127 018, Москва, Улица Образцова, 38
Телефон: (095) 933 1168
Факс: (095) 933 1168
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

# Средство Криптографической Защиты Информации

# КриптоПро CSP

Версия 3.0

# Описание реализации

ЖТЯИ.00015-01 90 01

Листов 14

2005 г.

**© ООО "Крипто-Про", 2000-2005. Все права защищены.**

Авторские права на средство криптографической защиты информации КриптоПРО CSP и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Свидетельство об официальной регистрации программ для ЭВМ № 2001610275 от 14 марта 2001 года.

Документ входит в комплект поставки программного обеспечения КриптоПРО CSP, и на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "Крипто-Про" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

# Содержание

**1. Аннотация ..... 4**

**2. Версия продукта ..... 4**

**3. Требования к системному ПО ..... 4**

**4. Назначение ..... 4**

**5. Основные характеристики ..... 5**

5.1. Размеры ключей ..... 5

5.2. Типы ключевых носителей ..... 5

**6. Реализация КриптоПро CSP ..... 5**

6.1. Состав программного обеспечения ..... 5

6.2. СКЗИ КриптоПро CSP ..... 7

6.3. ПКЗИ КриптоПро CSP ..... 7

**7. Применение КриптоПро CSP ..... 7**

**8. Использование КриптоПро CSP в стандартном программном обеспечении ..... 8**

**9. Встраивание КриптоПро CSP ..... 9**

9.1. Использование интерфейса CSP ..... 9

9.2. Использование интерфейса CryptoAPI 2.0. ..... 9

9.2.1. Базовые криптографические функции ..... 10

9.2.2. Функции кодирования/декодирования ..... 10

9.2.3. Функции работы со справочниками сертификатов ..... 10

9.2.4. Высокоуровневые функции обработки криптографических сообщений ..... 10

9.2.5. Низкоуровневые функции обработки криптографических сообщений ..... 10

9.3. Использование COM интерфейсов ..... 10

9.3.1. Certificate Enrollment Control ..... 10

9.3.2. CAPICOM ..... 11

9.3.3. Certificate Services ..... 11

9.4. Использование протокола TLS в прикладном ПО ..... 11

9.5. Использование функций CSP уровня ядра операционной системы ..... 11

9.6. Примеры использования средств криптографической защиты ..... 12

**10. Изменения ..... 12**

10.1. Изменения, внесенные в КриптоПро CSP версии 1.1 ..... 12

10.2. Изменения, внесенные в КриптоПРО CSP версии 2.0. ..... 12

10.3. Изменения, внесенные в КриптоПРО CSP версии 3.0. ..... 13

**11. Установка версии ..... 13**

**12. Информация для пользователей ..... 14**

# 1. Аннотация

Настоящий документ содержит описание реализации средства криптографической защиты информации (СКЗИ) КриптоПро CSP версии 3.0 и сведения о текущем состоянии продукта.

# 2. Версия продукта

СКЗИ КриптоПро CSP версии 3.0 является модификацией СКЗИ КриптоПро CSP версии 2.0 и совместима ним по выполняемым криптографическим функциям.

# 3. Требования к системному ПО

**СКЗИ КриптоПро CSP версии 3.0 функционирует в следующих операционных системах (ОС):**

- Windows 2000 (платформа IA32);
- Windows XP (платформа IA32);
- Windows 2003 (платформа IA32);
- Windows XP (платформа IA64);
- Windows 2003 (платформа IA64);
- Red Hat Linux 7 (платформа IA32);
- Red Hat Linux 9 (платформа IA32);
- FreeBSD 5 (платформа IA32);
- Solaris 9 Update 4 (платформа IA32);
- Solaris 9 Update 4 (платформа SPARC).

# 4. Назначение

**СКЗИ КриптоПро CSP предназначено для:**

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами:
  - ГОСТ Р 34.10-94 *"Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма."*;
  - ГОСТ Р 34.10-2001*. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".*
  - ГОСТ Р 34-11-94. *"Информационная технология. Криптографическая защита информации. Функция хэширования"*.
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89 *"Системы обработки информации. Защита криптографическая"*;
- контроля 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 средств защиты;

- обеспечения аутентификации связывающихся сторон, конфиденциальности и целостности пересылаемой информации с использованием сертификатов стандарта X.509;
- установления аутентичного защищенного соединения с использованием протокола КриптоПро TLS.

# 5. Основные характеристики

## 5.1. Размеры ключей

Размеры ключей электронной цифровой подписи:

- закрытый ключ – 256 бит;
- открытый ключ –1024 бита при использовании алгоритма ГОСТ Р 34.10-94
  - 512 бит при использовании алгоритма ГОСТ Р 34.10-2001

Размеры ключей, используемых при шифровании:

- закрытый ключ – 256 бит;
- открытый ключ –1024 бита на базе алгоритма ГОСТ Р 34.10-94
  - 512 бит на базе алгоритма ГОСТ Р 34.10-2001
- симметричный ключ – 256 бит;

## 5.2. Типы ключевых носителей

- дискета 3,5";
- процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК1, Оскар) с использованием считывателей смарт-карт, поддерживающий протокол PS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126 и др.);
- таблетки Touch-Memory DS1993 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS;
- электронный ключ с интерфейсом USB;
- сменный носитель с интерфейсом USB;
- реестр Windows для исполнений СКЗИ по уровню КС1;
- Раздел /var/CPROcsp/users/ жесткого диска для исполнений СКЗИ по уровню КС1.

Состав ключевых носителей конкретизуется в зависимости от платформ и исполнений.



**Примечание 1.** Дополнительное программное обеспечение, необходимое для использования устройств хранения ключевой информации, отличных от дискеты 3.5" и реестра Windows, можно установить с сервера http://www.cryptopro.ru/CryptoPro/products/key_moduls.asp.

**Примечание 2.** Допускается хранение закрытых ключей в реестре ОС Windows и в разделе жесткого диска для исполнений по уровню КС2 при условии распространения на ПЭВМ требований по обращению с ключевыми носителями

# 6. Реализация КриптоПро CSP

## 6.1. Состав программного обеспечения

В состав программного обеспечения для всех платформ входят СКЗИ КриптоПро CSP, модуль сетевой аутентификации КриптоПро TLS и ПКЗИ.

На рисунке 1 изображена общая структура СКЗИ КриптоПро CSP версии 3.0.

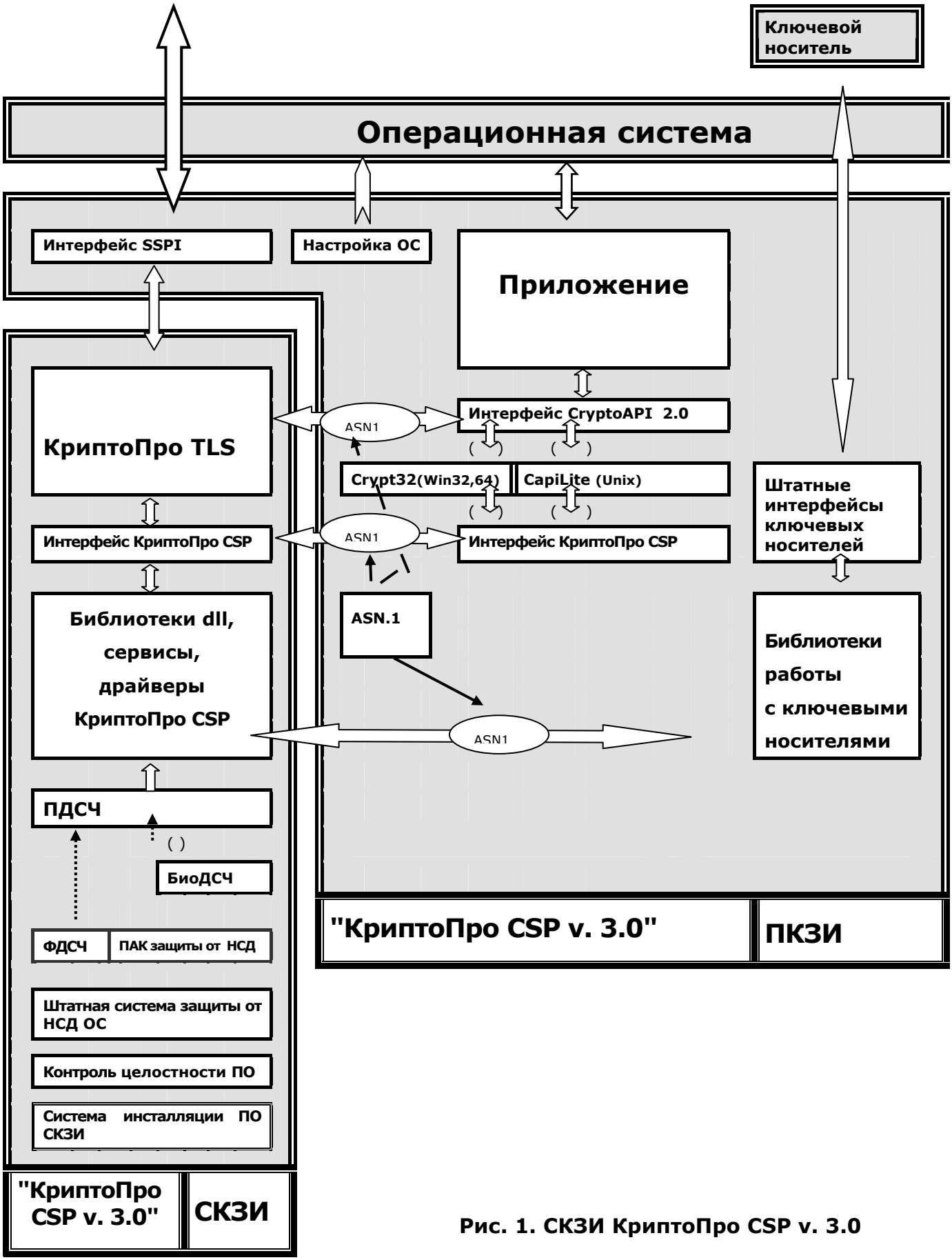



**Рис. 1. СКЗИ КриптоПро CSP v. 3.0**

## 6.2. СКЗИ КриптоПро CSP

В состав СКЗИ КриптоПро CSP входят:

- Библиотеки криптопровайдера (динамические) для исполнений по уровню КС1;
- Сервис хранения ключей для исполнений по уровню КС2;
- Криптодрайвер;
- Библиотеки протокола сетевой аутентификации КриптоПро TLS;
- Программно-аппаратный комплекс защиты от НСД (типа "Соболь", "Аккорд-АМДЗ") для всех исполнений уровня **КС2**, исключая платформу Solaris 9 Update 4 (SPARC);
- Подсистема контроля целостности, исполняемая в форме библиотеки либо драйвера в зависимости от исполнений.

## 6.3. ПКЗИ КриптоПро CSP

В состав ПКЗИ входят компоненты:

- Библиотека управления сертификатами открытых ключей CapiLite для исполнений под ОС Red Hat Linux, FreeBSD, Solaris;
- Библиотеки настройки ОС Windows, обеспечивающие совместимость CryptoAPI с СКЗИ “КриптоПро CSP”;
- Библиотеки работы с ключевыми носителями;
- Библиотека проверки цепочек сертификатов (Revocation Provider);
- Система настройки для обеспечения функционирования СКЗИ для исполнений под ОС Windows.

Состав модулей СКЗИ и ПКЗИ для соответствующих программно-аппаратных сред конкретизируется в дополнениях ЖТЯИ.00015-01 90 02-01, ЖТЯИ.00015-01 90 02-02, ЖТЯИ.00015-01 90 02-03, ЖТЯИ.00015-01 90 02-04, ЖТЯИ.00015-01 90 02-05 к документу ЖТЯИ.00015-01 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

Основной архитектурной особенностью ПО 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. осуществляется через дескрипторы соответствующих объектов; дескриптор объекта непосредственно не содержит его адреса.

В исполнениях СКЗИ по уровню защиты КС2 реализован **Криптографический сервис** для хранения объектов в отдельном от ПКЗИ адресном пространстве, что является дополнительной мерой защиты объектов СКЗИ от приложений.

# 7. Применение КриптоПро CSP

Возможны следующие способы применения КриптоПро CSP.

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

# 8. Использование КриптоПро CSP в стандартном программном обеспечении

Программное обеспечение КриптоПро CSP позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей X.509 с различным программным обеспечением Microsoft:

- Центр Сертификации - Microsoft Certification Authority, входящий в состав OS Windows 2000 Server, Advanced Server.
- Электронная почта - Microsoft Outlook 98, 2000, XP.
- Microsoft Word, Excel, Info Path.
- Электронная почта - Microsoft Outlook Express, входящая в состав Internet Explorer версии 5.0 или выше.
- Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.
- Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer - Web сервер IIS (4.0 и выше).

При этом российские криптографические алгоритмы и сертификаты открытых ключей X.509 используются в соответствии с проектами международных документов:

1. Проект "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" (**draft-ietf-pkix-gost-cppk-00.txt**) 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.
2. Проект "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" (**draft-popov-cryptopro-cpalgs-00.txt)** описывает дополнительные алгоритмы, необходимые для использования ГОСТ 28147-89, ГОСТ Р 34.10-94, 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 по ГОСТ Р 34.11-94), преобразование ключа и синхропосылки после обработки очередных 1 Кб данных, генерация псевдослучайной последовательности (аналог PRF на базе HMAC по ГОСТ Р 34.11-94), формирование ключа обмена (согласования) на базе ГОСТ Р 34.10-94, 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.
3. Проект "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)" (**draft-ietf-smime-gost-01.txt**) 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).
4. 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 34.10-94 и 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.

5. 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.

# 9. Встраивание КриптоПро CSP

Архитектура встраивания СКЗИ КриптоПро CSP версии 3.0 в прикладное программное обеспечение основана на структуре СКЗИ и ПКЗИ КриптоПро CSP.

Она обеспечивает возможность использования системы распределения открытых ключей и сертификатов в соответствии с приведенными выше проектами (см. пункт 8) с применением системы Удостоверяющего Центра, поддерживающего соответствующие форматы сертификатов (в частности КриптоПро УЦ).

Архитектура обеспечивает возможность встраивания КриптоПроCSP в различные ОС с целью реализации в их составе системы распределения открытых ключей на базе сертификатов X509.

## 9.1. Использование интерфейса CSP

СКЗИ КриптоПро CSP может быть использован прикладным программным обеспечением путем загрузки модуля вызовом 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.

## 9.2. Использование интерфейса CryptoAPI 2.0.

КриптоПро CSP может быть использовано прикладным программным обеспечением (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс **CryptoAPI 2.0**, подробное описание которого приведено в программной документацией **MSDN (Microsoft Developer Network)**. В этом случае способ выбора криптографического алгоритма в прикладном ПО может определяться информацией, описывающий алгоритм открытого ключа отправителя или получателя, содержащейся в сертификатах открытых ключей X.509.

Использование интерфейса CryptoAPI 2.0 в ОС Windows преследует две главные цели:

- Дать прикладному уровню доступ к криптографическим функциям для генерации ключей, формирования/проверки электронной цифровой подписи, шифрования/расшифрования данных. Эта цель достигается путем изолирования прикладного уровня от уровня реализаций 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 криптографических функций позволяет одновременно использовать разные алгоритмы и различные реализации этих алгоритмов, включая аппаратные.

Функционально интерфейс CryptoAPI 2.0 делится на 5 групп.

На Unix-платформах ПКЗИ КриптоПро CSP 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:

- **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 повторяют 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 Syntax Notation One), определенный серией рекомендаций X.680. К этой же группе функций можно отнести 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. Причем в качестве справочника могут использоваться самые различные типы хранилищ: от файла до LDAP.

### 9.2.4.Высокоуровневые функции обработки криптографических сообщений

Именно 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.

### 9.2.5.Низкоуровневые функции обработки криптографических сообщений

Данная группа функция (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, разработанных Microsoft.

- CAPICOM
- Certificate Services
- Certificate Enrollment Control

### 9.3.1.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 Центры Сертификации (VeriSign, Thawte и т. д.) при формировании сертификатов пользователей на платформе Windows.

### 9.3.2.CAPICOM

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 браузера Internet Explorer.

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

### 9.3.3.Certificate Services

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

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

## 9.4. Использование протокола TLS в прикладном ПО

Модуль поддержки сетевой аутентификации позволяет на базе КриптоПро CSP 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. Модуль использует КриптоПро CSP для реализации криптографических функций.

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, проверки 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. "**Руководство программиста**".

## 9.6. Примеры использования средств криптографической защиты

Для разработчиков в состав дистрибутива КриптоПро CSP 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. Так же в состав дистрибутива включены примеры использования CSP на уровне ядра ОС, подписи / проверки 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/forum/forum.asp) ведется конференция по вопросам использования криптографических функций и сертификатов открытых ключей. Соответствующие конференции по отдельным темам ведутся на сервере Microsoft:

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

# 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".

# 11. Установка версии

Установка ПО производится в соответствие с дополнениями ЖТЯИ.00015-01 90 02-01, ЖТЯИ.00015-01 90 02-02, ЖТЯИ.00015-01 90 02-03, ЖТЯИ.00015-01 90 02-04 к документу "ЖТЯИ.00015-01 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть", в зависимости от используемой платформы.

# 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, улица Образцова 38, ООО "Крипто-Про".

Телефон: +7 (095) 933 1168

Факс: +7 (095) 933 1168

e-mail: info@CryptoPro.ru

WWW: http://www.CryptoPro.ru