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 4.0 R4 КС1

1-Base

Описание реализации

ЖТЯИ.00087-03 90 01

Листов 33

2018 г.

© ООО «КРИПТО-ПРО», 2000-2018. Все права защищены.

Авторские права на средства криптографической защиты информации типа «КриптоПро CSP» и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Настоящий документ входит в комплект поставки программного обеспечения СКЗИ «КриптоПро CSP» версии 4.0 R4; 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 5

2. Назначение СКЗИ 6

3. Программно-аппаратные среды функционирования СКЗИ 8

4. Основные характеристики СКЗИ 10

4.1. Размеры ключей 10

4.2. Типы ключевых носителей 10

5. Структура и состав СКЗИ 11

5.1. Структура СКЗИ 11

5.2. Состав СКЗИ 12

5.3. Состав программного обеспечения 12

5.4. Состав SDK СКЗИ 12

5.5. Состав подсистемы программной среды функционирования комплекса (СФК) 12

6. Применение СКЗИ 14

7. Использование СКЗИ в стандартном программном обеспечении 15

8. Использование СКЗИ с программными продуктами разработки ООО «КРИПТО-ПРО» 18

9. Встраивание СКЗИ 19

10. Использование интерфейса CryptoAPI 2.0 20

10.1. Базовые криптографические функции 20

10.1.1. Функции кодирования/декодирования 20

10.1.2. Функции работы со справочниками сертификатов 20

10.1.3. Высокоуровневые функции обработки криптографических сообщений 21

10.1.4. Низкоуровневые функции обработки криптографических сообщений 21

10.2. Использование COM интерфейсов 21

10.2.1. CAPICOM 21

10.2.2. Certificate Enrollment Control (Windows Server 2003) 22

10.2.3. Certificate Enrollment API (Windows 2008/7/2008 R2/8/2012/8.1/2012 R2/10 22

10.2.4. Certificate Services 22

10.3. Использование СКЗИ в веб-браузерах 22

10.4. Поддержка протокола TLS 22

10.4.1. Основные понятия протокола TLS 24

10.4.2. Модуль сетевой аутентификации «КриптоПро TLS» 27

10.5. Приложение командной строки 29

10.6. Аутентификация в домене Windows 29

10.7. Использование функций CSP уровня ядра операционной системы 29
10.8. Примеры использования СКЗИ «КриптоПро CSP» версии 4.0 R4 29
11. История версий 30
11.1. «КриптоПро CSP» версии 1.1.....30
11.2. «КриптоПро CSP» версии 2.0.....30
11.3. «КриптоПро CSP» версии 3.0.....30
11.4. «КриптоПро CSP» версии 3.6.....31
11.5. «КриптоПро CSP» версии 3.6.1 31
11.6. «КриптоПро CSP» версии 3.8.....32
11.7. «КриптоПро CSP» версии 3.9.....32
11.8. «КриптоПро CSP» версии 4.0.....32
12. Информация для пользователей 33

1. Аннотация

Настоящий документ содержит описание реализации средства криптографической защиты информации «КриптоПро CSP» версии 4.0 R4 исполнения 1-Base (ЖТЯИ.00087-03) (далее — СКЗИ) и сведения о текущем состоянии продукта.

2. Назначение СКЗИ

СКЗИ предназначено для защиты открытой информации в информационных системах общего пользования (вычисление/проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах с выполнением следующих функций:

1) защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;
2) шифрование, вычисление имитовставки, хэширование, создание/проверка электронной подписи;
3) формирование сессионных ключей, ключей обмена и ключей создания/проверки ЭП, их импорт/экспорт из/в ключевой контейнер;
4) идентификация, аутентификация, шифрование и имитозащита TLS-соединений;
5) аутентификация в домене Windows с использованием «КриптоПро Winlogon».

СКЗИ обеспечивает выполнение следующих 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, ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
  - ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012. «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. Алгоритм криптографического преобразования»;
- контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- создание и управление ключевой информацией;
- обеспечение аутентификации связывающихся сторон, конфиденциальности и целостности пересылаемой информации с использованием сертификатов стандарта X.509;
- установление аутентичного защищенного соединения с использованием протокола «КриптоПро TLS»;
- обеспечение конфиденциальности и контроля целостности и авторизация файлов и информационных сообщений;
- обеспечение аутентификации пользователя в домене Windows.

Дополнительные алгоритмы поддержки ключевых систем, параметры алгоритмов, форматы сертификатов, поддерживаемые в СКЗИ, определены в документах RFC 4357, RFC 4490, RFC 4491, «Системы обработки информации. Защита криптографическая. Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012» Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS» Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10,

ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509» Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26).

Допустимо использовать следующие механизмы защиты информации:

- Конфиденциальность информации при хранении (на дисках, в базе данных) и передаче в сети связи обеспечивается использованием функций шифрования.
- Идентификация и авторство при сетевом взаимодействии (установлении сеанса связи) обеспечивается функциями ЭП при использовании их в процессе аутентификации (например, в соответствии со стандартом X.509). При электронном документообороте обеспечивается использованием функций ЭП электронного документа. Дополнительно должна быть предусмотрена защита от навязывания, повтора электронного документа и целостность справочников ключей проверки ЭП.
- Целостность информации обеспечивается использованием следующих функций:
  - функции ЭП электронного документа,
  - имитозащиты (при использовании функций шифрования без использования ЭП), авторство информации при этом не обеспечивается,
  - функции хэширования, авторство информации при этом не обеспечивается.
- Неотказуемость от факта передачи электронного документа обеспечивается использованием функций ЭП (подпись документа отправителем) и хранением документа с ЭП в течение установленного срока приемной стороной.
- Неотказуемость от факта приема электронного документа обеспечивается использованием функций ЭП и квитированием приема документа (подпись квитанции получателем), хранением документа и квитанции с ЭП в течение установленного срока отправляющей стороной.
- Защита от переповторов обеспечивается использованием криптографических функций ЭП, шифрования или имитозащиты с добавлением уникального идентификатора сетевой сессии (электронного документа) с последующей их проверкой приемной стороной или разработкой специализированного протокола аутентификации (обмена электронными документами).
- Защита от нарушителя с целью навязывания приемной стороне собственной информации, переданной якобы от лица санкционированного пользователя (нарушение авторства информации) обеспечивается использованием функций ЭП с проверкой атрибутов электронного документа и ключа проверки ЭП отправителя.
- Защита от закладок, вирусов, модификации системного и прикладного ПО обеспечивается совместным использованием криптографических средств, средств антивирусной защиты и организационных мероприятий.

3. Программно-аппаратные среды функционирования СКЗИ

СКЗИ функционирует в следующих группах программно-аппаратных сред:

Windows

Включает программно-аппаратные среды:

- Windows XP[1] (x86);
- Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
- Windows Server 2008 R2/2012/2012 R2/2016 (x64).

LSB Linux

Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:

- CentOS 4/5/6 (x86, x64);
- CentOS 7 (x86, x64, POWER, ARM, ARM64);
- ОСь (OS-RT) (x64);
- ТД ОС АИС ФССП России (GosLinux) (x86, x64);
- Red OS (x86, x64);
- Fedora 27/28/29 (x86, x64, ARM);
- Oracle Linux 4/5/6 (x86, x64);
- Oracle Linux 7 (x64);
- OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64);
- AlterOS (x64);
- SUSE Linux Enterprise Server 11SP4 (x86, x64);
- SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64);
- Red Hat Enterprise Linux 4/5/6 (x86, x64);
- Red Hat Enterprise Linux 7 (x64, POWER, ARM64);
- Синтез-ОС.РС (x86, x64);
- ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64);
- ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64);
- КП «ОС «СинтезМ-К» (x64);
- Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);
- Ubuntu 18.04/18.10 (x86, x64);
- Linux Mint 17/18/19 (x86, x64);
- Debian 7/8/9 (x86, x64, POWER, ARM, ARM64, MIPS);
- ОС Лотос (x86, x64);
- Astra Linux Special Edition, Common Edition (x64, MIPS, Эльбрус);
- МСВСфера 6.3 Сервер (x64, ARM64).

Unix

Включает программно-аппаратные среды:

- ОС Эльбрус версия 3 (Эльбрус);
- ALT Linux 6/7 (x86, x64, ARM);
- Альт Сервер 8, Альт 8 СП Сервер (x86, x64, ARM, ARM64);
- Альт Рабочая станция 8, Альт Рабочая станция К 8, Альт 8 СП Рабочая станция (x86, x64, ARM, ARM64);
- ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);
- РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);
- FreeBSD 11, pfSense 2.x (x86, x64);
- AIX 6/7 (POWER);
- Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14 (x64).

Solaris

Включает программно-аппаратные среды:

- Solaris 10 (sparc, x86, x64);
- Solaris 11 (sparc, x64).

Sailfish

Включает программно-аппаратную среду:

- SailfishOS 2.1.1.12 (ARMv7).

iOS

Включает программно-аппаратные среды:

- Apple iOS 8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1/9.3/9.3.1/9.3.2/9.3.3/9.3.4/9.3.5/10/11/12 (ARMv7, ARM64).

Виртуальные среды

- Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
- Microsoft Hyper-V 8/8.1/10 (x64);
- Citrix XenServer 7 (x64);
- VMWare WorkStation 11/12/14/15 (x86, x64);
- VMWare WorkStation Player 12/14/15 (x86, x64);
- VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64);
- Oracle VirtualBox 5.2 (x86, x64);
- RHEV 4 (x64).

Примечания:

1. Версия POSReady.

4. Основные характеристики СКЗИ

4.1. Размеры ключей

Размеры ключей электронной подписи:

- ключ электронной подписи — 256 бит или 512 бит;
- ключ проверки электронной подписи — 512 бит или 1024 бита.

Размеры ключей, используемых при шифровании:

- закрытый ключ — 256 бит или 512 бит;
- открытый ключ — 512 бит или 1024 бита;
- симметричный ключ — 256 бит.

4.2. Типы ключевых носителей

Используются ключевые носители:

- ГМД 3,5", USB диски;
- Смарткарты GEMALTO (GemSim1, GemSim2, Optelio, OptelioCL, OptelioCL2, Native);
- eToken, Jacarta;
- USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite Rutoken S;
- Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC;
- Рутокен S;
- Novacard;
- Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD);
- Смарткарта УЭК;
- Смарткарта MS_KEY K;
- Токен++ Lite;
- ESMART Token;
- Смарткарты Athena IDProtect, MorphoKST, Cha cardOS, Cha JCOP;
- Смарткарты Алиот INPASPOT Series, SCOne Series;
- Rosan;
- Раздел HDD ПЭВМ (в Windows - реестр);
- Идентификаторы Touch-Memory DS1995, DS1996.

Использование ключевых носителей в зависимости от программно-аппаратной платформы отражено в ЖТЯИ.00087-03 30 01. КриптоПро CSP. Формуляр, п. 3.8.

1. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.
2. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087–01 91 01. Руководство администратора безопасности общая часть).
3. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене.
4. Использование носителей других типов допускается только по согласованию с ФСБ России.

5. Структура и состав СКЗИ

5.1. Структура СКЗИ

Общая структура СКЗИ представлена на Рисунке 4.1.

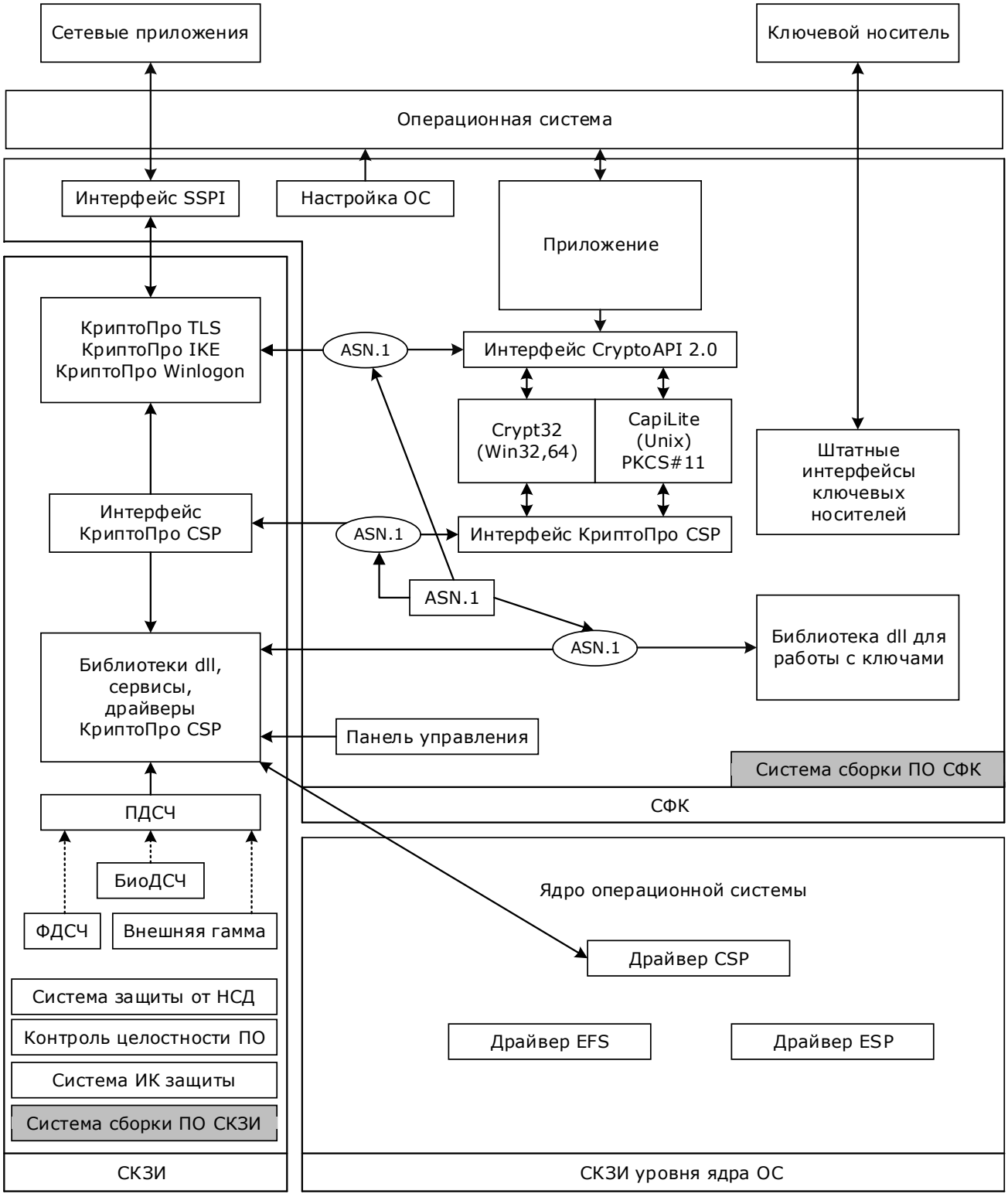


Рисунок 4.1 – Структура СКЗИ «КриптоПро CSP 4.0 R4».

5.2. Состав СКЗИ

Исполнение 1-Base класса защиты КС1 выполнено в следующем составе:

- криптопровайдер;
- криптодрайвер;
- модуль сетевой аутентификации (КриптоПро TLS);
- модуль обработки сертификатов и CMS протокола;
- утилита выработки внешней гаммы;
- утилита командной строки для шифрования файлов;
- утилита командной строки для работы с сертификатами;
- модуль аутентификации пользователя в домене Windows;
- пакет разработчика для использования протоколов IPsec (IPsec SDK);
- пакет разработчика для встраивания СКЗИ (CSP SDK);
- модуль поддержки интерфейса Mozilla NSS;
- сервисные модули (cpverify, wipefile, stunnel);
- библиотека, обеспечивающая подключение и функционирование ключевых носителей (RDK).

и функционирует в группах программно-аппаратных сред п.2.

5.3. Состав программного обеспечения

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 «КриптоПро Winlogon».
- Криптографический интерфейс «КриптоПро CSP».
- Программный датчик случайных чисел (ПДСЧ) с инициализацией от БиоДСЧ, внешней гаммы или физического ДСЧ (ФДСЧ) встраиваемого программно-аппаратного комплекса (ПАК) защиты от несанкционированного доступа (НСД).
- Модуль контроля целостности.
- Система инженерно-криптографической защиты.
- Система защиты от НСД (используется опционально).

5.4. Состав SDK СКЗИ

В состав SDK СКЗИ входят следующие документы, описывающие интерфейсы:

- CSP_4_0.chm;
- CAPILite_4_0.chm;
- SSPI_4_0.chm;
- reader_4_0.chm.

Так же в состав SDK СКЗИ входят примеры:

- rdk
- samples.

5.5. Состав подсистемы программной среды функционирования комплекса (СФК)

В состав подсистемы программной СФК входят следующие 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 Windows 2008/7/2008R2/8/2012/8.1/2012R2/10);
- 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 Windows 2008/7/2008R2/8/2012/8.1/2012R2/10;
- 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);
- КриптоПро Office Signature (в комплект поставки не входит);
- Штатные интерфейсы ключевых носителей;
- ASN.1 - система кодирования/декодирования данных в форматах ASN.1.

Состав модулей СКЗИ и подсистемы программной СФК для соответствующих программно-аппаратных сред конкретизируется в дополнениях ЖТЯИ.00087-03 91 02, ЖТЯИ.00087-03 91 03, ЖТЯИ.00087-03 91 04, ЖТЯИ.00087-03 91 05, ЖТЯИ.00087-03 91 06, ЖТЯИ.00087-03 91 07, ЖТЯИ.00087-03 91 08, ЖТЯИ.00087-03 91 09, ЖТЯИ.00087-03 91 10 к документу ЖТЯИ.00087-03 91 01 Руководство администратора безопасности. Общая часть.

Основной архитектурной особенностью СКЗИ «КриптоПро CSP» является то, что программная СФК 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, а дескриптор объекта не содержит его адрес в явном виде.

6. Применение СКЗИ

Возможны следующие применения КриптоПро CSP:

- Применение «КриптоПро CSP»КриптоПро CSP версии 4.0 R4 в составе стандартного программного обеспечения Microsoft и других компаний, использующих криптографический интерфейс в соответствии с архитектурой Microsoft (подробнее см. ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть);
- Встраивание «КриптоПро CSP»КриптоПро CSP версии 4.0 R4 во вновь разрабатываемое или существующее прикладное программное обеспечение (подробнее см. ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть и ЖТЯИ.00087-03 96 01. КриптоПро CSP. Руководство программиста).

7. Использование СКЗИ в стандартном программном обеспечении

Программное обеспечение СКЗИ позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509 совместно со следующим программным обеспечением Microsoft:

- Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows 2000 Server, Advanced Server, Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Windows 2012.
- Электронная почта - MS Outlook (Office 2003, Office 2007, Office 2010, Office 2013, Office 2016).
- Электронная почта - Microsoft Outlook Express в составе Internet Explorer/Microsoft Edge, Почта Windows Mail, Live Mail.
- Microsoft Word, Excel из состава Microsoft Office 2003, 2007, 2010, 2013, 2016 (с помощью плагина КриптоПро Office Signature).
- Microsoft Exchange Server 2010, 2013.
- 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/Microsoft Edge – web-сервер IIS, TLS-сервер, TLS-клиент (IE).
- Приложение командной строки для формирования запроса на сертификат certreq.
- SQL-сервер.
- ISA сервер.
- Сервер TMG
- Сервер UAG.
- Сервер терминалов и клиент (RDP).

Под управлением UNIX-подобных ОС СКЗИ используется совместно со следующим программным обеспечением:

- Apache Trusted TLS (Digt);
- Trusted TLS (Digt).

Примечание: Использование СКЗИ в стандартном программном обеспечении должно осуществляться в соответствии с п. 2 Правил пользования ЖТЯИ.00087-03 95 01.

Российские криптографические алгоритмы и сертификаты открытых ключей X.509 используются с указанным программным обеспечением в соответствии со следующими международными и российскими 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 их число входят: блочное шифрование по ГОСТ 28147-89 в режиме сцепления блоков (режиме CBC), режимы дополнения данных для блочного шифрования по ГОСТ 28147-89 в режиме 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 представления 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).
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Методические рекомендации по криптографическим алгоритмам, сопутствующим применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012».
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)».
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS».
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Рекомендации по стандартизации. Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012».
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Методические рекомендации по заданию узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89».
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 при согласовании ключей в протоколах IKE ISAKMP».

- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию дополнительных узлов замены ГОСТ 28147-89 для шифрования вложений IPsec ESP»
- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Системы обработки информации. Защита криптографическая. Техническая спецификация по использованию ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPsec AH и ESP.

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

СКЗИ может использоваться совместно со следующими программными продуктами разработки ООО «КРИПТО-ПРО»:

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

9. Встраивание СКЗИ

Архитектура СКЗИ 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.00087-03 96 01. «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.00087-03 96 01. КриптоПро CSP. «Руководство программиста» и соответствует интерфейсу Microsoft CSP.

10. Использование интерфейса CryptoAPI 2.0

СКЗИ может быть использовано прикладным программным обеспечением (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс CryptoAPI 2.0 (описание представлено в документации Microsoft Developer Network (MSDN)). 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 следующие цели:

- обеспечение доступа к криптографическим функциям на прикладном уровне (генерация ключей, создание/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 подсистема программной СФК 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 (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 v 4.0 R4 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», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Техническая спецификация. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».

СКЗИ КриптоПро CSP v 4.0 R4 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)», а также документа Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата 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

СКЗИ может взаимодействовать со следующими COM интерфейсами разработки Microsoft:

- CAPICOM;
- Certificate Enrollment Control;
- Certificate Enrollment API;
- Certificate Services.

10.2.1. 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/Microsoft Edge.

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

10.2.2. Certificate Enrollment Control (Windows Server 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 Server 2003.

10.2.3. Certificate Enrollment API (Windows 2008/7/2008R2/8/2012/8.1/2012 R2/10)

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 2008/7/2008R2/8/2012/8.1/2012R2/10.

10.2.4. Certificate Services

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

- способа 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», входящего в состав «КриптоПро PKI SDK» (ПАК «Службы УЦ»).

«КриптоПро ЭЦП Browser plug-in» содержит компоненту ActiveX для работы в Microsoft Internet Explorer/Microsoft Edge 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 «Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (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/Microsoft Edge, 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 хэш-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. Применение протоколов SSL/TLS (SSL - более ранние версии протокола) показано в Таблице 10.4.1.

Таблица 10.4.1 - Применение протокола SSL/TLS

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 SSL/TLS
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 пару сертификат открытого ключа/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/Microsoft Edge 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 сделать).

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) и 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 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.

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.

Соединение характеризуется следующими атрибутами:

- client_random – случайные 32 байта, задаваемые клиентом;
- server_random– случайные 32 байта, задаваемые сервером;
- client write MAC secret (ключ клиента для вычисления значения ключевой хэш–функции);
- server write MAC secret (ключ сервера для вычисления значения ключевой хэш–функции);
- 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.

Алгоритм преобразования информации при обмене с использованием протокола TLS включает следующие 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);
- вычисление значения ключевой хэш-функции (MAC) от конкатенации ключа хэш-функции, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента и заданной константы;
- конкатенация фрагмента и результата вычисления значения хэш-функции от него (расширенный фрагмент);
- зашифрование расширенного фрагмента (опционально);
- добавление открытого заголовка, содержащего тип сообщения (один байт), версию протокола TLS (два байта) и длину компрессированного фрагмента.

При приеме информации применяется обратная последовательность операций.

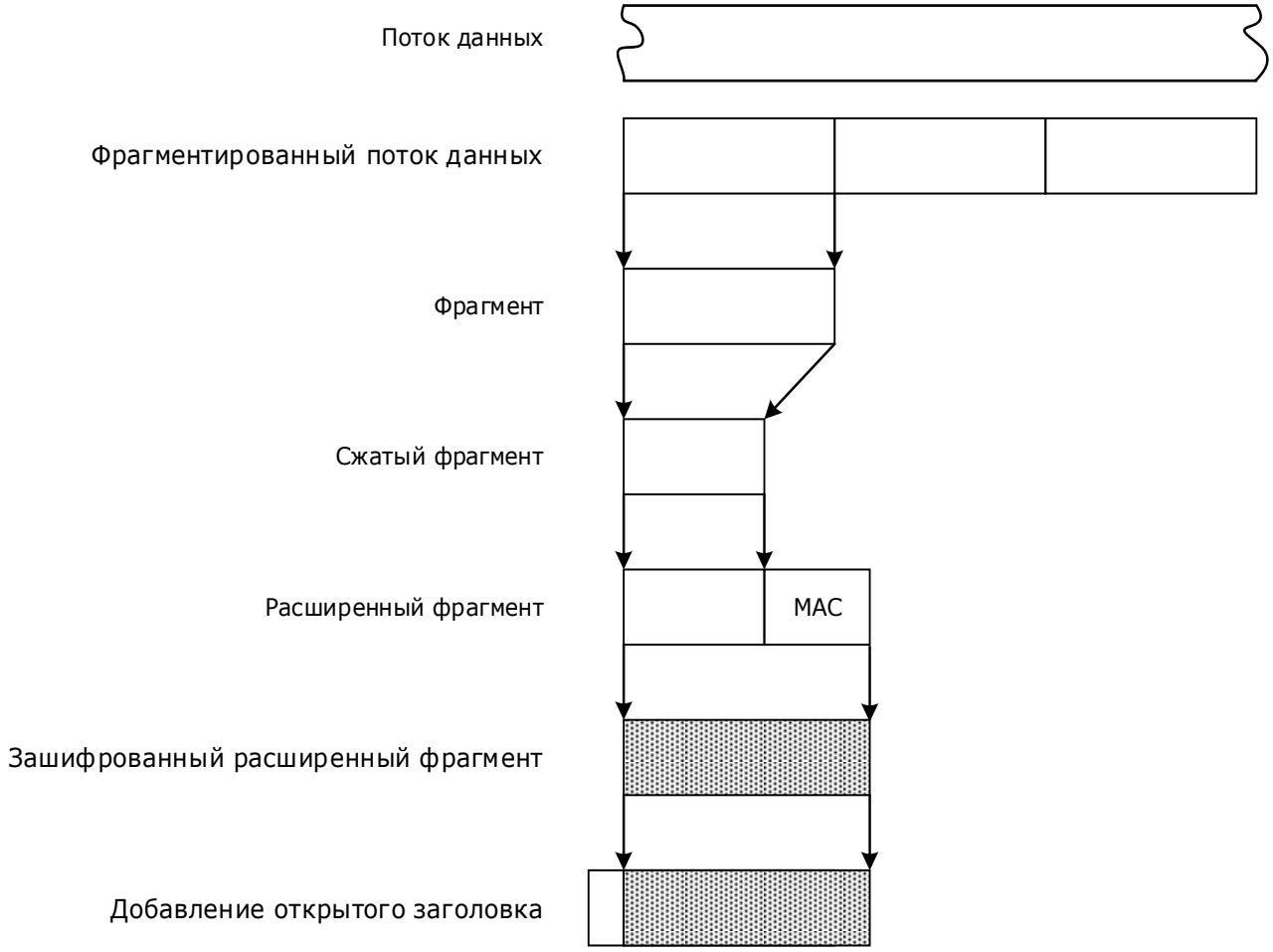


Рисунок 10.4.1 — Алгоритм преобразования информации при обмене с использованием протокола TLS

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).

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

TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением следующих 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.

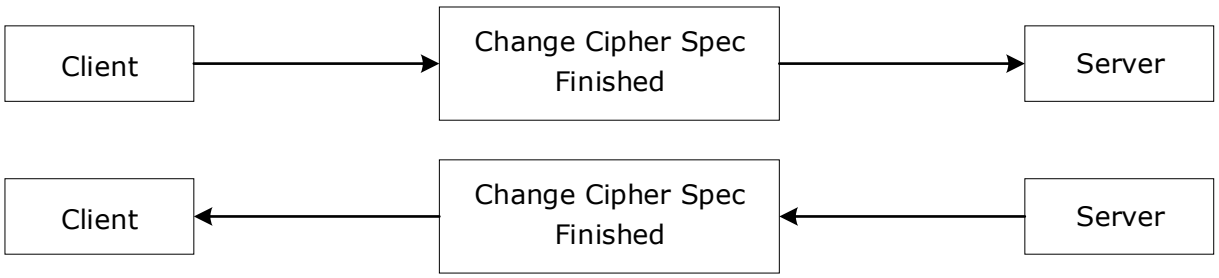
- клиент и сервер по pre_master secret, client_random и server_random формируют master secret (набор необходимой ключевой информации) сессии.

TLS Handshake Protocol работает по следующей схеме, представленной на Рисунке 10.4.2.

Установка версии протокола, идентификатора сессии, начального набора алгоритмов и параметров, метода компрессии.

Сервер посылает (опционально) свой сертификат и запрашивает (опционально) сертификат клиента, передача случайной величины server-random.

Клиент посылает свой сертификат (если был запрос сервера) Если сертификата у клиента нет, он посылает Certificate Verify.



Выбор алгоритмов и параметров для устанавливаемой сессии, завершение Handshake («рукопожатия»).

Рисунок 10.4.2 – Схема работы TLS Handshake 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 и ГОСТ Р 34.10-2012, алгоритмы

хэширования в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012). Используется также алгоритм Диффи-Хеллмана открытого распределения ключей на базе ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.

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.

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.

К такому сертификату предъявляются следующие требования:

- имя сертификата (Common name) должно совпадать с именем публикуемого Web-сервера прикладной системы. Например: pif.nikoil.ru;
- поле расширения сертификата «Использование ключа» должно содержать следующее назначение: «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 осуществляются через АРМ пользователя Центра регистрации. Порядок действий определяется в инструкции пользователю.

10.5. Приложение командной строки

Приложение командной строки предназначено для работы с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, создания/проверки электронной подписи и хэширования. Программа реализована в виде исполняемого файла «cryptcp.exe», подробнее см. ЖТЯИ.00087-03 93 01. Приложение командной строки для подписи и шифрования файлов.

10.6. Аутентификация в домене Windows

Для аутентификации пользователей в домене Microsoft Windows используется модуль «КриптоПро Winlogon», который предназначен для обеспечения контроля доступа пользователей к АРМ'у, как включенному в сеть домена, так и функционирующему локально. Используются Enterprise CA, КриптоПро УЦ или другие совместимые центры сертификации.

Модуль «КриптоПро Winlogon» реализует работу с российскими криптографическими алгоритмами для первого шага расширенного протокола Kerberos в соответствии с RFC 4556. Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), June 2006.

10.7. Использование функций CSP уровня ядра операционной системы

Модуль уровня ядра операционной системы позволяет использовать основные криптографические функции (шифрование/расшифрование, проверка подписи, вычисление значения хэш-функции) 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.00087-03 96 01. КриптоПро CSP. Руководство программиста».

10.8. Примеры использования СКЗИ «КриптоПро CSP» версии 4.0 R4

Для разработчиков в состав дистрибутива СКЗИ «КриптоПро CSP» версии 4.0 R4 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 форуме Крипто-Про (http://www.cryptopro.ru/CryptoPro/forum2/) ведется обсуждение по вопросам использования криптографических функций и сертификатов открытых ключей и ключей проверки ЭП.

Все вышеперечисленные варианты встраивания и использования СКЗИ «КриптоПро CSP» версии 4.0 R4 должны применяться с учетом п. 1.5 Формуляра. При этом указанные в настоящем документе интерфейсы являются уровнями встраивания СКЗИ «КриптоПро CSP» версии 4.0 R4 в прикладные системы и не являются приложениями, входящими в состав операционных систем.

11. История версий

11.1. «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 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. «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. «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» 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, 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 «КриптоПро CSP» 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. «КриптоПро CSP» версии 3.6

- Обновлен и расширен перечень программно-аппаратных сред функционирования «КриптоПро CSP» версии 3.6;
- 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;
- 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 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. «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.

11.6. «КриптоПро CSP» версии 3.8

- Добавлены механизмы управления лицензиями.

11.7. «КриптоПро CSP» версии 3.9

- Включено исполнение класса защиты КС3, функционирующее на программно-аппаратных платформах Windows 8/2012;
- Обеспечено функционирование СКЗИ на программно-аппаратных платформах Windows 8.1/2012R2.

11.8. «КриптоПро CSP» версии 4.0

- Реализована поддержка алгоритмов формирования и проверки электронной подписи по ГОСТ Р 34.10-2012;
- Реализована поддержка алгоритмов хэширования по ГОСТ Р 34.11-2012;
- Реализована поддержка алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012;
- Реализована поддержка Java-платформ с native-реализацией;
- Реализована поддержка устройств, работающих на ОС Android;
- Новый БиоДСЧ для устройств, работающих на ОС iOS и Android;
- Реализован модуль поддержки интерфейса Mozilla NSS;
- Обновлен и расширен перечень программно-аппаратных сред функционирования «КриптоПро CSP» версии 4.0;
- В связи с расширением поддерживаемых платформ «КриптоПро CSP» версии 4.0 реализовано в нескольких исполнениях, отличающихся программно-аппаратной средой функционирования, составом программных модулей и уровнем защиты.
- Для алгоритма ГОСТ Р 34.10-2012 реализована возможность вычисления кратной токи на основе эллиптических кривых в форме Эдвардса;
- Реализована интерфейсная надстройка над криптопровайдером в целях обеспечения возможности работы браузера Mozilla Firefox с использованием российских криптографических алгоритмов;

12. Информация для пользователей

Для получения дополнительной информации о данном продукте, а также 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