоритма открытого ключа отправителя/получателя, содержащегося в сертификате X.509.

Встраивание на уровне CryptoAPI 2.0 позволяет воспользоваться 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).

4.2. 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.

4.3. Использование COM интерфейсов

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

- CAPICOM 1.0
- 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 1.0

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/documentation/capicom.htm.

Certificate Services

Certificate Services включает в себя несколько COM интерфейсов, позволяющих изменить функциональность Центра Сертификации, входящего в состав ОС Windows 2000/2003 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.

4.4. Использование СКЗИ на платформе Microsoft .NET Framework

Компанией КРИПТО-ПРО был разработан программный продукт КриптоПро .NET, позволяющий использовать средство криптографической защиты информации КриптоПро CSP на платформе Microsoft .NET Framework. КриптоПро .NET реализует набор интерфейсов для доступа к криптографическим операциям .NET Cryptographic Provider:

- хеширование;
- подпись;
- шифрование;
- MAC;
- генерация ключей и т.д.

Кроме того КриптоПро .NET позволяет использовать стандартные классы Microsoft для высокоуровневых операций:

- разбор сертификата;
- построение и проверка цепочки сертификатов;
- обработка CMS сообщений;
- установление защищенного обмена через SSL/TLS, HTTPS и FTPS;
- XML подпись и шифрование.

Подробную информацию, дистрибутивы, документацию и сценарии использования можно найти на сайте продукта www.cryptopro.net.

4.5. Использование СКЗИ в веб-браузерах

СКЗИ ЖТЯИ.00050-03 может быть использовано в веб-браузерах на различных программно-аппаратных платформах путём вызова функций КриптоПро ЭЦП Browser plug-in.

КриптоПро ЭЦП Browser plug-in содержит компоненту ActiveX для работы в Microsoft Internet Explorer и плагин NPAPI для других веб-браузеров, поддерживающих данный интерфейс встраивания плагинов. Функции СКЗИ можно вызывать из сценариев JavaScript, содержащихся в отображаемой веб-браузером странице.

Подробная информация доступна странице плагина по адресу http://www.cryptopro.ru/products/cades/plugin.

4.6. Инициализация библиотеки SSPI

Производится загрузка библиотеки Secur32.dll.

С помощью функции GetProcAddress получается указатель на функцию InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode).

Вызовом функции InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode) получается таблица функций SSPI.

Или, вместо использования GetProcAddress, достаточно поключить библиотеку импорта secur32.lib (входит в MS Platform SDK)

Заполняется структура SCHANNEL_CRED. Поля этой структуры должны быть нулевыми, кроме:

```
SchannelCred.dwVersion = SCHANNEL_CRED_VERSION;
SchannelCred.dwFlags = SCH_CRED_NO_DEFAULT_CREDS |
SCH_CRED_MANUAL_CRED_VALIDATION;
```

Для сервера и не анонимного клиента заполняются также поля:

```
SchannelCred.cCreds     = 1;
SchannelCred.paCred     = &pCertContext.
```

Примечание. Контекст сертификата pCertContext должен содержать ссылку на закрытый ключ.

Производится вызов функции создания Credentials: AcquireCredentialsHandle с передачей ей структуры SCHANNEL_CRED и имени пакета - UNISP_NAME ("Microsoft Unified Security Protocol Provider").

Инициализация соединения клиентом производится вызовом InitializeSecurityContext без входного буфера и сервером – вызовом AcceptSecurityContext, после чего идет обычный цикл Handshake.

После установления соединения, но до начала передачи данных, приложение должно выполнить проверку параметров соединения и сертификата удаленной стороны.

Для получения сертификата удаленной стороны вызывается функция QueryContextAttributes с аргументом SECPKG_ATTR_REMOTE_CERT_CONTEXT.

Для построения цепочки сертификатов рекомендуется использование функции CertGetCertificateChain, описанную в MSDN/Platform SDK/Security, (с флагами проверки, соответствующими выбранному уровню безопасности. Рекомендуется использовать флаг

CERT_CHAIN_CACHE_END_CERT | CERT_CHAIN_REVOCATION_CHECK_CHAIN.

Цепочка сертификатов проверяется функцией CertVerifyCertificateChainPolicy, описанной там же, с аргументом pszPolicy, равным OIDCERT_CHAIN_POLICY_SSL, и аргументом pPolicyPara, заполненным следующим образом:

```
ZeroMemory(&polHttps, sizeof(HTTPSPolicyCallbackData));
polHttps.cbStruct           = sizeof(HTTPSPolicyCallbackData);
polHttps.dwAuthType         = AUTHTYPE_SERVER;
polHttps.fdwChecks          = 0;
polHttps.pwszServerName     = pwszServerName;
memset(&PolicyPara, 0, sizeof(PolicyPara));
PolicyPara.cbSize            = sizeof(PolicyPara);
PolicyPara.pvExtraPolicyPara = &polHttps;
```

Необходимо, чтобы для каждого сертификата в цепочке

pCertContext->pCertInfo->SubjectPublickeyInfo->Algoritm->pszObjId заканчивалась на szOID_GR3410.

Вызывается функция QueryContextAttributes с аргументом ulAttribute, равным SECPKG_ATTR_CONNECTION_INFO, для получения параметров соединения и их проверки на выполнение условий:

```
ConnectionInfo.dwProtocol == SP_PROT_TLS1_CLIENT
ConnectionInfo.aiCipher == CALG_G28147, ConnectionInfo.aiHash ==
CALG_GR3411
aiExch=CALG_DH_EX_EPHEM или CALG_DH_EX_SF
```

Шифрования/расшифрование реализуется с помощью функций EncryptMessage()/DecryptMessage().

Примечание. Должна быть обеспечена корректная обработка кодов возврата функций SSPI. При этом следует учитывать, что требуется разная обработка в зависимости от того, является код возврата кодом успешного выполнения функции, кодом не фатальной ошибки, не требующей разрыва соединения, кодом фатальной ошибки, требующей разрыва соединения. Все необрабатываемые коды возврата ошибок должны приводить к разрыву соединения.

4.7. Завершение сессии

Корректное завершение сессии осуществляется вызовом функции ApplyControlToken.

4.8. Требования безопасности

1. Применение модуля поддержки сетевой аутентификации допускается только при использовании открытых ключей сервера и клиента, сертифицированных доверенным центром сертификации

2. Приложением должны обеспечиваться проверка сертификатов в сообщениях Certificate и CertVerify, проверка 12 байт в сообщениях Finished клиента и сервера, являющихся имитовставками к информации всего диалога

клиент-сервер в процессе установления сессии, контроль соответствия имени клиента (сервера) IP-адресу, по которому установлена сессия.

5. Состав и назначение компонент программного обеспечения СКЗИ

Программное обеспечение СКЗИ КриптоПро CSP при функционировании под управлением ОС Windows 2000/2003/Vista/2008/7/2008R2/8/2012 состоит из следующих компонент:

1. Сервисные модули;
2. Модули настройки встроенной подсистемы криптографической защиты информации (ПКЗИ) ОС Windows;
3. Модули сопряжения КриптоПро CSP со встроенным ПКЗИ ОС Windows и интерфейс криптографического сервиса;
4. СКЗИ КриптоПро CSP, реализующее целевые функции криптопровайдера в форме:
5. - библиотек, загружаемых в адресное пространство приложения;
6. - криптографического сервиса хранения ключей;
7. - криптографического драйвера;
8. - библиотек протокола КриптоПро TLS.

5.1. Сервисные модули

Сервисные модули обеспечивают контроль целостности дистрибутива КриптоПро CSP, его установку и удаление из операционной системы, а так же конфигурацию параметров СКЗИ для каждого пользователя.

5.1.1. Модуль контроля целостности дистрибутива

Модуль **cpverify.exe,** см. Приложение 1, предназначен для контроля целостности дистрибутива при установке и использовании ПО СКЗИ КриптоПро CSP на компьютере пользователя (поставляется совместно с дистрибутивом).

5.1.2. Дистрибутив

Дистрибутив СКЗИ КриптоПро CSP поставляется в виде пакета "Windows Installer" (файл **csp-win32-kc1-rus.msi** или подобное название. В названии файла установщика присутствует обозначение платформы, для которой он предназначен, класс защиты и язык установки). При запуске файл **csp-win32-kc1-rus.msi** разворачивает структуры данных дистрибутива во временный каталог и проводит установку ПО СКЗИ КриптоПро CSP.

5.1.3. Модуль конфигурации

Модуль **cpconfig.cpl** обеспечивает возможность управления пользователем конфигурацией ПО СКЗИ КриптоПро CSP, а так же содержит возможности регистрации установленного ПО и получения пользователем дополнительной информации.

5.1.4. Модуль Wipefile

Модуль **wipefile** используется для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях.

5.1.5. Модуль контроля целостности в драйвере

Для работы с любым отладчиком модуль контроля целостности в драйвере должен быть отключен. Порядок отключения данного модуля описан в документе ЖТЯИ.00050-03 90 05. КриптоПро CSP. Руководство программиста.

5.2. Модули настройки ПКЗИ ОС Windows

Модули предназначены для обеспечения использования ПО СКЗИ КриптоПро CSP в ПКЗИ ОС Windows. Модули также реализуют форматы

криптографических сообщений, используемых в защищенной электронной почте (S/MIME), Office 2003/XP, Authenticode и функциях CryptoAPI 2.0, форматы сертификатов и их обработку.

Примечание. Полный перечень поддерживаемых приложений Microsoft приведен в документе ЖТЯИ.00050-03 90 01. КриптоПро CSP. Описание реализации.

Модули настройки классифицируются как ПКЗИ и ответственны за использование криптопровайдера КриптоПро CSP со стороны приложений. Они обеспечивают вызов сервиса криптографических функций, но не обрабатывают ключевую и криптографически опасную информацию (не имеют доступа к ключам и т. п.).

5.2.1. Модуль расширения и настройки CryptoAPI 2.0

Модуль **cpext.dll** является зарегистрированной в системном реестре Windows динамической библиотекой (DLL) расширения CryptoAPI 2.0 и обеспечивает:

- установку соответствия между идентификаторами объектов (OID) в криптографических сообщениях и сертификатах открытых ключей и функциями СКЗИ КриптоПро CSP;
- формирование и разбор криптографических сообщений и сертификатов открытых ключей.

5.2.2. Модули инициализации настройки встроенного ПКЗИ ОС Windows

Модуль инициализации для ОС Windows 2000/2003/Vista/2008/7/2008R2/8/2012 реализован в виде драйвера **CProCtrl.sys**. Драйвер обеспечивает загрузку определенных динамических библиотек (DLL) в адресное пространство процессов, использующих СКЗИ.

Дополнительно этот модуль осуществляет контроль целостности установленного ПО КриптоПро CSP **и ПКЗИ** (периодический и при загрузке ОС).

5.2.3. Модуль настройки для системного DLL crypt32.dll

Модуль **cpcrypt.dll** загружается в виртуальное адресное пространство каждого процесса, к которому подгружается **crypt32.dll**, для установления перехватов функций, использующих провайдер КриптоПро CSP.

Настройка заключается в добавлении ПКЗИ возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером КриптоПро CSP.

5.2.4. Модуль настройки для системного DLL inetcomm.dll

Модуль **cpintco.dll** загружается в виртуальное адресное пространство каждого процесса, использующего **inetcomm.dll**, для установления перехватов функций.

Настройка заключается в поддержке дополнительных идентификаторов алгоритмов и возможностей S/MIME, реализуемых криптопровайдером КриптоПро CSP, при использовании в ПО Microsoft Outlook и Microsoft Outlook Express.

5.2.5. Модуль настройки для системного DLL certocm.dll

Модуль **cpcertocm.dll** загружается в виртуальное адресное пространство процесса установки центра сертификации (CA) ОС Windows.

Модуль позволяет настроить центр сертификации при его установке так, чтобы поддерживались алгоритмы КриптоПро CSP.

5.2.6. Модуль настройки для системного DLL wininet.dll

Модуль **cpwinet.dll** загружается в виртуальное адресное пространство процесса Internet Explorer, если в него отображается **wininet.dll**.

Модуль позволяет правильно отображать алгоритмы КриптоПро TLS в Internet Explorer.

5.2.7. Модуль настройки для системного DLL advapi32.dll

Модуль **cpadvai.dll** загружается в виртуальное адресное пространство каждого процесса, использующего **advapi32.dll**, для установления перехватов функций.

Настройка заключается в добавлении возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером КриптоПро CSP.

5.2.8. Модуль настройки для системного DLL kerberos.dll

Модуль **cpkrb.dll** загружается в виртуальное адресное пространство процессов, использующих модуль **kerberos.dll**, и обеспечивает эмуляцию поддержки криптопровайдером стандарта **Triple DES**.

5.2.9. Модуль настройки TLS

Модуль **cpschan.dll** загружается в виртуальное адресное пространство процесса Internet Explorer, если он использует TLS.

Модуль позволят использовать алгоритмы КриптоПро TLS в Internet Explorer.

5.2.10. Модули настройки MS Office

Модуль **cpMSO.dll** загружается в виртуальное адресное пространство процессов MS Word и MS Excell и позволяет подписывать документы с помощью алгоритмов КриптоПро CSP.

Модуль **cpExSec.dll** загружается в виртуальное адресное пространство процесса MS Outlook, и настраивает его для правильной работы с КриптоПро CSP.

5.2.11. Модуль настройки XML

Модуль **cpXML.dll** загружается в виртуальное адресное пространство процессов, использующих XML, и позволяет применять алгоритмы КриптоПро CSP для подписи XML.

5.2.12. Модуль настройки контроллера домена

Модуль **cpkdc.dll** загружается в виртуальное адресное пространство процессов доменной аутентификации на контроллере домена и обеспечивает возможность использования для проверки подписи алгоритмов, реализуемых КриптоПро CSP.

5.3. Криптопровайдер КриптоПро CSP

5.3.1. Интерфейсная библиотека криптопровайдера

Интерфейсная библиотека **cpcsp.dll** реализует стандартный интерфейс криптопровайдера, соответствующий спецификации Microsoft Cryptographic Service Provider, и обеспечивает данный интерфейс для обычных приложений через криптографический сервис по RPC, или для привилегированных приложений (имеющих право доступа к устройствам носителей ключевого контейнера) - непосредственно.

5.3.2. Интерфейсная библиотека криптографического сервиса

Интерфейсная библиотека **cpcspr.dll** обеспечивает возможность обращения обычных приложений к сервису криптографических функций по протоколу RPC.

5.4. СКЗИ КриптоПро CSP

Собственно СКЗИ КриптоПро CSP реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, доступ к физическому ДСЧ.

5.4.1. Реализация СКЗИ в форме сервиса хранения ключей

Модуль **cpcspi.dll** реализует целевые функции криптографической защиты информации при обращении по RPC с локального компьютера для интерфейсной библиотеки криптографического сервиса.

Модуль обеспечивает:

- хранение и работу с контекстом уровня библиотеки;
- хранение криптографических объектов:
  - Ключевых пар (постоянных и временных);
  - Открытых ключей (временных);
  - Ключей сессий (временных симметричных);
  - Объектов функции хеширования.
- выполнение криптографических преобразований

5.4.2. Реализация криптопровайдера в форме подгружаемых библиотек

Интерфейс **cpcspi.dll** реализует целевые функции криптографической защиты информации для **Интерфейсной библиотеки криптопровайдера** (см. 5.3.1) в варианте функционирования ПО КриптоПро CSP без использования **Интерфейса криптографического сервиса** (см. 5.3.2).

5.4.3. Реализация криптопровайдера в форме драйвера ядра ОС

Интерфейс **cpdrvlib.sys** реализует подмножество целевых функций криптографической защиты информации для **Интерфейсной библиотеки криптопровайдера** в варианте функционирования ПО КриптоПро CSP в ядре ОС Windows. Драйвер поддерживает выполнение функций шифрования, имитозащиты, хеширования, проверки подписи и выработку ключей согласования на эфемерных ключах. Драйвер не поддерживает работу с пользовательскими ключами.

5.4.4. Интерфейс доступа к физическому и БиоДСЧ

Библиотека **cprndm.dll** обеспечивает унифицированный интерфейс доступа к физическому ДСЧ или БиоДСЧ.

5.4.5. Интерфейсные модули ДСЧ

Обеспечивают реализацию доступа к типам ДСЧ:

bio.dll БиоДСЧ

accord.dll ДСЧ ПАК "Аккорд-АМДЗ"

sable.dll ДСЧ электронного замка "Соболь"

5.4.6. Панель управления ресурсами СКЗИ КриптоПро CSP

Управление ресурсами СКЗИ КриптоПро CSP осуществляется командным файлом **cpconfig.cpl** через панель управления ”Свойства: КриптоПро CSP”. К основным средствам управления ресурсами СКЗИ относятся средства управления:

- лицензиями;
- ДСЧ;
- библиотеками считывания ключевой информации;
- закрытыми ключами и сертификатами открытых ключей;
- параметрами СКЗИ.

5.5. Модуль аутентификации в домене Windows

Модуль **winlogonmgmt.dll** обеспечивает аутентификацию на базе электронной подписи с использованием алгоритмов ГОСТ 34.10-2001, ГОСТ 34.11-94.

Модуль аутентификации обеспечивает разграничение доступа к сети домена Windows либо к локальной машине Windows на основе проверки ЭП, выработанной с использованием ключа доступа, расположенного на ключевом носителе пользователя в ключевом контейнере СКЗИ ЖТЯИ.00050-03. Сертификат открытого ключа проверки подписи заносится в системе при регистрации пользователя домена Windows.

5.6. Модуль поддержки сетевой аутентификации КриптоПро TLS

Модуль поддержки сетевой аутентификации реализуется в форме подгружаемой библиотеки и реализует подмножество интерфейса Microsoft SSPI(SSP/AP) (см. соответствующий раздел MSDN). Модуль обеспечивает аутентичное защищенное соединение между пользователем и сервером. **cpssl.dll**, **cpsspap.dll** – при установке модуля аутентификации поддерживающего аутентификацию в домене, **cpsspcore.dll**, **ssp.dll** – без возможности доменной аутентификации.

5.7. ПКЗИ КриптоПро CSP

5.7.1. Интерфейс доступа к ключевым носителям

Библиотека **cprdr.dll** обеспечивает унифицированный интерфейс доступа к ключевым носителям вне зависимости от их типа.

5.7.2. Интерфейсные модули устройств хранения ключевой информации

Модули обеспечивают реализацию доступа к конкретным типам ключевых носителей и считывателей:

fat12.dll - к дисководу и дискете 3.5"

reg.dll - к системнному реестру и ключам в них

accord.dll - к ПАК Аккорд-АМДЗ

sable.dll - к электронному замку "Соболь"

dallas.dll - к считывателю Touch-memory Dallas

ric.dll - к смарткарте РИК и Оскар

emv.dll - к смарткарте MPCOS EMV/3DES

hs.dll - к электронному ключу eToken

pcsc.dll - к считывателям смарткарт и eToken, поддерживающим интерфейс PC/SC

ds199x.dll - к таблеткам DS1996, DS1995.

5.7.3. Библиотека поддержки доступа к ключевым носителям

Библиотека **cpsuprt.dll** обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей.

5.7.4. Модуль ASN1

Поддерживает функции преобразования структур данных в машинно-независимое представление.

5.7.5. Использование ключей реестра Windows

Установка программного обеспечения должна производится пользователем с правами администратора. При этом программа установки требует доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE - полный доступ;
- HKEY_CLASSES_ROOT - полный доступ.

При использовании СКЗИ КриптоПро CSP и создании ключей пользователей без использования флага CRYPT_LOCALMACHINE требуется доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE - чтение, перечисление;
- HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Settings\USERS - создание подключей, чтение, перечисление;
- HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Settings\USERS\SID - полный доступ; SID - SID пользователя.

При использовании СКЗИ и создании ключей с использованием флага CRYPT_LOCALMACHINE дополнительно требуется доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings - полный доступ.

Для изменения конфигурации СКЗИ КриптоПро CSP с использованием панели управления (Control Panel), кроме того, требуется полный доступ к ключу реестра HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro.

Примечание 1. По умолчанию КриптоПро CSP может использовать до 65536 описателей криптографических объектов. Для увеличения этого значения необходимо добавить в реестр (HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters) параметр DWORD, равный требуемому числу описателей, но не более 1048576.

Примечание 2. Допускается хранение закрытых ключей в реестре ОС при условии распространения на HDD или ПЭВМ с HDD требований по обращению с ключевыми носителями, в том числе и после удаления ключей из реестра.

6. Криптографический интерфейс CryptoAPI

Криптографический интерфейс CryptoAPI позволяет:

1. Обеспечить прикладному уровню доступ к криптографическим функциям для генерации ключей, формирования/проверки электронной цифровой подписи, шифрования/расшифрования данных в условиях изолирования прикладного уровня от уровня реализаций криптографических функций. Приложениям и прикладным программистам не нужно детально вникать в особенности реализации того или иного алгоритма или изменять в зависимости от алгоритма прикладные программы.

2. Обеспечить одновременное использование разных алгоритмов и различных их реализаций как программных, так и аппаратных.

Общая архитектура криптографических функций показана на рис. 1.

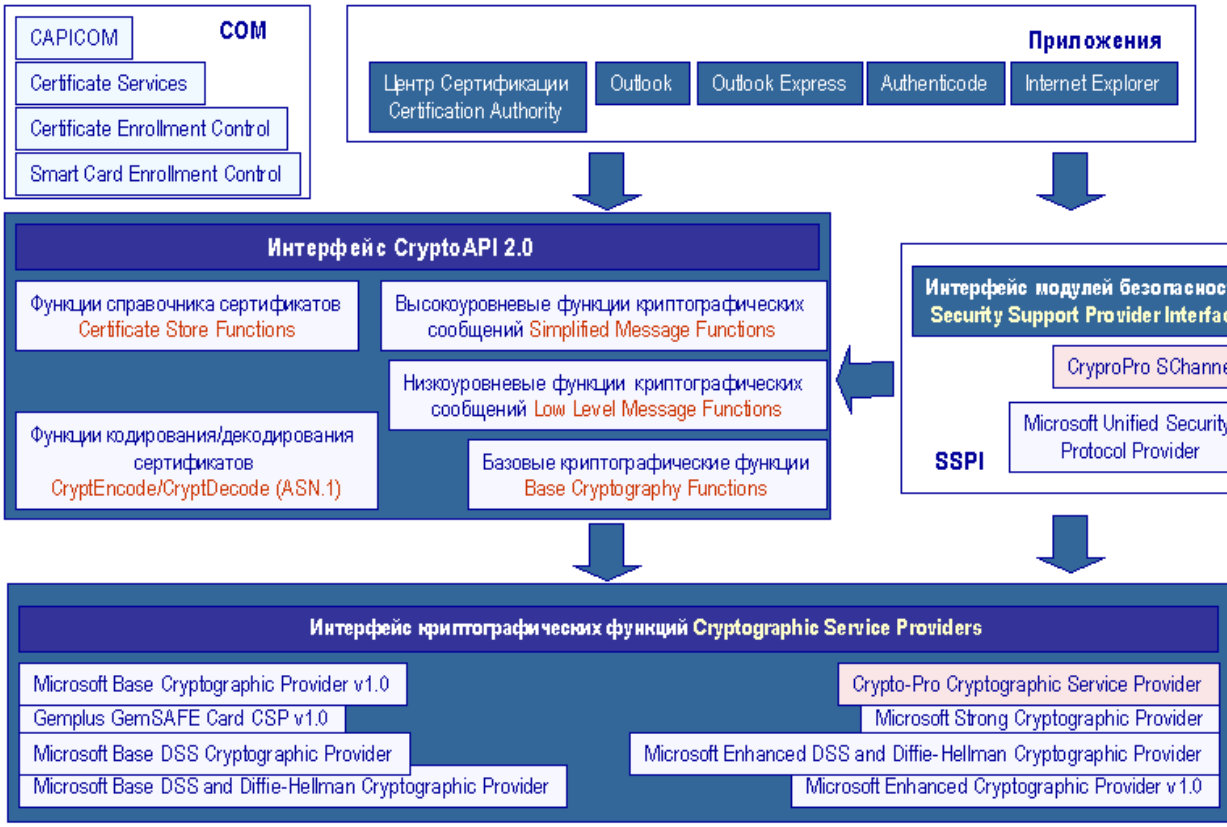


Рис. 1. Архитектура криптографических функций в ОС Windows

Общая архитектура CryptoAPI 2.0 представлена пятью основными функциональными группами:

Базовые криптографические функции

К базовым функциям относятся:

- функции инициализации (работы с контекстом). Эти функции предоставляют приложению возможность выбрать определенный криптопровайдер по типу имени или по требуемой функциональности;

- функции генерации ключей. Эти функции предназначены для формирования и хранения крипто-графических ключей различных типов;

- функции обмена ключами. Эти функции предназначены для того, чтобы приложения могли обмениваться различными типами ключевой информации для обеспечения взаимодействия между собой;

- функции кодирования/декодирования. Данные функции предназначены для преобразования (кодирования) из внутреннего представления объектов, используемых в CryptoAPI, во внешнее представление и обратно. В качестве внешнего представления объектов используется формат ASN.1 (Abstract Syntax Notation One), определенный серией рекомендаций X.680. К этой же группе функций относится набор функций, позволяющих расширить функциональность CryptoAPI путем реализации и регистрации собственных типов объектов;

- функции работы со справочниками сертификатов. Эта группа функций предназначена для хранения и обработки сертификатов в различных типах справочников. Причем в качестве справочника могут использоваться самые различные типы хранилищ: от простого файла до LDAP;

- высокоуровневые функции обработки криптографических сообщений. Эта группа функций (Simplified Message Functions) в первую очередь предназначена для использования в прикладном ПО. С помощью этих функций можно

- Зашифровать/расшифровать сообщение от одного пользователя к другому.

- Подписать данные.

- Проверить подпись данных.

Эти функции (так же как и функции низкого уровня) оперируют сертификатами открытых ключей X.509 для адресации отправителя/получателя данных. В качестве формата данных, формируемых функциями, используется формат PKCS#7 (RFC 2315) или CMS (RFC 2630) в Windows 2000.

- низкоуровневые функции обработки криптографических сообщений. Данная группа функций (Low Level Message Functions) предназначена для аналогичных целей, что и группа высокоуровневых функций, но обладает большей функциональностью и требует от прикладного программиста более детальных знаний в области прикладной криптографии.

7. Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 9 документа ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть и документа ЖТЯИ.00050-03 90 05. Крипто Про CSP. Руководство программиста.

8. Требования по организационно-техническим и административным мерам обеспечения эксплуатации СКЗИ

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме разделов 15 и 16 документа ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

8.1. Требования по подключению СКЗИ для работы по общедоступным каналам передачи данных

При подключении СКЗИ к общедоступным каналам передачи данных должна быть обеспечена безопасность защищенной связи. При этом должны быть определены:

- Порядок подключения СКЗИ к каналам.
- Выделено лицо, ответственное за безопасность работы по общедоступным каналам.
- Разработан типовой регламент защищенной связи, включающий:
  - политику безопасности защищенной связи.
  - допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных.
  - перечень допустимых сетевых протоколов.
  - защиту сетевых соединений (перечень допустимых сетевых экранов).
  - система и средства антивирусной защиты.

Порядок подключения СКЗИ к каналам связи должен быть определен эксплуатирующей организацией.

Лицом, ответственным за безопасность работы СКЗИ по общедоступным каналам, как правило, должен быть администратор безопасности.

Перечень штатных средств ОС, может включаться администратором в типовой регламент без проведения дополнительных исследований по оценке их влияния на СКЗИ. При этом должны выполняться:

1. своевременное обновление программных средств, включенных в состав регламента.
2. контроль среды функционирования СКЗИ.
3. определение и контроль за использованием сетевых протоколов.
4. соблюдение правил пользования СКЗИ и средой функционирования СКЗИ.

При использовании СКЗИ с другими стандартными программными средствами возможность подключения СКЗИ к общедоступным каналам передачи данных должна быть определена только после проведения дополнительных исследований с оценкой невозможности негативного влияния нарушителя на функционирование СКЗИ, использующего возможности общедоступных каналов.

9. Требования по защите от НСД

СКЗИ КриптоПро CSP в варианте исполнения 1 (класс защиты КС1) при условии выполнения требований настоящего Руководства обеспечивают защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

СКЗИ КриптоПро CSP в варианте исполнения 2 (класс защиты КС2) с ПАК защиты от НСД "Соболь" либо "Аккорд АМДЗ" при условии выполнения настоящих Правил обеспечивают защиту конфиденциальной информации также от внутреннего нарушителя, не являющегося пользователем средств вычислительной техники, на которых реализованы СКЗИ и ПКЗИ, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

Запрещается использование СКЗИ КриптоПро CSP в случае обнаружения отказа оборудования либо программного обеспечения ПАК защиты от НСД.

9.1. Организационно-технические меры защиты от НСД

Должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1. В системе регистрируется один пользователь с именем root, обладающий правами администратора, на которого возлагается обязанность конфигурировать ОС Windows, настраивать безопасность ОС, а также конфигурировать ПЭВМ, на которую установлена ОС Windows.
2. Для администратора выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 6 символов, среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц, доступ к паролю должен быть обеспечен только пользователю root.
3. Всем пользователям, зарегистрированным в ОС Windows, администратор в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС Windows, не являющийся администратором, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему администратором.
4. На компьютере устанавливается только одна ОС Windows. Не используют нестандартные, измененные или отладочные версии ОС

Windows такие, например, как Debug/Checked Build. На всех HDD должна быть установлена файловая система NTFS.

5. Права доступа к каталогам %Systemroot%\System32\ Config, %Systemroot%\System32\SPOOL, %Systemroot%\Repair, %Systemroot%\COOKIES, %Systemroot%\FORMS, %Systemroot%\HISTORY, %Systemroot%\SENDTO, %Systemroot%\PROFILES, %Systemroot%\OCCASHE, \TEMP, а также файлам boot.ini, autoexec.bat, config.sys, ntdetect.com и ntldr должны быть установлены в соответствии с политикой безопасности, принятой в организации
6. Должны быть установлены ограничения на доступ пользователей к системному реестру в соответствии с принятой в организации политикой безопасности, что реализуется при помощи ACL или установкой прав доступа при наличие NTFS.
7. Должна быть исключена возможность удаленного редактирования системного реестра.
8. Должна быть проведена установка SECURITY_ATTRIBUTES процессов и потоков в соответствии с требованиями безопасности всей системы в целом.
9. Если нет необходимости, не следует использовать протокол SMB. В случае необходимости использования протокола SMB параметры EnableSecuritySignature (REG_DWORD) и RequareSecuritySignature(REG_DWORD) в ключе HKLM\System\CurrentControlSet \Services\LanManServer\Parametrs должны быть установлены со значениями 1.

5. У группы Everyone должны быть удалены все привилегии.
6. Должен быть переименован пользователь Administrator.
7. Должна быть отключена учетная запись для гостевого входа (Guest).
8. Должно быть исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке.
9. Должно быть ограничено с учетом выбранной в организации политики безопасности использование пользователями сервиса Scheduler.
10. Должен быть отключен сервис DCOM.
11. Должны быть отключены сетевые протоколы, не используемые на данной ПЭВМ.\
12. В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть исключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети.
13. Должна быть исключена возможность сетевого администрирования для всех, включая группу Administrators.
14. Должен быть закрыт доступ ко всем не используемым портам.
15. Должны включаться фильтры паролей, устанавливаемые вместе с пакетами обновлений ОС Windows.
16. Должны быть исключены исполнение и открытие файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов.
17. Должны быть удалены все общие ресурсы на ПЭВМ с установленным СКЗИ «КриптоПро CSP» (в том числе и создаваемые по умолчанию при установке ОС Windows), которые не используются. Права доступа к используемым общим ресурсам должны быть заданы в соответствии с политикой безопасности принятой в организации.
18. После установки операционной системы из каталога %Systemroot%\System32\Config должен быть удален файл sam.sav.
19. Должны использоваться наиболее защищенные протоколы аутентификации, реализованные в Windows, если функционирование СКЗИ не предусматривает применение других протоколов.

20. По возможности следует применять самые сильные шаблоны безопасности (Templates).
21. Должна быть разработана система назначения и смены паролей.
22. Должно быть запрещено использование функции резервного копирования паролей.
23. Должны быть отключены режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей.
24. Должна быть отключена возможность удаленного администрирования ПЭВМ с установленным СКЗИ «КриптоПро CSP».
25. Должно быть ограничено количество неудачных попыток входа в систему, в соответствие с политикой безопасности, принятой в организации. Рекомендуется блокировать систему после трех неудачных попыток.
26. Должны использоваться система аудита в соответствие с политикой безопасности, принятой в организации, и организован регулярный анализ результатов аудита.
27. Должен проводиться регулярный просмотр сообщений в журнале событий Event viewer.
28. ОС Windows должна быть настроена на завершение работы при переполнении журнала аудита.
29. Должна быть обеспечена невозможность модификации ОС Windows через общедоступные каналы передачи данных (Windows Update, Remote Assistance, и т.п.).
30. После инсталляции ОС Windows должен быть установлен последний официальный Service Pack от фирмы Microsoft, существующий на момент установки ОС.
31. Должны использоваться подписанные драйверы.
32. На все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System).
33. Должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию.

9.2. Настройка системного реестра ОС Windows при установке СКЗИ

На ПЭВМ с ОС Windows 2000/2003/Vista/2008/7/2008R2/8/2012 при установке СКЗИ необходимо провести настройку системного реестра:

- в ключе

  HKLM\System\CurrentControlSet\Control\LSA,

  установить параметр RestrictAnonymous (REG_DWORD) со значением 1 для исключения доступа анонимного пользователя (null-session) к списку разделяемых ресурсов, а также для исключения доступа к содержимому системного реестра;
- для исключения утечки информации при передаче данных по именованному каналу \\server\PIPE\SPOOLSSудалить имя SPOOLSS из ключа HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes;
- в ключе

  HKLM\System\CurrentControlSet\Services\LanManServer\Parameters

  установить параметры AutoShareWks и AutoShareServer, имеющие тип

REG_DWORD, со значением 0 для запрета автоматического создания скрытых совместных ресурсов;

- в ключе

  HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

  установить параметр CashedLogonCount (REG_DWORD) со значением 0 для отключения кэширования паролей последних десяти пользователей, вошедших в систему;

- в ключе

  HKLM\System\CurrentControlSet\Services\Eventlog\<LogName>

  (LogName – имя журнала для которого следует ограничить доступ пользователям группы Everyone) установить параметр RestrictGuestAccess (REG_DWORD) со значением 1 для исключения доступа группы Everyone к системному журналу и журналу приложений;

- в ключе HKLM\System\CurrentControlSet\Control\SessionManager\MemoryManagment установить параметр ClearPageFileAtShutDown (REG_DWORD) со значением 1 для включения механизма затирания файла подкачки при перезагрузке;

- в ключе HKLM\System\CurrentControlSet\Control\SecurePipeServers\ установить в соответствии с политикой безопасности принятой в организации разрешения на доступ к параметру winreg для ограничения удаленного доступа к реестру;

- в ключе

  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\

  установить параметр AllocateFloppies (REG_SZ) со значением 1 для исключения параллельного использования дисковода для гибких дисков;

- в ключе HKLM\System\CurrentControlSet\Control\Lsa установить параметр AuditBaseObjects (REG_DWORD) со значением 1 для включения аудита на базовые объекты системы;

- в ключе HKLM\System\CurrentControlSet\Control\Lsa установить параметр FullPrivilegeAuditing (REG_BINARY) со значением 1 для включения аудита привилегий;

- для исключения передачи пароля пользователей по сети в открытом виде (ОС Windows 2000) в ключе HKLM\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters установить параметр EnablePlainTextPassword (REG_DWORD) со значением 0.

9.3. Использование СКЗИ со стандартными программными средствами СФК

Программное обеспечение СКЗИ ЖТЯИ.00050-03 позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509 с различным программным обеспечением Microsoft:

Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows 2000 Server, Advanced Server, Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Server, Windows 2012 Server.

Электронная почта - MS Outlook (Office 2013, Office 2010, Office 2007, Office 2003, Office XP, Office 2000).

Электронная почта - Microsoft Outlook Express в составе Internet Explorer.

Microsoft Word, Excel, Info Path из состава Microsoft Office 2003, 2007.

Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.

Службы терминалов для Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Server, Windows 2012 Server (включая шлюз служб терминалов).

Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – web-сервер IIS, TLS-сервер, TLS-клиент (IE).

- SQL-сервер.
- ISA/TMG сервер.
- Сервер терминалов и клиент (RDP).
- Средства функционирования комплекса разработки

ООО «КРИПТО-ПРО» Крипто-Про УЦ, КриптоПро OCSP, КриптоПро TSP, КриптоАРМ, CryptCP, Клиент КриптоПро HSM.

9.4. Требования по организации СКЗИ сетевого подключения к корпоративным сетям и сетям общего доступа.

При подключении СКЗИ к общедоступным каналам передачи данных должна быть обеспечена безопасность защищенной связи. При этом должны быть определены:

- Порядок подключения СКЗИ к каналам.
- Выделено лицо, ответственное за безопасность работы по общедоступным каналам.
- Разработан типовой регламент защищенной связи, включающий:
  - политику безопасности защищенной связи.
  - допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных.
  - перечень допустимых сетевых протоколов.
  - защиту сетевых соединений (перечень допустимых сетевых экранов).
  - система и средства антивирусной защиты.

Порядок подключения СКЗИ к каналам связи должен быть определен эксплуатирующей организацией.

Лицом, ответственным за безопасность работы СКЗИ по общедоступным каналам, как правило, должен быть администратор безопасности.

Перечень штатных средств ОС, может включаться администратором в типовой регламент без проведения дополнительных исследований по оценке их влияния на СКЗИ. При этом должны выполняться:

- своевременное обновление программных средств, включенных в состав регламента.
- контроль среды функционирования СКЗИ.
- определение и контроль за использованием сетевых протоколов.
- соблюдение правил пользования СКЗИ и средой функционирования СКЗИ.

При использовании СКЗИ с другими стандартными программными средствами возможность подключения СКЗИ к общедоступным каналам передачи данных должна быть определена только после проведения дополнительных исследований с оценкой невозможности негативного влияния нарушителя на функционирование СКЗИ, использующего возможности общедоступных каналов.

10. Требования по криптографической защите

- Должны выполняться требования по криптографической защите разделов 15 и 16 и документа ЖТЯИ.00050-03 90 02 в части, касающейся ОС Windows.
- Перед началом работы должен быть проведен контроль целостности.
- Контролем целостности должны быть охвачены файлы:

Windows 2000/2003 32-bit:

- accord.dll, apmdz.dll, bio.dll, charismathics.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpdrvlib.sys, cpet.dll, cpExSec.dll, cpext.dll, cpintco.dll, cpkdc.dll, cpkrb.dll, cplicmgmt.dll, cpmail.dll, cpMSO.dll, cpoutlm.dll, cprastls.dll, cprdr.dll, cprevchk.dll, cprndm.dll, CProCtrl.sys, CProDs64.dll.IA, CProDspr.dll.IA, cpschan.dll, cpsecur.dll, cpssl.dll, cpsslsdk.dll, spsspap.dll, cpsuprt.dll, cpui.dll, cpverify.exe, cpwinet.dll, cpXML5.dll, csptest.exe, dallas.dll, detoured.dll, ds199x.dll, dsrf.dll, emv.dll, esmarttoken.dll, etok.dll, fat12.dll, genkpim.exe, inpapspot.dll, isbc.dll, jcard.dll, pcsc.dll, pkimgmt.dll, pkivalidator.dll,reg.dll, reprovmgmt.dll, ric.dll, rtsupcp.dll, sable.dll, setuptest.exe, snet.dll, usbccid.sys, winlogonmgmt.dll, wipefile.exe, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.

Дополнительно для Windows Vista/7/2008/2008R2/8/2012

- cpcng.dll, cpenroll.dll, cpksp.sys, cryptsp.dll, sspicli.dll.

Windows 2003 Itanium (x86)

- bio.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpenroll.dll, cpExSec.dll, cpext.dll, cpintco.dll, cpmail.dll, cpMSO.dll, cpoutlm.dll, cprdr.dll, cprevchk.dll, cprndm.dll, cpschan.dll, cpsecur.dll,cpssl.dll, cpsslsdk, cpsspap.dll, cpsuprt.dll, cpui.dll, cpverify.exe, cpwinet.dll, cpXML5.dll, csptest.exe, detoured.dll, dsrf.dll, emv.dll, fat12.dll, genkpim.exe, pcsc.dll, reg.dll, ric.dll, setuptest.exe, snet.dll, wipefile.exe, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.

Windows 2003 Itanium (ia64)

- bio.dll, cpadvai.dll, cpcertocm.dll, cpcng.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpdrvlib.sys, cpext.dll, cpintco.dll, cpmail.dll, cprdr.dll, cprevchk.dll, cprndm.dll, CProCtrl.sys, CProDs64.dll, CProDspr.dll, cpschan.dll, cpsecur.dll, cpsuprt.dll, cpui.dll, cpverify.exe, cpwinet.dll, csptest.exe, detoured.dll, dsrf.dll, emv.dll, fat12.dll, pcsc.dll, reg.dll, ric.dll, setuptest.exe, snet.dll, wipefile.exe; cpssl.dll, cpsspap.dll, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.

Windows 2003 64-bit (x86)

- accord.dll, apmdz.dll, bio.dll, charismathics.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpenroll.dll, cpet.dll, cpExSec.dll, cpext.dll, cpintco.dll, cpkrb.dll, cpkdc.dll, cpkrb.dll, cplicmgmt.dll, cpmail.dll, cpMSO.dll, cpoutlm.dll, cprastls.dll, cprdr.dll, cprndm.dll, cprevchk.dll, cpschan.dll, cpsecur.dll,cpsuprt.dll, cprndm.dll, cpsslsdk.dll, cpui.dll, cpverify.exe, cpwinet.dll, cpXML5.dll, csptest.exe, dallas.dll, detoured.dll, ds199x.dll, dsrf.dll, emv.dll, esmarttoken.dll, etok.dll, fat12.dll, genkpim.exe, inpaspot.dll, isbc.dll, jcard.dll, pcsc.dll, pkimgmt.dll, pkivalidator.dll, reg.dll, reprovmgmt.dll, ric.dll, rtsupcp.dll, sable.dll, setuptest.exe, snet.dll, winlogonmgmt.dll, wipefile.exe; cpssl.dll, cpsspap.dll, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.

Дополнительно для Windows Vista/7/2008/2008R2/8/2012

- cpcng.dll, cpenroll.dll, cryptsp.dll, sspicli.dll.

Windows 2003 64-bit (amd64)

- accord.dll, apmdz.dll, bio.dll, charismathics.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpenroll.dll, cpet.dll, cpext.dll, cpintco.dll, cpkrb.dll, cpkdc.dll, cpkrb.dll, cplicmgmt.dll, cpmail.dll, cpoutlm.dll, cprastls.dll, cprdr.dll, cprevchk.dll, cprndm.dll, CProDs64.dll, CProDspr.dll, cpschan.dll, cpsecur.dll,cpsuprt.dll, cprndm.dll, cpui.dll, cpverify.exe, cpwinet.dll, csptest.exe, dallas.dll, detoured.dll, ds199x.dll, dsrf.dll, emv.dll, esmarttoken.dll, etok.dll, fat12.dll, genkpim.exe, inpaspot.dll, isbc.dll, jcard.dll, pcsc.dll, pkimgmt.dll, pkivalidator.dll, reg.dll, reprovmgmt.dll, ric.dll, rtsupcp.dll, sable.dll, setuptest.exe, snet.dll, winlogonmgmt.dll, wipefile.exe; cpssl.dll, cpsspap.dll, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.

Дополнительно для Windows Vista/7/2008/2008R2/8/2012

- cpcng.dll, cpenroll.dll, cpksp.sys, cryptsp.dll, sspicli.dll.

Для добавления под контроль целостности следующих файлов:

- crypt32.dll
- inetcomm.dll
- wininet.dll
- schannel.dll
- winscard.dll
- cryptsp.dll
- sspicli.dll
- kerberos.dll

необходимо reg-файл данного вида импортировать в реестр.

Для 64разрядных систем:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity]
"HaltFileCorrupt"=dword:00000000
…
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity\
system\{название библиотеки}]
"Path"="C:\\Windows\\SysWOW64\\{название библиотеки}"
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity\
system\{название библиотеки}.64]
"Path"="C:\\Windows\\system32\\{название библиотеки}"
…
Для 32разрядных систем необходима только одна строка для каждой библиотеки:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity\
system\{название библиотеки}]
"Path"="C:\\Windows\\system32\\{название библиотеки}"

Затем необходимо в командной строке от имени администратора выполнить команду:
                        cpverify -rm system
```

Приложение 1. Контроль целостности программного обеспечения

Модуль **cpverify.exe** позволяет осуществлять контроль целостности установленного программного обеспечения. Контроль целостности файлов осуществляется при загрузке файла на исполнение (и периодически во время выполнения) или при ручном запуске программы контроля целостности (см. опцию **–rv** ниже).

При помощи перечисленных ниже опций модуль **cpverify.exe** может быть использован для следующих контрольных целей:

- **cpverify –r2x out_file [xmlcatname]** - формирование xml-файла с именем **out_file**, содержащего список файлов, находящихся в каталоге **xmlcatname** под контролем целостности;
- **cpverify –x2r in_file [xmlcatname]** - установление под контроль целостности файлов из каталога **xmlcatname**, перечисленных в xml-файле с именем **in_file**;
- **cpverify –xv in_file [xmlcatname]** - проверка целостности файлов из каталога **xmlcatname**, перечисленных в xml-файле с именем **in_file**;

- **cpverify –rv [xmlcatname]** - проверка целостности файлов из каталога **xmlcatname**;
- **cpverify –xm in_file out_file [xmlcatname]** - вычисление значения хеш-функции для каждого из файлов, содержащихся в каталоге **xmlcatname** и перечисленных в xml-файле с именем **in_file**, и запись полученных значений в xml-файл с именем **out_file**. Текущее значение хеш-функций при этом заменяется на вновь посчитанное.
- **cpverify –rm [xmlcatname]** - вычисление значения хеш-функции для каждого из файлов, содержащихся в каталоге **xmlcatname**. Текущее значение хеш-функций при этом заменяется на вновь посчитанное.
- **cpverify –d [catname]** – удаление каталога **catname** из списка контрлируемых файлов.
- **cpverify –mk filename –** вычисление значения хеш-функции для файла с именем **filename**.
- Во всех перечисленных выше случаях, если не указано имя каталога **xmlcatname**, то принимается имя каталога **cpcsp,** используемое csp для контроля целостности входящих в его состав модулей. Список контролируемых модулей зависит от исполнения и может быть получен при помощи команды **cpverify –r2x in_file cpcsp**.

Для того, чтобы поставить под контроль целостности установленное программное обеспечение, нужно выполнить следующую последовательность действий:

1. Создать xml-файл, содержащий список устанавливаемых под контроль целостности файлов. Данный xml-файл должен иметь следующую структуру:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<CProIntegrity>
        <catalog name="TestControl">
<entry name="calc.exe">
    <Path>C:\WINDOWS\system32\calc.exe</Path>
    </entry>
<entry name=" verifier.exe">
    <Path>C:\WINDOWS\system32\verifier.exe</Path>
    </entry>
        </catalog>
</CProIntegrity>
```

2. Запустить модуль **cpverify –xm in_file out_file TestControl**, указав в качестве параметра **in_file** имя созданного xml-файла. Результатом работы модуля будет являться xml-файл с именем **out_file**, содержащий вычисленные значения хеш-функции для перечисленных в **in_file** файлов и имеющий следующую структуру:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<CProIntegrity>
        <catalog name="TestControl">
<entry name="calc.exe">
<Path>C:\WINDOWS\system32\calc.exe</Path>
<Tag>0941E781760004B3AEE0DF6BC53CF460A6B137083948C0BF6D5DD153D2
55FE86</Tag>
    </entry>
<entry name=" verifier.exe">
<Path>C:\WINDOWS\system32\verifier.exe</Path>
<Tag>A9CD3307A16F76DCE4E6E3A67ED7359658202C44D9812C532FCD8E07B1
D7A7D6</Tag>
```

```
        </entry>
                </catalog>
</CProIntegrity>
```

3. Установить под контроль целостности файлы, для которых было вычислено значение хеш-функции, используя модуль **cpverify –x2r in_file TestControl**, где параметром **in_file** является xml-файл, полученный в результате вычисления значения хеш-функции в пункте 2.

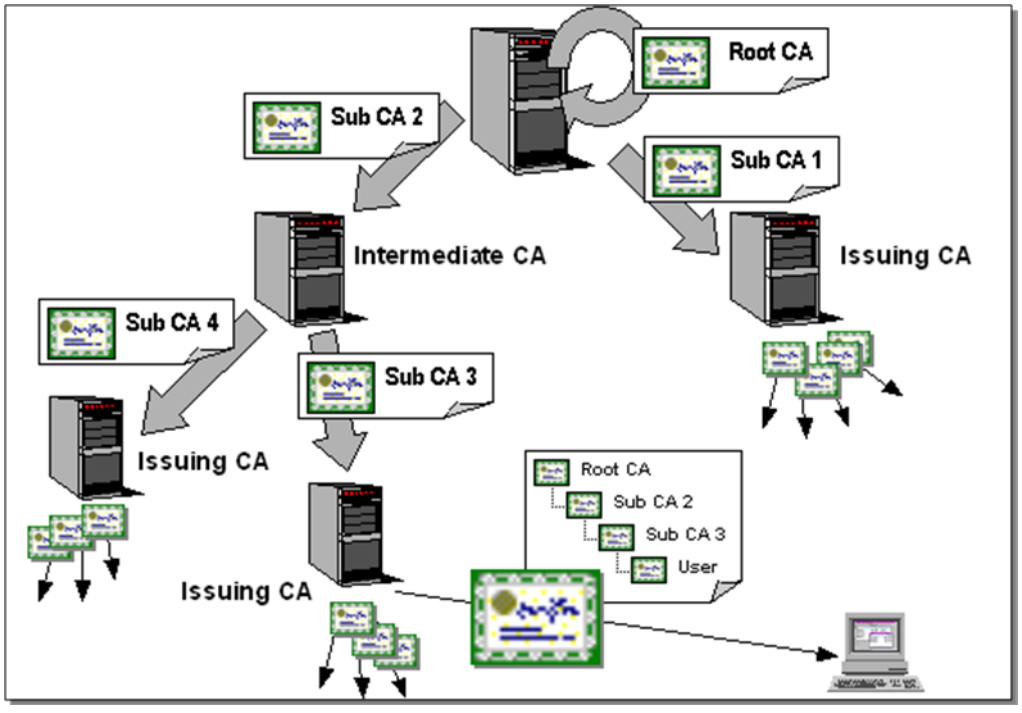
Приложение 2. Службы сертификации операционной системы Windows

Ведущие мировые производители системного и прикладного программного обеспечения активно интегрируют решения, основанные на Инфраструктуре открытых ключей в операционные системы и приложения. Ярким примером является операционная система Windows, полностью поддерживающая ИОК.

В операционной системе Microsoft Windows в полном объеме реализована Инфраструктура открытых ключей. Эта инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими.

Инфраструктура открытых ключей предполагает иерархическую модель построения центров сертификации. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом продуктов и центров сертификации. Простейшая форма иерархии состоит из одного центра сертификации, а в общем случае – из множества с явно определенными отношениями родительский-дочерний.

Инфраструктура открытых ключей, реализованная в операционной системе Microsoft Windows 2000/2003 полностью поддерживает и позволяет создать иерархическую модель центров сертификации.



В состав служб сертификации операционной системы Windows 2000 входят следующие службы и компоненты.

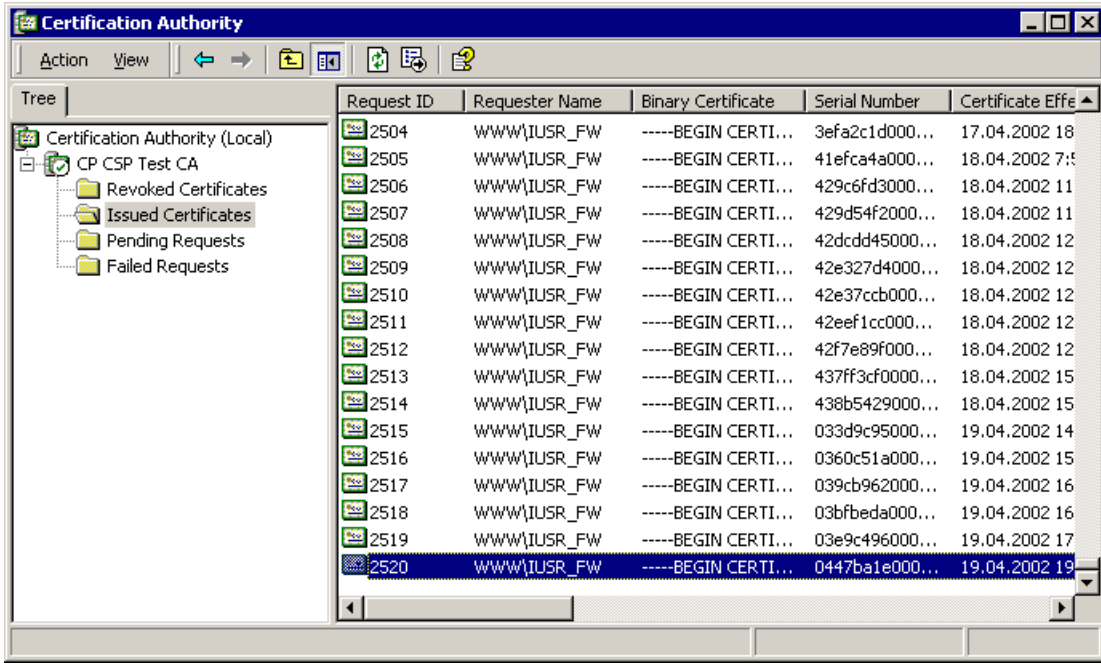
Сервис сертификации

Сервис сертификации предоставляет набор служб для выпуска, управления и использования сертификатов открытых ключей в защищенных технологиях и приложениях, использующих ИОК. Сервис сертификации выполняет основную

роль в управлении безопасностью технологий и приложений и обеспечивает процесс достоверного и конфиденциального обмена информацией.

Консоль центра сертификации

Консоль центра сертификации является рабочим местом администратора безопасности, позволяющим управлять сертификатами открытых ключей.



Средства расширения функциональности сервиса сертификации

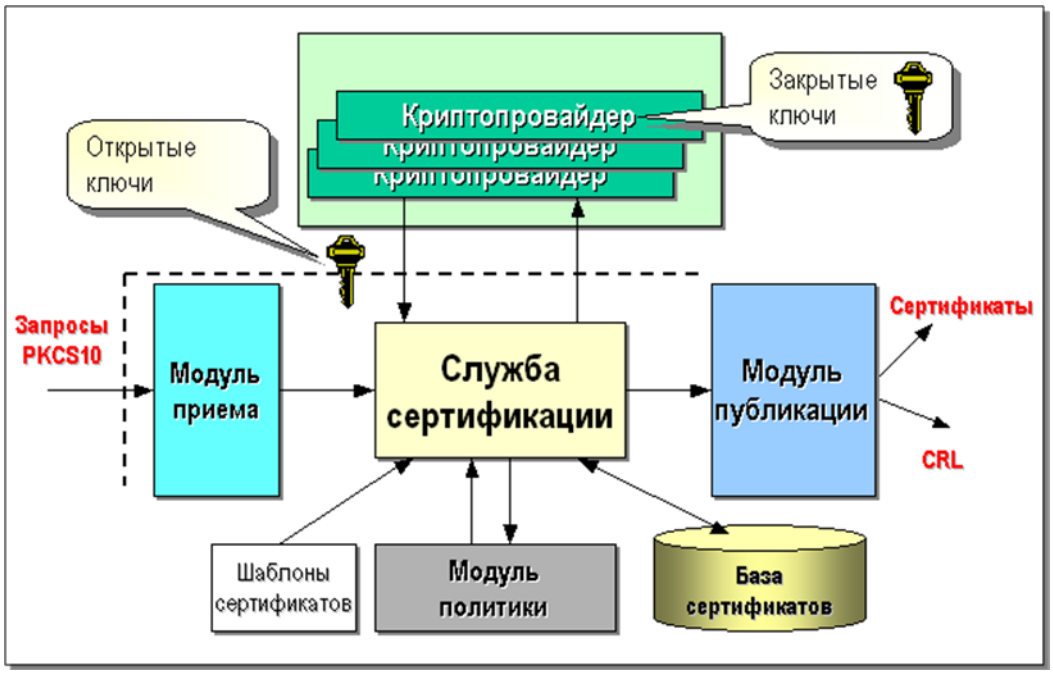
Средства расширения функциональности сервиса сертификации предоставляют набор методов, позволяющих изменять и развивать функциональность стандартного сервиса сертификации для удовлетворения потребности конкретной прикладной системы или технологии. Эти средства позволяют интегрировать сервиса сертификации с различными сетевыми справочниками и приложениями, формировать состав сертификатов открытых ключей, модифицировать процесс управления сертификатами.

Клиентские средства взаимодействия со службой сертификации

Клиентские средства предоставляют пользователям различные методы для формирования закрытых ключей, запросов на сертификаты и обработки сертификатов, выпущенных службой сертификации.

Архитектура сервиса сертификации

Архитектура сервиса сертификации представлена на следующем рисунке.



Приложение 3. Управление протоколированием

Для включения/отключения протоколирования для Windows 32[Windows 64] добавляется в реестр:

HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node]Crypto Pro\Cryptography\CurrentVersion\debug\

DWORD параметр ***cpcsp*** для определения уровня протокола

DWORD параметр ***cpcsp_fmt*** для определения формата протокола

Значением параметра уровнь протокола является битовая маска:
N_DB_ERROR = 1 # сообщения об ошибках
N_DB_LOG = 8 # сообщения о вызовах

Значением параметра формат протокола является битовая маска:
DBFMT_MODULE = 1 # выводить имя модуля
DBFMT_THREAD = 2 # выводить номер нитки
DBFMT_FUNC = 8 # выводить имя функции
DBFMT_TEXT = 0x10 # выводить само сообщение
DBFMT_HEX = 0x20 # выводить HEX дамп
DBFMT_ERR = 0x40 # выводить GetLastError

Лист регистрации изменений

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводи-тельного документа, дата	Подпись	Дата
	измененных	замененных	новых	аннулиро-ванных					