127 018, Москва, Сущевский вал, 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

Описание реализации

ЖТЯИ.00050-03 90 01

Листов 23

2013

Содержание

Аннотация

Настоящий документ содержит описание реализации средства криптографической защиты информации КриптоПро CSP версии 3.6.1 (СКЗИ ЖТЯИ.00050-03) и сведения о текущем состоянии продукта.

1. Назначение СКЗИ

СКЗИ ЖТЯИ.00050-03 обеспечивает выполнение следующих защитных функций:

- авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки (с использованием сертификатов стандарта X.509 Удостоверяющего центра) электронной подписи в соответствии с отечественными стандартами:

  ГОСТ Р 34.10-2001. *"Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".*

  ГОСТ Р 34-11-94. *"Информационная технология. Криптографическая защита информации. Функция хэширования"*.

- обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с отечественным стандартом ГОСТ 28147-89 *"Системы обработки информации. Защита криптографическая"*;

- контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;

- управления ключевыми элементами системы в соответствии с регламентом;

- обеспечение аутентификации связывающихся сторон, конфиденциальности и целостности пересылаемой информации с использованием сертификатов стандарта X.509;

- установление аутентичного защищенного соединения с использованием протокола КриптоПро TLS;

- защита IP-соединений с использованием протоколов КриптоПро IKE, КриптоПро ESP;

- обеспечение конфиденциальности и контроля целостности и авторизация файлов и информационных сообщений;

- обеспечение аутентификации;

- обеспечение аутентификация пользователя в домене Windows.

Примечание. Юридическая значимость электронных документов обеспечивается за счет функционирования СКЗИ и используемого совместно с ним УЦ в соответствии требованиями, предъявляемыми Федеральным законом «об электронной подписи». При автоматическом создании и проверке электронная подпись и сертификат ключа проверки электронной подписи, сформированный УЦ, удовлетворяют требованиям данного закона для квалифицированной электронной подписи (Статьи 5, 12 закона об ЭП).

Для обеспечения создания квалифицированной подписи в среде функционирования комплекса средства ЭП должны удовлетворять следующим требованиям Федерального закона «об электронной подписи»:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;
- однозначно показывать, что ЭП создана;

При проверке ЭП средства ЭП должны:

- показывать содержание электронного документа, подписанного ЭП;
- показывать информацию о внесении изменений в подписанный ЭП электронный документ;
- указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

---

2. Программно-аппаратные среды функционирования СКЗИ

СКЗИ ЖТЯИ.00050-03 функционирует в следующих программно-аппаратных средах:

- Windows 2000 (ia32);
- Windows 2003/Vista/2008/7/2008R2/8/2012 (ia32, ia64, x64).
- Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x:
  - CentOS 5/6/7 (ia32, x64)
  - ТД ОС АИС ФССП России (GosLinux) (x86, x64)
  - Fedora 16/17 (ia32, x64)
  - Linpus Lite 1.3 (ia32)
  - Mandriva Server 5 (ia32, x64)
  - Oracle Enterprise Linux 5/6 (ia32, x64)
  - Open SUSE 12 (ia32, x64)
  - Red Hat Enterprise Linux 5/6 (ia32, x64)
  - SUSE Linux Enterprise 11 (ia32, x64)
  - Ubuntu 8.04/10.04/11.04/11.10/12.04 (ia32, x64)
- ALT Linux 5/6 (ia32, x64);
- Red Hat Enterprise Linux Version 3 Update 3 (ia32, x64);
- Debian 6 (ia32, x64);
- FreeBSD 7/8/9 (ia32, x64);
- Solaris 10/11 (sparc, ia32, x64);
- AIX 5/6/7 (Power PC);
- Apple iOS 4.2.1-4.2.10/4.3.1-4.3.5/5.0.1/5.1/5.1.1/6.0/6.0.1/6.0.2/6.1/6.1.2/6.1.3/ /6.1.4/7.0/7.0.1/7.0.2/7.0.3 (ARM);
- Mac OS X 10.6/10.7/10.8 (x64).

3. Исполнения СКЗИ

СКЗИ ЖТЯИ.00050-03 выпускается в пяти исполнениях:

Исполнение 1 класса защиты КС1 выполнено в составе:

криптопровайдер;

криптодрайвер;

модуль сетевой аутентификации (TLS);

модуль аутентификации пользователя в домене Windows (в ОС Windows);

модуль протоколов КриптоПро IKE, КриптоПро ESP (в ОС Windows, Linux);

модуль шифрующей файловой системы КриптоПро EFS (ОС Windows);

модуль поддержки интерфейса Microsoft CNG;

модуль поддержки интерфейса Mozilla NSS;

сервисные модули (cpverify, wipefile, stunnel)

и функционирует в программно-аппаратных средах п.2.

Исполнение 2 класса защиты КС2 выполнено в составе исполнения 1 с добавлением утилиты выработки внешней гаммы, и функционирует в программно-аппаратных средах п.2 за исключением Apple iOS (ARM) и Mac OS X (x64).

Исполнение 3 класса защиты КС3 выполнено в составе:

криптодрайвер;

криптосервис;

модуль сетевой аутентификации (TLS);

модуль аутентификации пользователя в домене Windows
модуль шифрующей файловой системы КриптоПро EFS (ОС Windows);
модуль командной строки;
утилита выработки внешней гаммы;
сервисные программы
и функционирует в программно-аппаратных средах Windows 2003 (платформа ia32, x64).
с пакетом Secure Pack Rus версии 3.0.

Исполнение 4 класса защиты КС3 выполнено в составе:
криптодрайвер;
криптосервис;
модуль сетевой аутентификации (TLS);
модуль аутентификации пользователя в домене Windows;
модуль протоколов КриптоПро IKE, КриптоПро ESP (ОС Windows, Linux);
модуль протокола КриптоПро IPSec;
модуль шифрующей файловой системы КриптоПро EFS (ОС Windows);
модуль командной строки;
утилита выработки внешней гаммы;
сервисные программы
и функционирует в программно-аппаратных средах Windows 2003/7/2008R2 (платформа ia32, x64) с пакетом Secure Pack Rus версии 3.0.

Исполнение 5 класса защиты КС3 выполнено в составе:
криптодрайвер;
криптосервис;
модуль сетевой аутентификации (TLS);
модуль шифрующей файловой системы КриптоПро EFS (ОС Windows);
сервисные программы;
и функционирует в программно-аппаратных средах Windows 2003 (платформа ia32), Windows 2003 (платформа x64) с программным обеспечением СЗИ Secret Net 6.

4. Основные характеристики СКЗИ

4.1. Размеры ключей

Размеры ключей электронной подписи:
- ключ электронной подписи – 256 бит;
- ключ проверки электронной подписи - 512 бит.

Размеры ключей, используемых при шифровании:
- закрытый ключ – 256 бит;
- открытый ключ - 512 бит;
- симметричный ключ – 256 бит.

4.2. Типы ключевых носителей

Используются ключевые носители:
- ГМД 3,5’’;
- USB диски
- электронный ключ с интерфейсом USB (e-Token);
- Смарткарты РИК, Оскар, Магистра

- идентификаторы Touch-Memory DS1995 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь";
- Rutoken;
- Раздел HDD ПЭВМ (в ОС Windows – реестр)

Использование ключевых носителей в зависимости от программно-аппаратной платформы, см. 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 драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

Примечание 2. Допускается хранение закрытых ключей и ключей подписи 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.

5. Реализация КриптоПро CSP

5.1. Структура СКЗИ

Структура СКЗИ КриптоПро CSP v. 3.6.1 (ЖТЯИ.00050-03) представлена на рис. 1.

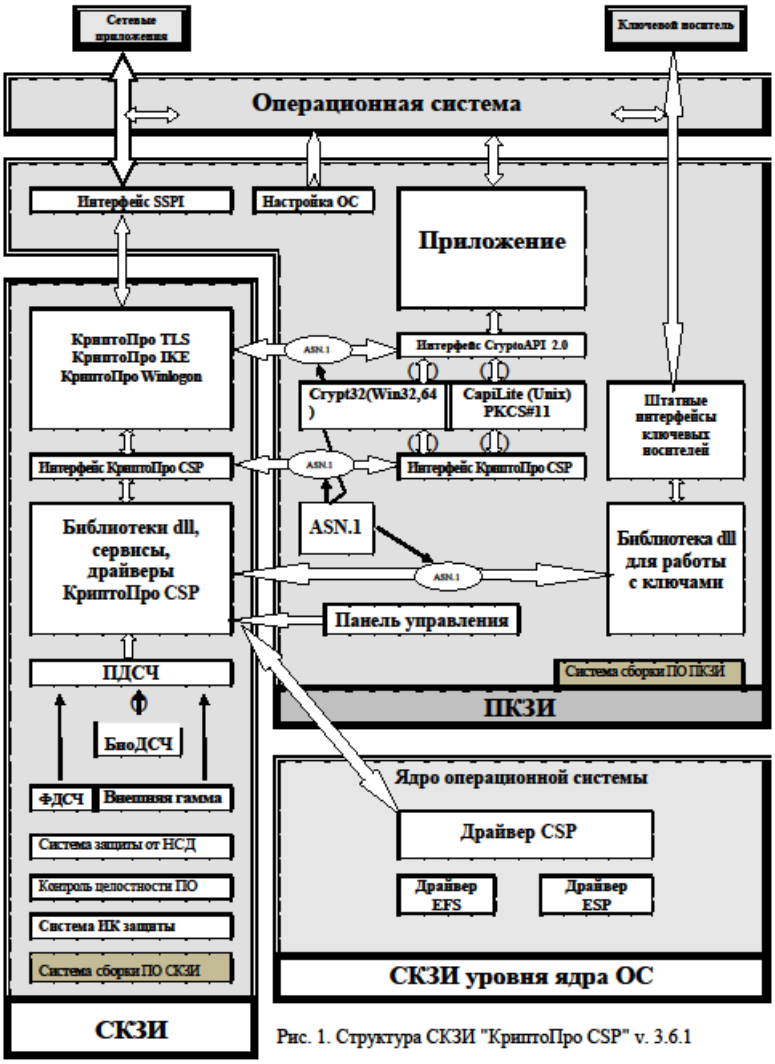


Рис. 1. Структура СКЗИ "КриптоПро CSP" v. 3.6.1

5.2. Состав программного обеспечения СКЗИ

СКЗИ функционирует на одном из двух уровней:

- уровень приложения;
- уровень ядра ОС.

В состав СКЗИ входят:

- Библиотеки dll, сервисы, драйверы КриптоПро CSP.
- Модуль сетевой аутентификации КриптоПро TLS.
- Модуль IKE, ESP для использования в протоколе КриптоПро IPSec.
- Модуль КриптоПро Winlogon.
- Криптографический интерфейс КриптоПро CSP.
- Программный датчик случайных чисел (ПДСЧ) с инсталляцией от физического ДСЧ (ФДСЧ) встраиваемого программно-аппаратного комплекса (ПАК) защиты от НСД, БиоДСЧ, внешней гаммы.
- ПАК защиты от НСД (в исполнениях 2 - 5).
- Контроль целостности программного обеспечения.
- Система инженерно-криптографической защиты.
- Система защиты от НСД (используется опционально).

5.3. Состав SDK СКЗИ

В состав SDK СКЗИ входят документы, описывающие интерфейсы:

- CSP_3_6.chm
- CAPILite_3_6.chm
- SSPI_3_6.chm
- reader_3_6.chm

Примеры:

- rdk
- samples

В состав КриптоПро EFS (ЖТЯИ.00051-01 30 02) входит документация:

- cpefs.chm

В состав КриптоПро IPSec входит документация:

- ikespah.chm

5.4. Состав программной СФК.

В состав ПКЗИ входят компоненты:

- Приложение (Прикладное программное обеспечение, использующее СКЗИ).
- Интерфейс SSPI (подмножество интерфейса криптографических протоколов Secure Support Provider Interface (SSPI, CryptoAPI v. 2.0) для реализации протокола сетевой аутентификации TLS v. 1.0 (под управлением ОС Windows2000/2003/Vista/2008/7/2008R2/8/2012).
- Модули настройки ОС Windows для обеспечения функционирования СКЗИ.
- Интерфейс CryptoAPI 2.0.
- Средства Crypt32(Win32,64) для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс КриптоПро CSP под управлением ОС Windows2000/2003/Vista/2008/7/2008R2/8/2012.
- Средства CapiLite - для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс КриптоПро CSP под управлением ОС семейства UNIX (Linux , FreeBSD, Solaris, AIX).
- Криптографический интерфейс КриптоПро CSP.
- Штатные интерфейсы ключевых носителей.
- ASN.1 - система кодирования/декодирования данных в форматах ASN.1.

Состав модулей СКЗИ и ПКЗИ для соответствующих программно-аппаратных сред конкретизируется в дополнениях ЖТЯИ.00050-03 90 02-01, ЖТЯИ.00050-03 90 02-02, ЖТЯИ.00050-03 90 02-03, ЖТЯИ.00050-03 90 02-04, ЖТЯИ.00050-03 90 02-05, ЖТЯИ.00050-03

90 02-06, ЖТЯИ.00050-03 90 02-07 к документу ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

Основной архитектурной особенностью СКЗИ КриптоПро CSP является то, что ПКЗИ не имеет непосредственного доступа к ключевой и криптографически значимой информации. Все операции с закрытыми и сессионными (симметричными) ключами, незавершенными значениями хэш-функций и т. п. осуществляются через дескрипторы соответствующих объектов; дескриптор объекта не содержит его адрес в явном виде.

6. Применение СКЗИ ЖТЯИ.00050-03

Возможны следующие применения КриптоПро CSP:

1. Применение КриптоПро CSP в составе стандартного программного обеспечения Microsoft и других компаний, использующих криптографический интерфейс в соответствии с архитектурой Microsoft.
2. Встраивание КриптоПро CSP во вновь разрабатываемое или существующее прикладное программное обеспечение.

7. Использование СКЗИ в стандартном программном обеспечении

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, Почта Windows Mail, Live Mail.
- Microsoft Word, Excel, InfoPath из состава Microsoft Office 2003, 2007, 2010 (с помощью плагина КриптоПро Office Signature).
- 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 сервер.
- Сервер TMG
- Сервер UAG.
- Сервер терминалов и клиент (RDP).

Под управлением UNIX-подобных ОС СКЗИ ЖТЯИ.00050-03 КриптоПро CSP используется с программным обеспечением:

- Certmgr (КриптоПро Certmgr).
- CryptCP.
- Apache Trusted TLS (Digt).
- Trusted TLS (Digt).

Российские криптографические алгоритмы и сертификаты открытых ключей X.509 используются с указанным программным обеспечением в соответствии с международными рекомендациями:

- "Using the GOST R 34.10-94, GOST R 34.10-2001 and GOST R 34.11-94 algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile" (**rfc4491**) описывает использование российских криптографических алгоритмов в инфраструктуре открытых ключей интернет (PKIX, Internet X.509 Public Key Infrastructure). В данном документе описаны форматы представления открытых ключей ЭП, используемых для создания сертификатов открытых ключей и списков отозванных сертификатов X.509, идентификаторы алгоритмов, соответствие параметров криптографических алгоритмов их идентификаторам.
- "Additional cryptographic algorithms for use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 algorithms" (**rfc4357)** описывает дополнительные алгоритмы, необходимые для использования ГОСТ 28147-89, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94. В число этих дополнений входят: режимы дополнения данных для блочного шифрования по ГОСТ 28147-89 и CBC, блочное шифрование с зацеплением (режим шифрования CBC), ключевое хэширование (HMAC на базе ГОСТ Р 34.11-94), преобразование ключа и синхропосылки после обработки очередных 1 Кб данных, генерация псевдослучайной последовательности (аналог PRF на базе HMAC), формирование ключа обмена (согласования) на базе ГОСТ Р 34.10-2001, формирование ключа экспорта рабочего ключа, диверсификация ключа, экспорт рабочего ключа на ключе экспорта, экспорт рабочего ключа на ключе обмена, наборы стандартных параметров алгоритмов (например, для шифрования - узел замены, режим шифрования, алгоритм усложнения ключа), задаваемые идентификаторами.
- "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94 and GOST R 34.10-2001 algorithms with the Cryptographic Message Syntax (CMS)" (**rfc4490**) описывает использование российских криптографических алгоритмов в документах, удовлетворяющих стандарту CMS (Cryptographic Message Syntax), в частности, применяемом для обмена защищёнными сообщениями по электронной почте и являющимся стандартом на представление электронного документа в защищенном виде с использованием электронной подписи и шифрования. Для шифрованных сообщений описаны оба варианта: обмен ключами и транспорт ключа (key agreement и key transport).
- Проект "Addition of GOST Ciphersuites to Transport Layer Security (TLS)" (**draft-chudov-cryptopro-cptls-01.txt**) является дополнением к спецификации RFC 2246 в части описания применения российских алгоритмов. Протокол TLS(SSL) широко используется для защиты сетевых соединений, и, в частности, для защищенного доступа к Веб-сайтам (HTTPS). Документ описывает четыре механизма (Cipher Suites), реализующих ключевые протоколы при использовании открытых ключей ГОСТ Р 34.10-2001. Первые два используют шифрование ГОСТ 28147-89 и контроль целостности с помощью имитовставки, третий и четвертый не используют шифрование и контролируют целостность с помощью ключегого хеша (MAC) на основе алгоритма ГОСТ Р 34.11-94.
- Проект "Using algorithms GOST R 34.10-2001, GOST R 34.10-94 and GOST R 34.11-94 for XML Digital Signatures" (**draft-chudov-cryptopro-cpxmldsig-00.txt**) является дополнением к существующему документу, описывающему правила применения ЭП в документах формата XML "XML-Signature Syntax and Processing", принятому консорциумом W3C, в части использования российских алгоритмов электронно-цифровой подписи.

8. Использование СКЗИ с программными продуктами разработки ООО «КРИПТО-ПРО»

Программное обеспечение СКЗИ ЖТЯИ.00050-03 может использоваться с программными продуктами разработки ООО «КРИПТО-ПРО»:

- «КриптоПро УЦ»;
- «КриптоПро OCSP»;
- «КриптоПро TSP»;
- «КриптоАРМ»;
- «CryptCP»;
- «Клиент КриптоПро HSM».

9. Встраивание СКЗИ

Архитектура СКЗИ ЖТЯИ.00050-03 обеспечивает возможность его встраивания в различные программно-аппаратные среды.

СКЗИ может быть использовано прикладным программным обеспечением с помощью загрузки модуля вызовом функции **LoadLibrary()**. Для этих целей в комплект поставки включается документ "ЖТЯИ.00050-03 90 05. КриптоПро CSP. Руководство программиста", описывающий состав функций и тестовое ПО. При такой реализации прикладному ПО доступен лишь ограниченный набор низкоуровневых криптографических функций, соответствующий интерфейсу Microsoft CSP.

При использовании СКЗИ под управлением операционной системы iOS загрузка библиотек при помощи функции LoadLibrary() невозможна. Для этой операционной системы встраивание должно производиться в соответствии с документацией, входящей в состав фреймворка для разработки. Программный интерфейс, предоставляемый СКЗИ под управлением iOS, также описан в документе "ЖТЯИ.00050-03 90 05. КриптоПро CSP. Руководство программиста" и соответствует интерфейсу Microsoft CSP.

10. Использование интерфейса CryptoAPI 2.0.

СКЗИ ЖТЯИ.00050-03 может быть использовано прикладным программным обеспечением (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс **CryptoAPI 2.0 (**описание – в документации **MSDN - Microsoft Developer Network)**. В этом случае способ выбора криптографического алгоритма в прикладном программном обеспечении может определяться информацией, содержащейся в сертификатах открытых ключей X.509.

Использование интерфейса CryptoAPI 2.0 в ОС Windows преследует цели:

- обеспечение для прикладного уровня доступа к криптографическим функциям (генерация ключей, формирование/проверка электронной подписи, шифрование/расшифрование данных). Эта цель достигается путем изолирования прикладного уровня от уровня реализации криптографических функций. При этом прикладным программистам не нужно детально изучать особенности реализации того или иного алгоритма или изменять код в зависимости от алгоритма.
- изолирование прикладного уровня от уровня криптографических функций с возможностью использования разных алгоритмов в различных их реализациях, включая аппаратные.

На Unix-платформах ПКЗИ дополнительно комплектуется модулем capilite, который соответствует подмножеству интерфейса CryptoAPI 2.0 и обеспечивает те же интерфейсные функции в этих ОС, что и в ОС Windows.

10.1. 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 криптографических ключей различных типов.
- **Функции обмена ключами**. Эти функции предназначены для того, чтобы приложения могли обмениваться различными типами ключевой информации для обеспечения взаимодействия между собой.

По своей функциональности базовые функции дублируют низкоуровневый интерфейс CSP.

10.1.1. 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 (Abstracy Syntax Notation One), определенный серией рекомендаций X.680. К этой же группе функций может быть отнесен набор функций, позволяющих расширить функциональность CryptoAPI 2.0 путем реализации и регистрации собственных типов объектов.

10.1.2. Функции работы со справочниками сертификатов

Эта группа функций предназначена для хранения и обработки сертификатов в различных типах справочников. В качестве справочника могут использоваться самые различные типы хранилищ: от файла до LDAP.

10.1.3. Высокоуровневые функции обработки криптографических сообщений

Эта группа функций (Simplified Message Functions) в первую очередь предназначена для использования в прикладном программном обеспечении. С их помощью можно:

- Зашифровать/расшифровать сообщения 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 используется формат PKCS#7 или CMS.

СКЗИ КриптоПро CSP поддерживает сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

СКЗИ КриптоПро CSP поддерживает формат криптографических сообщений согласно RFC 3852 "Cryptographic Message Syntax (CMS)" с учетом RFC 4490 "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)".

10.1.4. 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. Вместе с тем, большая функциональность требует от прикладного программиста более детальных знаний в области прикладной криптографии.

10.2. Использование COM интерфейсов

КриптоПро CSP может быть использовано из COM интерфейсов разработки Microsoft:

- CAPICOM
- Certificate Services
- Certificate Enrollment Control

10.2.1. Certificate Enrollment Control (Windows 2000/2003)

COM интерфейс Certificate Enrollment Control (реализован 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.

Этот интерфейс используют различные Центры Сертификации (VeriSign, Thawte и т. д.) при формировании запросов на сертификат пользователей на платформе Windows 2000/2003.

10.2.2. Certificate Enrollment API (Windows Vista/2008/7/2008R2/8/2012)

Интерфейсы Certificate Enrollment API (реализованные в файле certenroll.dll) предназначены для генерации ключей, запросов на сертификаты, обработки сертификатов, полученных от Центра Сертификации с использованием различных языков программирования.

Этот интерфейс используют различные Центры Сертификации (VeriSign, Thawte и т. д.) при формировании запросов на сертификат пользователей на платформе Windows Vista/2008/7/2008R2/8/2012.

10.2.3. CAPICOM

CAPICOM (реализован 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.

CAPICOM позволяет использовать функции формирования и проверки электронной 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 браузера Internet Explorer.

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

10.2.4. 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 изменение:

- обработки поступающих от пользователей запросов на сертификаты;
- состава данных (в том числе дополнений X.509), записываемых в издаваемые центром сертификаты;
- способа публикации (хранения) изданных центром сертификатов.

10.3. Использование СКЗИ в веб-браузерах

КриптоПро CSP 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.

10.4. Поддержка протокола TLS

Модуль поддержки сетевой аутентификации позволяет реализовать защищенный сетевой протокол в соответствии с рекомендациями RFC 2246 "The TLS Protocol. Version 1.0" и проектом рекомендаций "Алгоритмы ГОСТ для Transport Layer Security (TLS)". Модуль обеспечивает двустороннюю и одностороннюю аутентификацию приложений при их взаимодействии по сети с использованием алгоритма ЭП и сертификатов открытых ключей, а также шифрование данных, передаваемых в сетевом соединении.

Прикладное программное обеспечение может использовать протокол TLS для аутентификации и защиты данных, передаваемых по собственным протоколам на основе TCP/IP и HTTPS.

Протокол TLS (Transport Layer Security, спецификация IETF - RFC2246) относится к средствам защиты прикладных пакетов Microsoft Internet Explorer, Internet Information Services (IIS), Microsoft SQL Server 2000 и COM+. Он обеспечивает аутентификацию связывающихся сторон, конфиденциальность и целостность пересылаемой информации. Аутентификация обеспечивается использованием сертификатов стандарта X.509 (в средах с сильной аутентификацией), конфиденциальность – шифрованием пересылаемых данных, целостность — применением хеш-функции и кода аутентификации сообщения (Message Authenticity Code, MAC).

Для подключения по протоколу TLS используется префикс *https,* при этом обозреватель Web-сервера по умолчанию будет подключаться к порту TCP 443 вместо стандартного порта TCP 80. Если сервер не поддерживает протокол TLS, соединение не устанавливается. Протокол SSL/TLS (SSL - более ранние версии протокола) применяется Интернет-протоколами (Таблица 1).

Таблица 1.

Протокол	Порт	Описание
HTTPS	443	HTTP по SSL/TLS
SMTPS	465	SMTP (электронная почта) по SSL/TLS
NNTPS	563	NNTP (новости) по SSL/TLS
LDAPS	636	LDAP (доступ к каталогам) по SSL/TLS
POP3S	995	POP (электронная почта) по SSLДLS
IRCS	994	IRC по SSL/TLS
IMAPS	993	IMAP (электронная почта) по SSL/TLS
FTPS	990	FTP (передача файлов) по SSL/TLS

Для того, чтобы протокол SSL/TLS действовал, Web-сервер должен иметь сертификат (открытый ключ) и свой закрытый ключ. Владелец сертификата должен подтвердить, что он является владельцем закрытого ключа, связанного с сертификатом. Это дает возможность клиенту аутентифицировать сервер, с которым он хочет связаться.

В процессе взаимной аутентификации:

- выполняется криптографическая проверка наличия у сервера закрытого ключа, соответствующего открытому ключу, указанному в сертификате;
- проверяется степень доверия издателю сертификата;
- проверяется, не истек ли срок действия сертификата;
- проверяется, не отозван ли сертификат; по умолчанию Internet Explorer эту проверку не выполняет — это делает IIS.

Если любая из указанных проверок приводит к отрицательному результату, пользователь получает предупреждение и может разорвать соединение (это рекомендуется делать).

Достигнув доверия, стороны вырабатывают сеансовый ключ, на основе которого обеспечивается шифрование данных в течение сеанса.

10.4.1. Основные понятия протокола TLS

Протокол TLS предназначен для обеспечения криптографическими средствами аутентификации отправителя (клиента) – адресата (сервера), контроля целостности и шифрования данных информационного обмена.

Аутентификация опционально может быть односторонней (аутентификация сервера клиентом), взаимной (встречная аутентификация сервера и клиента) или не использоваться.

Иерархия организации информационного обмена

Иерархия информационного обмена включает в себя сессии, соединения и поток сообщений в соединении. Поток сообщений при большой длине разбивается на фрагменты с пакетной передачей фрагментов. В одной сессии может быть реализовано несколько соединений, произвольно разнесенных по времени. В каждом соединении может быть обработан необходимый поток сообщений.

Алгоритм преобразования информации при обмене

Алгоритм преобразования информации при обмене с использованием протокола TLS включает операции:

- прием от протокола верхнего уровня потока не интерпретируемых данных в блоках произвольного размера;
- фрагментация принятых с верхнего уровня данных в структурированные блоки (фрагменты) протокола TLS. Размер фрагмента – не более 2^{14} байт;
- компрессия фрагментов (опционально);
- хеширование фрагментов (используется ключевой MAC);
- конкатенация фрагмента и результата его хеширования (расширенный фрагмент);
- зашифрование расширенного фрагмента (опционально);

- передача зашифрованного расширенного фрагмента с добавленным открытым заголовком протокола транспортного уровня (например, TCP).

При приеме информации применяется обратная последовательность операций.

Атрибуты сессии

Сессия характеризуется следующими атрибутами:

- идентификатор сессии (случайное число, 32 байта, задается сервером при открытии сессии);
- метод компрессии;
- сертификат сервера (опционально);
- сертификат клиента (опционально);
- спецификация алгоритмов и параметров защиты (алгоритмы шифрования и MAC, криптографические параметры);
- master secret (используется при генерации ключей шифрования, ключей MAC, векторов инициализации);
- флаг, разрешающий/запрещающий новые соединения в сеансе.

Сертификаты представляются в стандарте X509. v3. Спецификация алгоритмов и параметров защиты может меняться в течение сессии.

Атрибуты соединения

К атрибутам соединения относятся:

- client_random – случайные 32 байта, задаваемые клиентом;
- server_random– случайные 32 байта, задаваемые сервером;
- client write MAC secret (ключ клиента для ключевого хеширования);
- server write MAC secret (ключ сервера для ключевого хеширования);
- client write key (ключ, используемый для шифрования данных клиентом и расшифрования их сервером);
- server write key (ключ, используемый для шифрования данных сервером и расшифрования их клиентом);
- client write IV, server write IV (векторы инициализации, используемые клиентом и сервером соответственно);
- порядковый номер соединения (поддерживается независимо для передаваемых и принимаемых сообщений).

Вектор инициализации задается для первого фрагмента сообщения в соединении; для последующих фрагментов вектор инициализации формируется из конечного блока зашифрованного текста предыдущего фрагмента.

Порядковые номера соединений поддерживаются независимо для передаваемых и принимаемых сообщений. При смене сессии, изменении спецификации алгоритмов и параметров защиты нумерация соединений начинается с 0; Диапазон нумерации: $0 \div 2^{64}-1$.

Соединение ассоциируется с одной сессией.

Типы сообщений

В протоколе TLS используются следующие типы сообщений:

- Hello message (ClientHello, ServerHello);
- Change cipher specs message (изменение спецификации алгоритмов и параметров защиты);
- Key exchange message (передача ключа обмена ключами шифрования и MAC клиента, сервера);
- Alert message (предупреждение, оповещение о фатальной ошибке);
- Application_data message (передача данных);

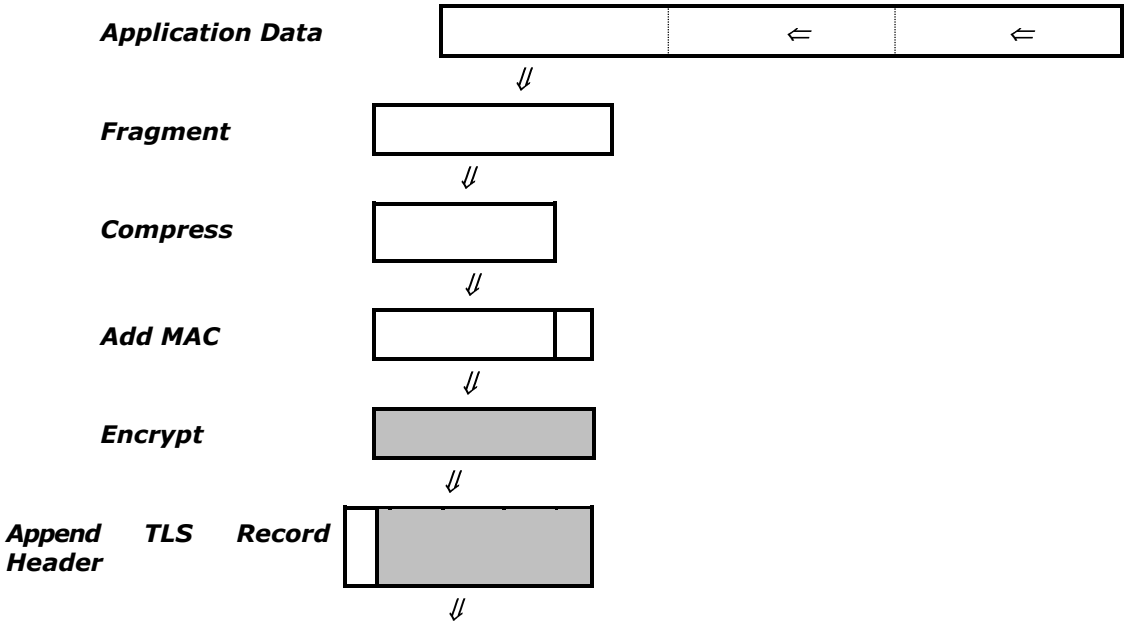
- Finished message (сообщение о возможности работы в созданной сессии).

Фрагмент сообщения, передаваемый протоколу транспортного уровня

Для передачи фрагмента сообщения транспортному уровню производятся операции:

- компрессия фрагмента (опционально);
- вычисление хеша от конкатенации ключа хеширования, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента, заданной константы;
- шифрование расширенного фрагмента (конкатенация компрессированного фрагмента и его хеша);
- добавление открытого заголовка, содержащего тип сообщения (один байт), версию протокола TLS (два байта), длину компрессированного фрагмента.

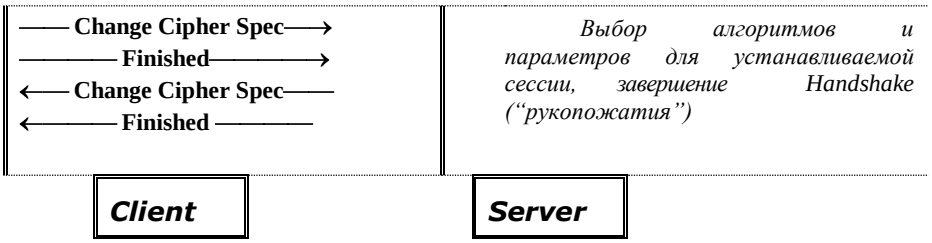
Операции протокола TLS



TLS Handshake Protocol

TLS Handshake Protocol работает по следующей схеме:

——— **ClientHello** ——→	*Установка версии протокола, идентификатора сессии, начального набора алгоритмов и параметров, метода компрессии*
←——— **ServerHello** ——— ←——— **Certificate** ———— ←—— **Certificate Request** —— ←**Server Key Exchange** —— ←— **ServerHelloDone** ——	*Сервер посылает (опционально) свой сертификат и запрашивает (опционально) сертификат клиента, передача случайной величины server-random*
——— **Certificate** ———→ —**Client Key Exchange** —→ —— **Certificate Verify** ——→	*Клиент посылает свой сертификат (если был запрос сервера) Если сертификата у клиента нет, он посылает Certificate Verify*

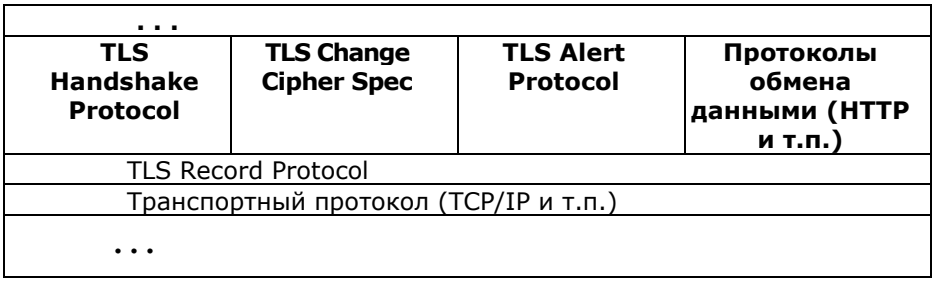


TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением операций:

- клиент и сервер договариваются об используемых в сессии алгоритмах и параметрах защиты, обмениваются случайными величинами client_random, server_random, договариваются, будут или нет новые соединения;
- производится обмен сертификатами для аутентификации клиента и сервера (по заданным опциям);
- клиент генерирует случайную величину pre_master secret, шифрует ее и передает серверу.
- Клиент и сервер по pre_master secret, client_random и server_random формируют master secret (набор необходимой ключевой информации) сессии.

Стек протокола TLS

Протокол TLS является двухуровневым и действует над транспортным протоколом. К первому уровню относятся TLS Handshake Protocol, TLS Change Cipher Spec, TLS Alert Protocol. Ко второму уровню относится TLS Record Protocol.



10.4.2. Модуль сетевой аутентификации КриптоПро TLS

Модуль сетевой аутентификации КриптоПро TLS реализован на базе протокола TLS v.1.0 и российских стандартов криптографической защиты конфиденциальной информации (алгоритмы шифрования в соответствии с ГОСТ 28147-89, алгоритмы выработки и проверки электронной подписи в соответствии с ГОСТ Р 34.10-2001, хеширования в соответствии с ГОСТ Р 34.11-94). Используется также алгоритм Диффи-Хеллмана открытого распределения ключей на базе ГОСТ Р 34.10-2001.

На ПЭВМ клиента и на сервере (IIS, ISA) устанавливается СКЗИ ЖТЯИ.00050-03 с модулем поддержки сетевой аутентификации КриптоПро TLS.

Аутентификация клиент-сервер может быть односторонней и двусторонней.

Односторонняя аутентификация обеспечивает минимально необходимый уровень защиты, и включает в себя:

- обязательную аутентификацию сервера без аутентификации клиентов;
- шифрование трафика между клиентом и сервером.

При работе в данном режиме сервер на этапе "рукопожатия" не запрашивает сертификат клиента и устанавливается "анонимное" защищенное соединение. В этом случае клиент может не иметь закрытого ключа и сертификата, однако при этом он лишается возможности формировать электронную подпись под документами. Режим с односторонней аутентификацией сервера может использоваться для предоставления некоторой группе пользователей конфиденциальной информации на основании парольной защиты, однако пароль в этом случае будет предъявляться пользователем только после установления защищенного TLS-соединения с Web-сервером, что повышает уровень защиты от несанкционированного доступа по сравнению с

передачей пароля по открытым соединениям. При односторонней аутентификации сервер запрашивает сертификат клиента, но его отсутствие не считается ошибкой.

В СКЗИ «КриптоПро CSP» используется двусторонняя аутентификация.

Двусторонняя аутентификация включает в себя:

- взаимную аутентификацию клиента и Web-сервера с помощью их сертификатов;
- шифрование трафика между клиентом и сервером;
- формирование и проверку электронной подписи под электронными HTML-формами, заполняемыми пользователями.

Двусторонняя аутентификация позволяет обеспечить доступ в закрытую часть Web - сервера только зарегистрированным владельцам сертификатов. При этом нужно иметь в виду, что разграничение доступа к информационным ресурсам сервера, основанное на проверке сертификатов клиентов, гораздо надежнее, чем просто парольная защита.

В данном режиме работы клиенту необходимо сгенерировать закрытый и открытый ключи и получить сертификат открытого ключа в УЦ.

Требования к техническим и программным средствам компьютера, на который устанавливается ISA сервер, определяются в документации, поставляемой вместе с данным сервером. Дополнительно, на компьютер должны быть установлены СКЗИ «КриптоПро CSP» и модуль поддержки сетевой аутентификации КриптоПро TLS.

Для возможности установления защищенного соединения между клиентом и сервером ISA необходимо вначале выпустить сертификат открытого ключа, который будет использоваться для серверной аутентификации по протоколу TLS.

Требования к сертификату:

- имя сертификата (Common name) должно совпадать с именем публикуемого Web-сервера прикладной системы. Например: pif.nikoil.ru
- область использования ключа должна содержать: «Аутентификация Сервера»

Данный сертификат должен быть установлен на сервер ISA в привязке с ключом подписи (закрытым ключом). При этом закрытый ключ подписи должен быть помещен в реестр ОС.

Выпуск и установка сертификата осуществляется через АРМ пользователя Центра регистрации. Порядок действий определяется в инструкции пользователю.

10.5. Модуль КриптоПро EFS

Для защиты конфиденциальной информации при ее хранении на ПЭВМ используется модуль КриптоПро EFS. Модуль обеспечивает:

- конфиденциальность хранимой информации (шифрование файлов, хранящихся в разделах NTFS в соответствии с алгоритмом ГОСТ 28147 89);

- контроль целостности хранящейся информации (вычисление/проверка имитовставки в соответствии с алгоритмом ГОСТ 28147 89);

- совместный доступ к защищенным файлам группе пользователей;

- удаленная работа с защищенными файлами, размещаемыми в Web-папках (Web Distributed Authoring and Versioning - распределенная система хранения файлов с доступом через Web или WebDAV);

- шифрование общих файлов (CIFS);

- восстановление данных в случае удаления пользователей из системы, компрометации или утраты закрытого ключа пользователя.

10.6. Поддержка протокола IPSec

Для защиты IP-соединений по протоколу IPSec в СКЗИ реализованы модули протоколов КриптоПро IKE, КриптоПро ESP, КриптоПро AH в соответствии с документами, разработанными

группой IPSec по рекомендации Технического комитета по стандартизации "Криптографическая защита информации" (ТК 26):

Методические рекомендации по ИспользованиЮ ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при управлении ключами IKE и ISAKMP. Проект первой редакции, июль 2012(rus-fedchenko-cpike-ipsecme-gost-00-rt).

Методические рекомендации по использованию комбинированного алгоритма шифрования вложений IPSec ESP на основе ГОСТ 28147-89. Проект первой редакции, июль 2012 (rus-fedchenko-cpesp-ipsecme-gost-00-rt).

Методические рекомендации по использованию алгоритмов обеспечения целостности IPSec (AH, ESP) на основе ГОСТ Р 34.11-94. Проект первой редакции, апрель 2012 (rus-fedchenko-cpah-ipsecme-gost-00-rn).

10.7. Приложение командной строки

Модуль защиты файлов и сообщений с использованием ключей симметричной и ассиметричной криптографии.

10.8. Аутентификация в домене Windows

КриптоПро Winlogon предназначен для аутентификации пользователей в домене Microsoft Windows с использованием Enterprise CA, КриптоПро УЦ или других совместимых центров сертификации.

Модуль КриптоПро Winlogon реализует работу с Российскими криптографическими алгоритмами для первого шага расширенного протокола Kerberos в соответствии с RFS 4556. Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), June 2005.

10.9. Использование функций CSP уровня ядра операционной системы

Модуль уровня ядра операционной системы позволяет использовать основные криптографические функции (шифрование/расшифрование, проверка подписи, хеширование) на уровне ядра операционной системы. Данный модуль в первую очередь предназначен для использования в приложениях уровня ядра операционной системы (шифраторы IP протокола, жесткого диска и т.д.). Интерфейс модуля аналогичен интерфейсу CSP уровня пользователя, с тем исключением, что он не позволяет работать с секретными ключами пользователя и не предоставляет оконный интерфейс. Подробнее об использовании модуля см. документ "ЖТЯИ.00050-03 90 05. КриптоПро CSP. Руководство программиста".

10.10. Примеры использования СКЗИ

Для разработчиков в состав дистрибутива СКЗИ ЖТЯИ.00050-03 включаются рекомендации, содержащие описание интерфейса TLS, подмножество CryptoAPI 2.0, реализуемое библиотекой capilite.dll, и примеры использования на уровне вызова основных функций CryptoAPI 2.0. В состав дистрибутива включены также примеры использования CSP на уровне ядра ОС, подписи/проверки подписи XML, использования xenroll, capicom, вызов функций CSP через интерфейс CSP.

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/forum2/) ведется конференция по вопросам использования криптографических функций и сертификатов открытых ключей и ключей проверки ЭП.

11. Изменения

11.1. Изменения, внесенные в КриптоПро CSP версии 1.1

- Изменен базовый идентификатор, используемый для представления алгоритмов в сертификатах и криптографических сообщениях;
- Изменено представление параметров p, q, a, узлов замены хеш-функции и шифрования в сертификатах открытых ключей и формате сообщений S/MIME (PKCS#7, RFC 2630). В связи с этим, версия 1.0 не совместима с версией 1.1;
- Добавлено отображение алгоритмов ГОСТ в диалогах ПО Microsoft Outlook Express и ПО Microsoft Outlook;
- Добавлена поддержка электронного замка "Соболь" (НИП Информзащита);
- Добавлена регистрация установленной версии КриптоПро CSP;
- Обеспечена поддержка КриптоПро CSP в ОС Windows ME;
- Удалена поддержка открытых ключей длиной 512 бит;
- Обеспечена работоспособность с Internet Explorer 5.5;
- Реализовано хранение сертификатов открытых ключей и ключей проверки ЭП в ключевом контейнере;
- Реализована возможность установки сертификата пользователя из ключевого контейнера в справочник сертификатов Windows из панели управления КриптоПРО CSP.

11.2. Изменения, внесенные в КриптоПРО CSP версии 2.0.

- Реализована возможность установки сертификата в справочник сертификатов Windows и формирование ссылки с личным закрытым ключом пользователя из панели управления КриптоПРО CSP;
- Реализован интерфейс смены и удаления пароля ключевого носителя из панели управления КриптоПро;
- Обеспечена поддержка КриптоПро CSP в ОС Windows XP;
- Реализован интерфейс PC/SC для работы со считывателями смарт-карт;
- Добавлена поддержка UCB ключей eToken;
- Реализованы алгоритмы диверсификации ключей и аутентификации, позволяющие выпускать и обслуживать интеллектуальные карточки "Оскар 1.*" и РИК-1, реализующие алгоритм шифрования ГОСТ 28147-89;
- Реализован алгоритм ЭП в соответствии с ГОСТ Р 34.10-2001;
- Поддерживаются наборы параметров ГОСТ Р 34.10-2001, запланированные к использованию в интеллектуальных картах "Оскар 2.*" и РИК.

11.3. Изменения, внесенные в КриптоПРО CSP версии 3.0.

- Исключена поддержка ОС Windows 98/ME (на этих платформах возможно использование КриптоПро CSP версии 2.0, которая совместима по выполняемым криптографическим функциям с СКЗИ КриптоПро CSP версии 3.0);
- Обеспечена поддержка ОС Windows 2003; добавлена поддержка платформ Linux 7, 9, FreeBSD 5, Solaris 9 Update 4 (ранее только Solaris 8);
- Реализован протокол сетевой аутентификации КриптоПро TLS в СКЗИ на всех платформах;
- На UNIX-платформах добавлены модули обработки сертификатов открытых ключей и поддержки списка отозванных сертификатов;
- На UNIX-платформах добавлены модули работы хранилищами сертификатов;
- На UNIX-платформах добавлены модули обработки подписанных, зашифрованных и других сообщений формата CMS (PKCS#7);
- На Windows-платформах добавлены модули обработки подписанных XML сообщений (XMLdsig);

- На Windows-платформах расширена поддержка Microsoft Office (Word, Excel, InfoPath, Outlook);
- Улучшена масштабируемость на многопроцессорных SMP и HyperThreading системах;
- Увеличена производительность криптографических преобразований на платформах IA32 в 2-3 раза.
- Закрытые ключи ГОСТ Р 34.10-94 намечены к удалению в будущих версиях "КриптоПРО CSP", о чём выдаётся предупреждающее сообщение в момент их создания.
- К существующим способам управления ключами добавлена возможность осуществления защиты ключа при помощи зашифрования данного закрытого ключа на другом закрытом ключе и при помощи разделения доступа к нему между несколькими ключевыми носителями;
- В состав СКЗИ на всех платформах добавлена реализация криптопровайдера в форме драйвера;
- Исполнения, обеспечивающие защиту класса КС1, реализованы для криптопровайдера в форме подгружаемой библиотеки;
- Исполнения, обеспечивающие защиту класса КС2, реализованы для криптопровайдера в форме сервиса хранения ключей;
- В связи с расширением поддерживаемых платформ КриптоПро CSP версии 3.0 реализовано в 10 исполнениях, отличающихся программно-аппаратной средой функционирования, составом программных модулей и классом защиты "Требований к средствам криптографической защиты конфиденциальной информации".

11.4. Изменения, внесенные в КриптоПРО CSP версии 3.6

- Обновлен и расширен перечень программно-аппаратных сред. КриптоПро CSP версии 3.6 функционирует в программно-аппаратных средах, приведенных в п. 2:
- В коде исключена возможность использования стандарта ГОСТ Р 34.10-94.
- В состав основных модулей включен Winlogon - модуль аутентификации пользователя в домене Windows;
- В составе автономного АРМ используется утилита выработки гаммы; используется гамма поставщика для инициализации ПДСЧ;
- Расширен внешний интерфейс СКЗИ для обеспечения работы провайдера с функциональным ключевым носителем (ФКН), согласования ключей для использования в реализациях протокола IPSec, работы с другими приложениями;
- Реализовано исполнение СКЗИ с обеспечением класса защиты КС3 (исполнение 3);
- Внедрена библиотека 64-разрядной арифметики;
- Усовершенствованы функции вычисления кратной точки эллиптической кривой;
- Изменен код ассемблерных вставок под компилятор JASM для унифицированного использования на платформах Windows, Linux, FreeBSD, SPARC на платформе Intel;
- Обеспечена реализация протокола EAP/TLS;
- Переработан драйвер настройки ОС и контроля целостности ПО СКЗИ в связи с изменением кода операционных систем и расширения их перечня (Windows Vista/2008);
- Введено ограничение обработки информации в режиме CRYPT_SIMPLEMIX_MODE на одном ключе не более 4 мегабайта, при использовании алгоритма ГОСТ 28147-89.

11.5. Изменения, внесенные в КриптоПРО CSP версии 3.6.1

- Добавлены исполнения 3 – 5 класса защиты КС3;
- Обеспечена работа с шифрующей файловой системой КриптоПро EFS;
- Добавлен модуль протоколов КриптоПро IKE, ESP.

12. Информация для пользователей

Для получения дополнительной информации о данном продукте, а так же о других продуктах ООО "КРИПТО-ПРО", можно обращаться по адресу:

Служба маркетинга и технической поддержки Крипто-Про.

127018, Москва, Сущевский вал 18, ООО "КРИПТО-ПРО".

Телефон: +7 (495) 995 4820

Факс: +7 (495) 995 4820

e-mail: info@CryptoPro.ru WWW: http://www.CryptoPro.ru