127 018, Москва, Сущевский вал, д.16/5
Телефон: (495) 780 4820
Факс: (495) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 3.6

Описание реализации

ЖТЯИ.00050-02 90 01
Листов 13

2010

Содержание

Аннотация

Настоящий документ содержит описание реализации средства криптографической защиты информации КриптоПро CSP версии 3.6 (СКЗИ ЖТЯИ.00050-02) и сведения о текущем состоянии продукта.

1. Версия и исполнения продукта

СКЗИ ЖТЯИ.00050-02 является модификацией СКЗИ КриптоПро CSP версии 3.6 (СКЗИ ЖТЯИ.00050-01) и совместимо с ним по выполняемым криптографическим функциям.

СКЗИ ЖТЯИ.00050-02 изготовляется в двух исполнениях:

- Исполнение 1 класса защиты КС1;
- Исполнение 2 класса защиты КС2.

2. Требования к системному ПО

СКЗИ ЖТЯИ.00050-02 функционирует в программно-аппаратных средах:

- Windows 2000 (ia32);
- Windows XP/2003/Vista/2008/7/2008R2 (ia32, ia64, x64).
- Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x/3.x:
  - Linpus (ia32)
  - Mandriva (ia32, x64)
  - MontaVista Linux (ia32, x64)
  - Oracle Enterprise Linux (ia32, x64)
  - Open SUSE (ia32, x64)
  - Red Hat Enterprise Linux (ia32, x64)
  - Red Flag Linux (ia32)
  - SUSE Linux Enterprise (ia32, x64)
  - SUSE LINUX (ia32)
  - Ubuntu (ia32, x64)
  - Xandros (ia32)

  ALT Linux (ia32, x64);
  Debian (ia32, x64);
  Red Hat Enterprise Linux Version 3 Update 3 (ia32, x64);
  Trustverse Linux XP (ia32);
- FreeBSD 7/8 (ia32);
- Solaris 9/10 (sparc, ia32, x64);
- AIX 5/6 (Power PC). Только в исполнении 1.

3. Назначение

СКЗИ ЖТЯИ.00050-02 обеспечивает выполнение 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 цифровой 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"*.

Для обеспечения юридической значимости электронных документов при обмене УЦ, используемый совместно с СКЗИ, и СКЗИ пользователя должны функционировать в соответствии с законом об ЭЦП.

- 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.

4. Основные характеристики СКЗИ КриптоПро CSP

4.1. Размеры ключей

Размеры ключей электронной цифровой подписи:
- закрытый ключ – 256 бит;
- открытый ключ - 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 типы носителей:
- ГМД 3,5'';
- USB диски
- электронный ключ с интерфейсом USB (e-Token);
- Смарткарты РИК, Оскар, Магистра
- идентификаторы Touch-Memory D S1995 – 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.00050-02 30 01. СКЗИ "КриптоПро CSP". Формуляр, п.п. 3.8, 3.9.

Примечание 1. В состав дистрибутива СКЗИ ЖТЯИ.00050-02 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.

Примечание 3. Вопрос об использовании ключевых носителей других типов должен согласовываться с ООО "КРИПТО-ПРО".

5. Реализация КриптоПро CSP

5.1. Структура СКЗИ

Структура СКЗИ ЖТЯИ.00050-02 представлена на рис. 1.

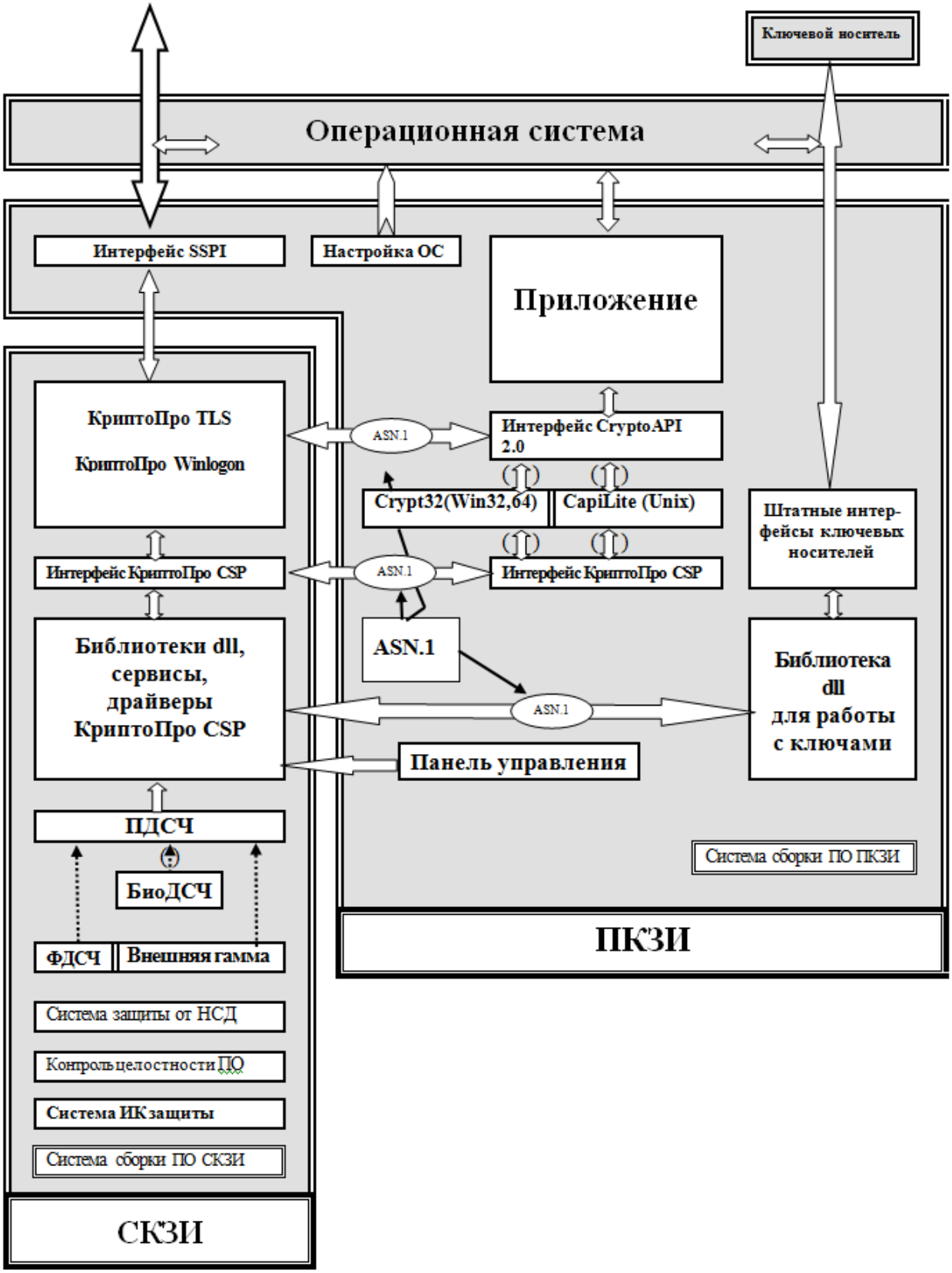

Рис. 1. Структура СКЗИ ЖТЯИ.00050-02.

5.2. Состав программного обеспечения СКЗИ

В состав СКЗИ ЖТЯИ.00050-02 входят:

- Библиотеки dll, сервисы, драйверы КриптоПро CSP.
- Модуль сетевой аутентификации КриптоПро TLS.
- 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 исполнении 2).
- Контроль целостности программного обеспечения.
- Система инженерно-криптографической защиты.
- Система защиты от НСД (используется опционально).

5.3. Состав программного обеспечения ПКЗИ

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/XP/2003/Vista/2008/7/2008R2).
- 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/XP/2003/Vista/2008/7/2008R2.
- 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.00050-02 90 02 -01, ЖТЯИ.00050-02 90 02 -02, ЖТЯИ.00050-02 90 02-03, ЖТЯИ.00050-02 90 0 2-04, ЖТЯИ.00050-02 90 0 2-05 к документу "ЖТЯИ.00050-02 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть".

ПКЗИ в СКЗИ ЖТЯИ.00050-02 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, при этом дескрипторы непосредственно не содержат адреса объектов.

В исполнении 2 СКЗИ реализован **Криптографический сервис** с хранением объектов в отдельном от ПКЗИ адресном пространстве, что обеспечивает дополнительный рубеж защиты объектов СКЗИ от приложений.

6. Установка ПО СКЗИ ЖТЯИ.00050-02

Установка ПО в зависимости от используемой платформы производится в соответствии с дополнениями ЖТЯИ.00050-02 90 02 -01, ЖТЯИ.00050-02 90 02 -02, ЖТЯИ.00050-02 90 02 -03, ЖТЯИ.00050-02 90 02-04, ЖТЯИ.00050-02 90 02-05 к документу "ЖТЯИ.00050-02 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть".

7. Применение СКЗИ ЖТЯИ.00050-02

Возможны следующие применения СКЗИ ЖТЯИ.00050-02:

1. Применение СКЗИ в составе стандартного программного обеспечения компании Microsoft и других компаний, реализующих криптографический интерфейс в соответствии с архитектурой Microsoft.

2. Встраивание СКЗИ во вновь разрабатываемое или существующее прикладное программное обеспечение.

8. Использование СКЗИ в стандартном программном обеспечении

Программное обеспечение СКЗИ ЖТЯИ.00050-02 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.
- Электронная почта - MS Outlook (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 (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 терминалов и клиент (RDP).
- Средства функционирования комплекса разработки ООО «КРИПТО-ПРО» Крипто-Про УЦ 1.4, КриптоПро OCSP, КриптоПро TSP, КриптоАРМ, CryptCP, Клиент КриптоПро HSM.

СКЗИ ЖТЯИ.00050-02 при функционировании под управлением ОС Windows может использоваться с дополнительными программными средствами защиты:

ЖТЯИ.00032-01 30 01. КриптоПро Winlogon. Средство сетевой аутентификации.

ЖТЯИ.00051-01 30 01. КриптоПро EFS. Средство хранения конфиденциальной информации.

Под управлением UNIX-подобных ОС СКЗИ ЖТЯИ.00050-02 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 стандартами:

"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 преставления открытых ключей и ЭЦП, 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 de-facto являющемся стандартом на представление электронного документа в защищенном виде как с использованием алгоритма ЭЦП, так 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 использует шифрование ГОСТ 28147-89 и контроль целостности с помощью имитовставки, третий и четвертый не использует шифрование и контролирует 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 ЭЦП в документов формата XML "XML-Signature Syntax and Processing", принятому консорциумом W3C, в части использования российских алгоритмов электронно-цифровой подписи.

Программное обеспечение СКЗИ ЖТЯИ.00050-02 совместимо со средствами антивирусной защиты:

- McAfee VirusScan Enterprise Version 8.0i.
- Norton (Symantec) Antivirus.
- Антивирус Касперского
- Антивирус NOD32.

9. Встраивание СКЗИ

Архитектура СКЗИ ЖТЯИ.00050-02 обеспечивает возможность его встраивания в различные ОС с целью распределения открытых ключей на базе сертификатов стандарта X.509.

9.1. Использование интерфейса CSP

СКЗИ ЖТЯИ.00050-02 может быть использовано прикладным программным обеспечением путем загрузки модуля вызовом функции **LoadLibrary()**. Для этих целей в комплект поставки включается документ "ЖТЯИ.00050-02 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.

9.2. Использование интерфейса CryptoAPI 2.0.

СКЗИ ЖТЯИ.00050-02 может быть использовано прикладным программным обеспечением (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс **CryptoAPI 2.0 (**описание – в документацией **MSDN - Microsoft Developer Network)**. В этом случае способ выбора криптографического алгоритма в прикладном ПО может определяться информацией, содержащейся в сертификатах открытых ключей X.509.

Использование интерфейса CryptoAPI 2.0 в ОС Windows преследует цели:

- Обеспечение прикладному уровню доступа к криптографическим функциям (генерация ключей, формирование/проверка электронной цифровой 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.

9.2.1. 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.

9.2.2. 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 S yntax No tation 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.

9.2.3. 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.

9.2.4. Высокоуровневые функции обработки криптографических сообщений

Эта группа функций (Simplified Message Functions) в первую очередь предназначена для использования в прикладном ПО. С их помощью 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, используется формат PKCS#7 (RFC 2315) или CMS (RFC 2630) в Windows 2000.

9.2.5. 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.

9.3. Использование COM интерфейсов

КриптоПро CSP может быть использовано из COM интерфейсов разработки Microsoft:

- CAPICOM
- Certificate Services
- Certificate Enrollment Control

9.3.1. Certificate Enrollment Control (Windows 2000/XP/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/XP/2003.

9.3.2. Certificate Enrollment API (Windows Vista/2008/7/2008R2)

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.

9.3.3. 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 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 браузера Internet Explorer.

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

9.3.4. 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.

9.4. Использование протокола TLS в прикладном ПО

Модуль поддержки сетевой аутентификации позволяет на базе СКЗИ ЖТЯИ.00050-02 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 ЭЦП и сертификатов открытых ключей, а так же шифрование данных, передаваемых в сетевом соединении.

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

9.5. 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.00050-02 90 05. КриптоПро CSP. Руководство программиста".

9.6. Примеры использования СКЗИ

Для разработчиков в состав дистрибутива СКЗИ ЖТЯИ.00050-02 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.

10. Изменения

10.1. 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 хэш-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 в ключевом контейнере;
- Реализована возможность установки сертификата пользователя из ключевого контейнера в справочник сертификатов Windows из панели управления КриптоПРО CSP.

10.2. 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 ЭЦП 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.

10.3. 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 по уровню КС1, реализованы для криптопровайдера в форме подгружаемой библиотеки;
- Исполнения, обеспечивающие защиту по уровню 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".

10.4. 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; используется в исполнени 3 (класс защиты КС3);
- В составе автономного АРМ используется утилита выработки гаммы; гамма 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 уровня 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. 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 16/5, ООО "КРИПТО-ПРО".

Телефон: +7 (495) 780 4820

Факс: +7 (495) 780 4820

e-mail: info@CryptoPro.ru

WWW: http://www.CryptoPro.ru