127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 5.0 КС1

1-Base

Описание реализации

ЖТЯИ.00101-01 90 01
Листов 23

2019 г

Содержание

Аннотация

Настоящий документ содержит описание реализации средства криптографической защиты информации КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base (далее — СКЗИ) и сведения о текущем состоянии продукта.

1 Назначение СКЗИ

СКЗИ КриптоПро CSP версии 5.0 КС1 представляет собой программный комплекс, предназначенный для реализации широкого набора решений по обеспечению криптографическими методами информационной безопасности на отдельных рабочих местах, в архитектуре «клиент-сервер», а также в информационных и телекоммуникационных системах различного назначения.

СКЗИ КриптоПро CSP может выступать как в качестве готового к применению средства, так и в качестве платформы для построения на его основе программных, программно-аппаратных и аппаратных решений в области обеспечения информационной безопасности, основанных на применении криптографических алгоритмов.

СКЗИ КриптоПро CSP предназначено для:

• авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур создания и проверки (с использованием сертификатов стандарта X.509 удостоверяющего центра) электронной подписи в соответствии со стандартами ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 34.10-2018 (с использованием ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ 34.11-2018);

• обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты в соответствии со стандартом ГОСТ 28147-89;

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

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

• установления аутентичного защищенного соединения с использованием протокола «КриптоПро TLS»;

• защиты IP-соединений («КриптоПро IPsec»);

• обеспечения конфиденциальности и контроля целостности и авторизация файлов и информационных сообщений;

• управления ключевыми элементами системы в соответствии с регламентом средств защиты.

СКЗИ КриптоПро CSP обеспечивает выполнение следующих функций:

1) защищенное хранение пользовательских ключей в ключевом контейнере с использованием шифрования, имитозащиты и аутентификации доступа;

2) шифрование, вычисление имитовставки, хэширование, создание/проверка ЭП;

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) защита IP-соединений («КриптоПро IPsec»).

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 и повтора электронного документа.

• 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, навязывающего 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, вредоносного ПО, модификации системного и прикладного ПО обеспечивается совместным использованием криптографических средств, средств антивирусной защиты и организационных мероприятий.

2 Основные характеристики СКЗИ

2.1 Программно-аппаратные среды функционирования СКЗИ

СКЗИ функционирует в программно-аппаратных средах, перечисленных в ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.2.

2.2 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.

2.3 Типы ключевых носителей

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.9.

Использование носителей других типов допускается только по согласованию с ФСБ России.

Примечание. 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.

3 Структура и состав СКЗИ

3.1 Структура СКЗИ

Общая структура СКЗИ представлена на рис. 1.

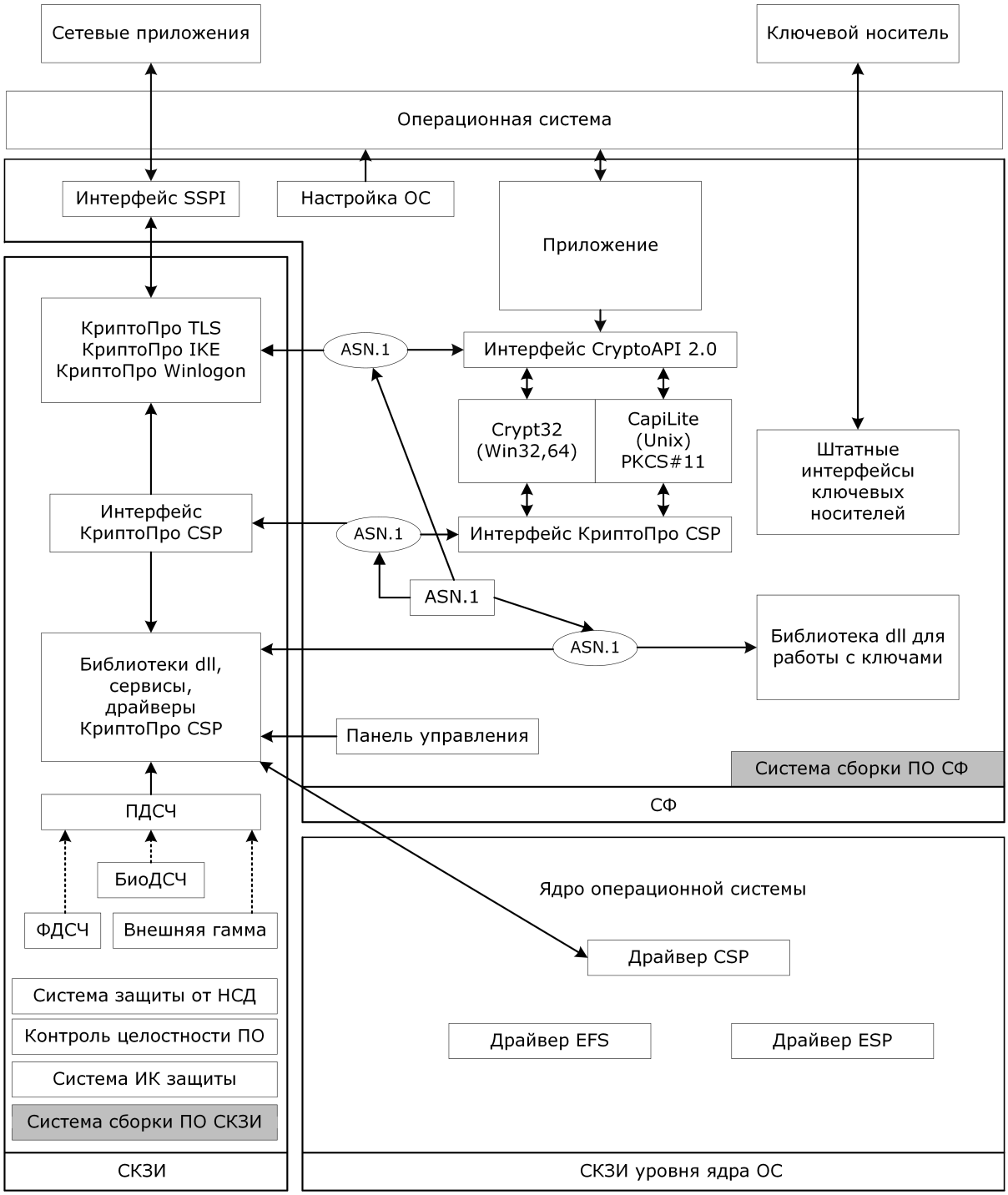


Рисунок 1. Структура СКЗИ КриптоПро CSP 5.0 КС1

3.2 Состав СКЗИ

СКЗИ КриптоПро CSP версии 5.0 КС1 выполнено в следующем составе:
- криптодрайвер (модуль на уровне ядра ОС)
- криптопровайдер
- модуль проверки статусов сертификатов открытых ключей «КриптоПро Revocation Provider»
- модуль защиты IP-соединений с использованием протоколов IPsec «КриптоПро IPsec»
- модуль сетевой аутентификации «КриптоПро TLS»
- модуль «КриптоПро JavaCSP»
- пакет разработчика для использования протоколов IPsec (IPsec SDK)
- пакет разработчика для встраивания СКЗИ (CSP SDK)
- пакет разработчика для создания библиотек модулей поддержки оборудования (RDK)
- кроссплатформенное графическое приложение «Инструменты КриптоПро»
- АРМ выработки внешней гаммы
- приложение командной строки для подписи и шифрования файлов cryptcp
- приложение командной строки для работы с сертификатами certmgr
- приложение для создания TLS-туннеля stunnel
- сервисные модули:
  - модуль контроля целостности cpverify
  - модуль безопасного удаления файлов и папок wipefile
- модуль обработки сертификатов и CMS протокола
- модуль поддержки интерфейса Microsoft CNG

3.3 Состав SDK СКЗИ

В состав SDK СКЗИ входят следующие документы, описывающие интерфейсы:
- CSP_5_0.chm;
- CAPILite_5_0.chm;
- SSPI_5_0.chm;
- PKCS11_5_0.chm;
- reader_5_0.chm.

Также в состав SDK СКЗИ входят примеры:
- rdk
- samples.

3.4 Состав подсистемы программной среды функционирования криптосредства (СФ)

В состав подсистемы программной СФ 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 (под управлением ОС Windows);

• 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;

• 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 подсистемы программной СФ для соответствующих программно-аппаратных сред

конкретизируется в дополнениях ЖТЯИ.00101-01 91 02, ЖТЯИ.00101-01 91 03, ЖТЯИ.00101-01 91 04, ЖТЯИ.00101-01 91 05, ЖТЯИ.00101-01 91 06, ЖТЯИ.00101-01 91 07, ЖТЯИ.00101-01 91 08, ЖТЯИ.00101-01 91 09, ЖТЯИ.00101-01 91 10, ЖТЯИ.00101-01 91 11, ЖТЯИ.00101-01 91 12 к документу ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть.

Основной архитектурной особенностью СКЗИ КриптоПро CSP является то, что программная СФ 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.

3.5 Получение прав на использование СКЗИ КриптоПро CSP

При использовании СКЗИ КриптоПро CSP версии 5.0 КС1 допускаются следующие способы получения подтверждения права использовать СКЗИ:

1) Ручной ввод лицензионных данных.

2) Получение данных из соответствующих расширений сертификатов ключей проверки электронной подписи в ключевом контейнере. Таким образом может передаваться право на использование СКЗИ КриптоПро CSP версии 5.0 КС1 при операциях с соответствующим ключом электронной подписи в рамках срока его действия.

Порядок действий, необходимых для ручного ввода лицензии, зависит от используемой платформы и подробно описан в соответствующих документах: ЖТЯИ.00101-01 92 01, ЖТЯИ.00101-01 91 03, ЖТЯИ.00101-01 91 04, ЖТЯИ.00101-01 91 05, ЖТЯИ.00101-01 91 06, ЖТЯИ.00101-01 91 07, ЖТЯИ.00101-01 92 02, ЖТЯИ.00101-01 91 09, ЖТЯИ.00101-01 91 10.

4 Реализуемые криптографические алгоритмы и протоколы

• Алгоритм шифрования/расшифрования данных и вычисления имитовставки реализован в соответствии с требованиями:

– **ГОСТ 28147-89** «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»

• Алгоритмы формирования и проверки ЭП реализованы в соответствии с требованиями:

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

– **ГОСТ Р 34.10-2012** «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

– **ГОСТ 34.10-2018** «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

• Алгоритмы выработки значения хэш-функции реализованы в соответствии с требованиями:

– **ГОСТ Р 34.11-94** «Информационная технология. Криптографическая защита информации. Функция хэширования»

– **ГОСТ Р 34.11-2012** «Информационная технология. Криптографическая защита информации. Функция хэширования»

– **ГОСТ 34.11-2018** «Информационная технология. Криптографическая защита информации. Функция хэширования»

• S-боксы, группы точек на эллиптических кривых, значения функций хэширования определены в документе RFC 4357, Федеральное агентство по техническому регулированию и метрологии (РОССТАНДАРТ), 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».

• Ключевая система СКЗИ КриптоПро CSP версии 5.0 КС1 обеспечивает возможность парно-выборочной связи абонентов сети с выработкой для каждого сеанса связи ключей на основе принципа открытого распределения ключей с использованием алгоритма Диффи-Хеллмана.

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), «ТС 26.2.002-2013. Информационная технология. Криптографическая защита информации. Использование ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPSEC и ESP».

• Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «ТС 26.2.001-2015. Информационная технология. Криптографическая защита информации. Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP».

• Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «ТС 26.2.001-2013. Информационная технология. Криптографическая защита информации. Использование ГОСТ 28147-89 и ГОСТ Р 34.10-2001 при согласовании ключей в протоколах IKE и ISAKMP».

• Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), «ТС 26.2.002-2014. Информационная технология. Криптографическая защита информации. Использование ГОСТ 28147-89 при шифровании вложений в протоколах IPSEC ESP».

5 Применение СКЗИ

Возможны следующие применения КриптоПро CSP:

• Применение КриптоПро CSP версии 5.0 КС1 в составе стандартного программного обеспечения Microsoft и других компаний, использующих криптографический интерфейс в соответствии с архитектурой Microsoft (подробнее см. разд. 6.1);

• Использование СКЗИ совместно с программными продуктами разработки ООО «КРИПТО-ПРО»;

• Встраивание КриптоПро CSP версии 5.0 КС1 во вновь разрабатываемое или существующее прикладное программное обеспечение (подробнее см. ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть и ЖТЯИ.00101-01 96 01. КриптоПро CSP. Руководство программиста, ЖТЯИ.00101-01 96 02. КриптоПро CSP. Руководство программиста JavaCSP и Android, ЖТЯИ.00101-01 96 03. КриптоПро CSP. Руководство программиста JavaTLS).

5.1 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 Server 2008/2008R2/2012/2012R2/2016.

• Электронная почта — Microsoft Outlook, входящая в пакет офисных программ Microsoft Office 2003, 2007, 2010, 2013, 2016, 2019.

• Электронная почта — Microsoft Outlook Express в составе Internet Explorer/Microsoft Edge, Почта Windows Mail, Live Mail.

• Microsoft Word, Excel, входящие в пакет офисных программ Microsoft Office 2003, 2007, 2010, 2013, 2016, 2019 (с помощью плагина КриптоПро Office Signature).

• Microsoft Exchange Server 2010, 2013, 2016.

• Средства контроля целостности ПО, распространяемого по сети — Microsoft Authenticode.

• Службы терминалов для Windows 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 разд. 1 Правил пользования ЖТЯИ.00101-01 95 01.

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

СКЗИ может использоваться совместно со следующими программными продуктами разработки ООО «КРИПТО-ПРО» без проведения дополнительных исследований (оценки влияния на КриптоПро CSP):

• КриптоПро УЦ

• Службы УЦ (КриптоПро OCSP, КриптоПро TSP, КриптоПро SVS, КриптоПро Revocation Provider)

• КриптоПро DSS

• КриптоПро HSM

- КриптоПро NGate
- КриптоПро ЭЦП Browser plug-in
- КриптоАРМ
- КриптоПро EFS
- КриптоПро Office Signature

Кроме того, обеспечена техническая совместимость СКЗИ с продуктами:
- КриптоПро SSF
- КриптоПро PDF

5.3 Встраивание СКЗИ

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

5.3.1 Встраивание на уровне CryptoAPI 2.0

СКЗИ может быть использовано в прикладном программном обеспечении (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс CryptoAPI 2.0 (подробнее см. Использование интерфейса CryptoAPI 2.0).

Встраивание на уровне CryptoAPI 2.0 позволяет воспользоваться набором функций, решающих большинство проблем, связанных с представлением (форматами) различных криптографических сообщений (подписанных, зашифрованных), способами представления открытых ключей в виде цифровых сертификатов, способами хранения и поиска сертификатов в различных справочниках, включая LDAP.

Функции CryptoAPI 2.0 позволяют полностью реализовать представление и обмен данными в соответствии с международными рекомендациями и Инфраструктурой Открытых Ключей (Public Key Infrastructure).

5.3.2 Встраивание на уровне CSP

СКЗИ может быть непосредственно использовано прикладным программным обеспечением с помощью загрузки модуля вызовом функции `LoadLibrary()`. Для этих целей в комплект поставки включается документ ЖТЯИ.00101-01 96 01. КриптоПро CSP. Руководство программиста, описывающий состав функций и тестовое ПО. При такой реализации прикладному ПО доступен лишь ограниченный набор низкоуровневых криптографических функций, соответствующий интерфейсу Microsoft CSP.

При использовании СКЗИ под управлением операционной системы iOS загрузка библиотек при помощи функции LoadLibrary() невозможна. Для этой операционной системы встраивание должно производиться в соответствии с документацией, входящей в состав фреймворка для разработки. Программный интерфейс, предоставляемый СКЗИ под управлением iOS, также описан в документе CAPILite_5_0.chm и соответствует интерфейсу Microsoft CSP.

6 Особенности реализации и использования СКЗИ

6.1 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 криптографического интерфейса CryptoAPI 2.0 позволяет:

• обеспечить доступ к криптографическим функциям на прикладном уровне (генерация ключей, создание/проверка электронной подписи, шифрование/расшифрование данных) в условиях 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.

• обеспечить возможность одновременного использования разных алгоритмов и различных их реализаций, как программных, так и аппаратных.

Общая архитектура криптографических функций в ОС Windows показана на рис. 2.

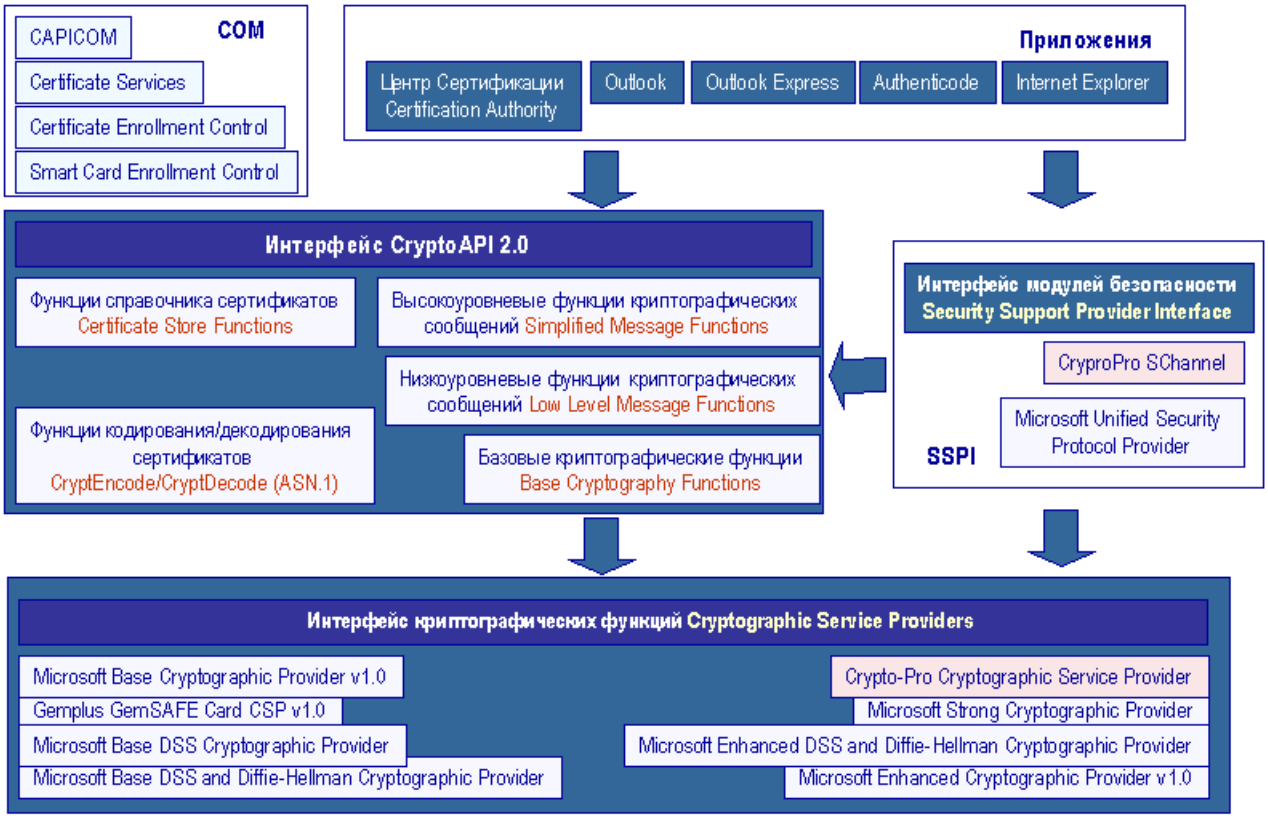


Рисунок 2. Архитектура криптографических функций в ОС Windows

Примечание. На Unix-платформах подсистема программной СФ 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.

6.1.1 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.

6.1.2 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 может быть отнесен набор функций, позволяющих расширить функциональность CryptoAPI 2.0 путем реализации и регистрации собственных типов объектов.

6.1.3 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.

6.1.4 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 версии 5.0 КС1 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 версии 5.0 КС1 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».

6.1.5 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.

6.2 Использование COM интерфейсов

СКЗИ может взаимодействовать со следующими COM интерфейсами разработки Microsoft:

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

6.2.1 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 создания 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.

6.2.2 Certificate Enrollment API

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 2008/7/2008R2/8/2012/8.1/2012R2/10/2016/2019.

6.2.3 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.

6.3 Использование СКЗИ в веб-браузерах

КриптоПро CSP может быть использован 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 на странице плагина по адресу на странице плагина.

6.4 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 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 табл. 1.

Таблица 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.

6.4.1 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 214 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.

Схема алгоритма представлена на рис. 3.

При приеме информации применяется обратная последовательность операций.

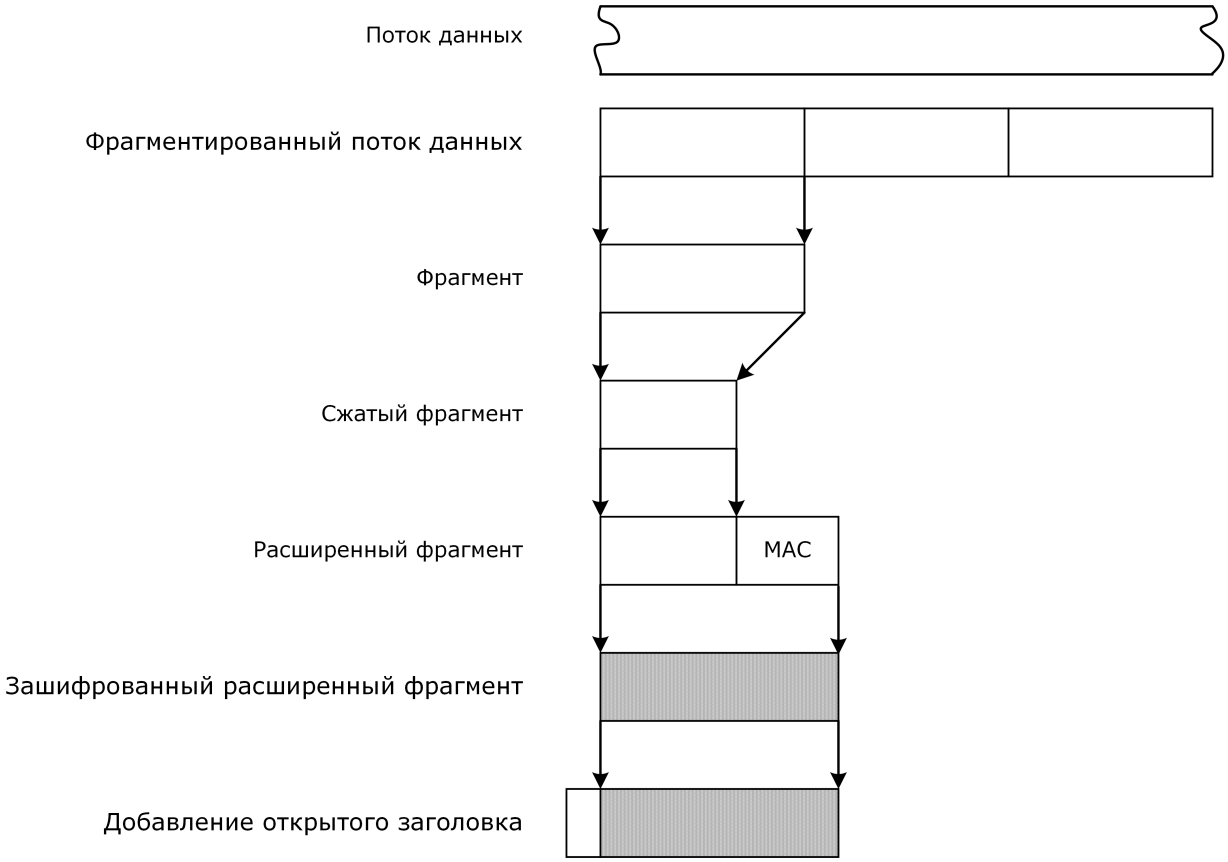


Рисунок 3. Алгоритм преобразования информации при обмене с использованием протокола TLS

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.

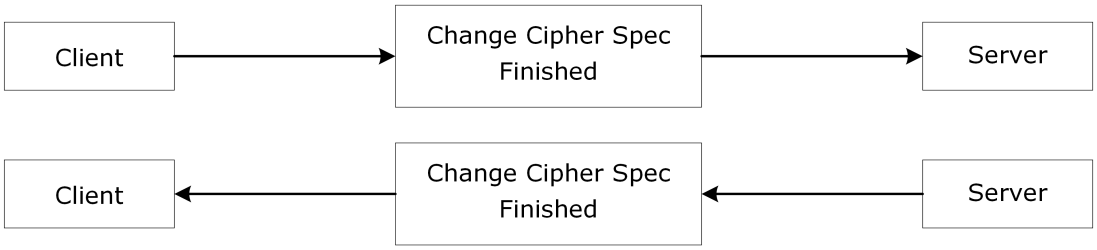
TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением следующих операций:
- клиент и сервер договариваются об используемых в сессии алгоритмах и параметрах защиты, обмениваются случайными величинами client_random, server_random, договариваются, будут или нет новые соединения;
- 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 схеме, представленной на рис. 4.

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 4. Схема работы TLS Handshake Protocol

6.4.2 Модуль сетевой аутентификации «КриптоПро TLS»

Модуль сетевой аутентификации «КриптоПро TLS» реализован на базе протокола TLS 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 (ГОСТ 34.10-2018), алгоритмы хэширования в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018)). Также используется алгоритм Диффи-Хеллмана открытого распределения ключей на базе ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018).

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. 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.

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.

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.

6.5 Приложения командной строки

В состав дистрибутива КриптоПро CSP версии 5.0 КС1 входят следующие приложения:
- **Приложение командной строки для подписи и шифрования файлов** предназначено для работы с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, создания/проверки электронной подписи и хэширования (подробнее см. ЖТЯИ.00101-01 93 01. КриптоПро CSP. Приложение командной строки для подписи и шифрования файлов).
- **Приложение командной строки для работы с сертификатами** используется для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами сертификатов (подробнее см. ЖТЯИ.00101-01 93 02. КриптоПро CSP. Приложение командной строки для работы с сертификатами).
- **Приложение для создания TLS-туннеля** предназначено для создания TLS защищенного соединения между клиентом и локальным (Inetd-запускаемым) или удаленным сервером (подробнее см. ЖТЯИ.00101-01 93 03. КриптоПро CSP. Приложение для создания TLS-туннеля).
- **Приложение csptest** предназначено для выполнения отдельных настроек СКЗИ, а также для тестирования и апробации технических решений, построенных с использованием СКЗИ.

Примечание. Утилиту csptest допускается использовать только в **тестовых целях**.

6.6 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.00101-01 96 01. КриптоПро CSP. Руководство программиста.

6.7 Примеры использования СКЗИ КриптоПро CSP версии 5.0 КС1

Для разработчиков в состав дистрибутива СКЗИ КриптоПро CSP версии 5.0 КС1 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 5.0 КС1 должны применяться с учетом п. 1.5 Формуляра. При этом указанные в настоящем документе интерфейсы являются уровнями встраивания СКЗИ КриптоПро CSP версии 5.0 КС1 в прикладные системы и не являются приложениями, входящими в состав операционных систем.

7 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

WWW: http://www.cryptopro.ru

Портал технической поддержки: https://support.cryptopro.ru

E-mail: info@cryptopro.ru

Форум: https://www.cryptopro.ru/forum2