127 018, Москва, Сущевский вал, д.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 КС 2

2-Base

Руководство программиста

ЖТЯИ.00088-01 96 01

Листов 12

2016 г.

Аннотация

Настоящий документ описывает состав функций и тестовое ПО СКЗИ «КриптоПро CSP» и предназначен для разработки прикладного ПО с непосредственным вызовом функций СКЗИ, а также определяет требования к операционным системам при встраивании СКЗИ.

1. Описание программных интерфейсов

Использование низкоуровневого интерфейса криптопровайдера, позволяющего выполнять такие функции как генерация и работа с ключами, шифрование/расшифрование данных, хэширование и электронная подпись, описывается в файле

CSP_4_0.chm - System Program Interface (CryptoAPI).

При использовании данного типа дистрибутивов для аутентификации требуется использовать дополнительные механизмы.

Использование интерфейса SSPI, обеспечивающего реализацию протокола TLS, обеспечивающего работу с пакетами безопасности при выборе и инициализации пакета, с удостоверениями субъектов безопасности, установление соединений, передачу данных, распределение памяти, описывается в файле

SSPI_4_0.chm - Security Support Provider Interface (SSPI).

Использование высокоуровневого интерфейса CryptoAPI, обеспечивающего набор функций для обработки сертификатов, списков отозванных сертификатов, расширенного использования ключа, работы с провайдером, выработки значения функции хэширования и электронной подписи, зашифрования и расшифрования данных, работы с хранилищем сертификатов и поддержки идентификатора объекта, описано в файле

CAPILite_4_0.chm - CryptoAPI Lite (CAPILite).

Общая информация, используемая для создания модуля поддержки считывателей, носителей и датчиков случайных чисел, содержащая необходимые описания и определения, содержится в файле

reader_4_0.chm

Интерфейс PKCS#11, реализующий базовое описание RSA Labs v2.30, с доработками в соответствии с требованиями поддержки российских стандартов на реализацию криптографических функций.

PKCS11_4_0.chm

Совместно с дистрибутивом поставляются следующие пакеты, позволяющие интегрировать «КриптоПро CSP» версии 4.0 в приложения, использующие OpenSSL API (такие как Web-сервер ngnix): cprocsp-cpopenssl, cprocsp-cpopenssl-base, cprocsp-cpopenssl-devel, cprocsp-cpopenssl-gost.

Подробнее об их установке и настройке можно узнать на портале техподдержки и форуме КриптоПро.

2. Требования к операционной системе для встроенного применения. Linux.

СКЗИ для своего функционирования требует следующие библиотеки базовой операционной системы:

LSB 4.x, раздел III. Base Libraries

Список необходимых библиотек по пакетам:

cprocsp-curl
libc.so.6
libdl.so.2
libgcc_s.so.1
libidn.so.11
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
librt.so.1
libstdc++.so.6
libz.so.1
linux-gate.so.1

cprocsp-ipsec-ike
libc.so.6
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libstdc++.so.6
linux-gate.so.1

cprocsp-npcades
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

cprocsp-rdr-gui
libc.so.6
libdl.so.2
libgcc_s.so.1
libICE.so.6
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libSM.so.6
libstdc++.so.6
libuuid.so.1
libX11.so.6
libXau.so.6
libxcb.so.1
libXdmcp.so.6
libXext.so.6
libXm.so.3
libXmu.so.6
libXp.so.6
libXt.so.6
linux-gate.so.1

cprocsp-rdr-pcsc
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

cprocsp-rsa
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-cades
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-capilite
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-kc1
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libncurses.so.5
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-kc2
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-ocsp-util
libc.so.6
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-pkcs11

libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-rdr
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0

libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-rdr-fkc
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

lsb-cprocsp-rdr-sobol
libc.so.6
libdl.so.2
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

rtsupcp
libc.so.6
libgcc_s.so.1
/lib/ld-linux.so.2
libm.so.6
libpthread.so.0
libstdc++.so.6
linux-gate.so.1

Кроме того, пакету lsb-cprocsp-capilite для работы с сетью необходим либо пакет cprocsp-curl либо пакет curl (последний можно взять из дистрибутива ОС, из поставки CSP или с сайта разработчика: http://curl.haxx.se/). При отсутствии этого пакета базовая функциональность сохранится, но такие функции работы с сетью как автоматическое выкачивание CRL или запрос сертификата на УЦ через утилиту cryptcp будут не доступны.

Пакету lsb-cprocsp-rdr-pcsc для работы со смарт-картами необходим пакет libpcsclite из дистрибутива ОС. В зависимости от того, какой используется дистрибутив Linux название пакета может варьироваться (libpcsclite, libpcsclite1).

LSB 4.x, раздел VI. Commands and Utilities

Для установки необходимого пакета lsb-cprocsp-base требуются утилиты:

'cat'
'chmod'
'cp'
'crontab'
'echo'
'fgrep'
'grep'
'ln'
'mkdir'
'rm'
'sed'
'sysctl'
'test'
'true'
'dpkg' * только для Debian и Ubuntu

Для установки всех остальных пакетов за исключением cprocsp-drv-devel достаточно подмножества этих утилит. Для установки cprocsp-drv-devel также необходима утилита

'uname'

LSB 4.x, раздел VI. Execution Environment 16. File System Hierarchy

Необходимы следующие разделы со следующими возможностями:

Таблица 2.1 – Необходимые разделы

/opt/cprocsp	После установки дистрибутива для функционирования продукта достаточно прав только на чтение.
/etc/opt/cprocsp	После установки дистрибутива для функционирования продукта достаточно прав только на чтение. При изменении настроек, а также при операциях с лицензией также необходимы права на запись.
/var/opt/cprocsp	Во время работы с CSP необходимы права на чтение и на запись. Содержимое директории должно сохраняться между перезагрузками.

При использовании в качестве отчуждаемого ключевого носителя дискет ожидается, что дискетам соответствуют устройства

/dev/fd0, /dev/fd1 и так далее.

LSB 4.0, раздел VIII. System Initialization 20. System Initialization 20.1. Cron Jobs

Необходимо базовое функционирование cron .

Для использования в качестве отчуждаемого ключевого носителя USB flash drive необходимо функционирование службы udev.

LSB 4.0, раздел X. Package Format and Installation

Необходима поддержка механизма установки rpm.

3. Требования к операционной системе для встроенного применения. Solaris.

СКЗИ для своего функционирования требует следующие библиотеки базовой операционной системы:

libc_psr.so.1
libmd_psr.so.1
libCstd_isa.so.1
libnspr_flt4.so
libCrun.so.1
libCstd.so.1
libICE.so.6
libSM.so.6
libX11.so.4
libXext.so.0
libXm.so.4
libXt.so.4
libXtsol.so.1
libadm.so.1
libaio.so.1
libbsm.so.1
libc.so.1
libcmd.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
lib/libldap.so.5
libm.so.1
libm.so.2
libmd.so.1
libmp.so.2
libnsl.so.1
libnspr4.so
libnss3.so
libplc4.so
libplds4.so
libpthread.so.1
librt.so.1
libsasl.so.1
libscf.so.1
libsecdb.so.1
libsocket.so.1
libsoftokn3.so
libssl3.so
libthread.so.1
libtsol.so.2
libuutil.so.1
libvolmgt.so.1
libz.so.1

Список необходимых библиотек по пакетам:

CPROCades
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libm.so.2
libmd.so.1
libpthread.so.1
librt.so.1
libthread.so.1

CPROcpl
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libm.so.2
libmd.so.1
libpthread.so.1
librt.so.1
libthread.so.1
libnsl.so.1
libnspr4.so
libnss3.so
libnssutil3.so
libplc4.so
libplds4.so
libpthread.so.1
librt.so.1
libsasl.so.1
libscf.so.1
libsocket.so.1
libssl3.so
libthread.so.1
libuutil.so.1
libz.so.1

CPROcurl
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
libldap.so.5
libm.so.2
libmd.so.1
libmp.so.2
libnsl.so.1
libnspr4.so

libnss3.so
libnssutil3.so
libplc4.so
libplds4.so
libpthread.so.1
librt.so.1
libsasl.so.1
libscf.so.1
libsocket.so.1
libssl3.so
libthread.so.1
libuutil.so.1
libz.so.1

CPROkc1
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libcurses.so.1
libdl.so.1
libm.so.2
libmd.so.1
libpthread.so.1
librt.so.1
libthread.so.1

CPROkc2
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
libm.so.2
libmd.so.1
libmp.so.2
libnsl.so.1
libpthread.so.1
librt.so.1
libthread.so.1
libuutil.so.1

CPROOCSPut
libc.so.1
libCrun.so.1
libCstd.so.1
libm.so.2
libc.so.1
libCrun.so.1
libCstd.so.1
libm.so.2

CPROrdfk
libadm.so.1
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libgen.so.1
libm.so.2
libmd.so.1
libpthread.so.1
librt.so.1
libthread.so.1
libvolmgt.so.1

libadm.so.1
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libgen.so.1
libm.so.2
libmd.so.1
libpthread.so.1
librt.so.1
libthread.so.1
libvolmgt.so.1

CPROrdg
libaio.so.1
libbsm.so.1
libc.so.1
libcmd.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
libICE.so.6
libm.so.2
libmd.so.1
libmp.so.2
libnsl.so.1
libpthread.so.1
librt.so.1
libscf.so.1
libsecdb.so.1
libSM.so.6
libsocket.so.1
libthread.so.1
libtsol.so.2
libuutil.so.1
libX11.so.4
libXext.so.0
libXm.so.4
libXt.so.4
libXtsol.so.1
libaio.so.1
libbsm.so.1
libc.so.1
libcmd.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
libICE.so.6

libm.so.2
libmd.so.1
libmp.so.2
libnsl.so.1
libpthread.so.1
librt.so.1
libscf.so.1
libsecdb.so.1
libSM.so.6
libsocket.so.1
libthread.so.1
libtsol.so.2
libuutil.so.1
libX11.so.4
libXext.so.0
libXm.so.4
libXt.so.4
libXtsol.so.1

CPROrdp
libaio.so.1
libc.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
libm.so.2
libmd.so.1
libmp.so.2
libnsl.so.1
libpthread.so.1
librt.so.1
libscf.so.1
libsocket.so.1
libthread.so.1
libuutil.so.1

CPROrdr
libadm.so.1
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libgen.so.1
libm.so.2
libmd.so.1
libpthread.so.1
librt.so.1
libthread.so.1
libvolmgt.so.1

Кроме того, пакету CPROcpl для работы с сетью необходим либо пакет CPROcurl из поставики CSP либо пакет curl (последний можно взять из дистрибутива ОС, из поставки CSP или с сайта разработчика: http://curl.haxx.se/). При отсутствии этого пакета базовая функциональность сохранится, но такие функции работы с сетью как автоматическое выкачивание CRL или запрос сертификата на УЦ через утилиту cryptcp будут не доступны.

Пакету CPROrdp для работы со смарт-картами необходим пакет pcsclite (например, пакет SUNWpcsclite из дистрибутива ОС).

Требования к системным утилитам.

Для установки необходимых пакетов CPRObase CPROrdr необходимо функционирование утилит:

'cat'
'chmod'
'cp'
'crontab'
'echo'
'fgrep'
'grep'
'ln'
'mv'
'rm'
'sed'
'sysctl'

'test'

'true'

Для установки всех остальных пакетов за исключением CPROdrv и CPROdrvd достаточно подмножества этих утилит. Для установки CPROdrv также необходимы утилит:

'add_drv'

'isainfo'

'rem_drv'

'sync'

Для установки CPROdrvd:

'add_drv'

'isainfo'

'rem_drv'

'sync'

'uname'

Требования к файловой системе.

Необходимы следующие разделы со следующими возможностями:

Таблица 3.1 – Необходимые разделы

/opt/cprocsp	После установки дистрибутива для функционирования продукта достаточно прав только на чтение.
/etc/opt/cprocsp	После установки дистрибутива для функционирования продукта достаточно прав только на чтение. При изменении настроек, а также при операциях с лицензией также необходимы права на запись.
/var/opt/cprocsp	Во время работы с CSP необходимы права на чтение и на запись. Содержимое директории должно сохраняться между перезагрузками.

Требования к службам.

Необходимо базовое функционирование cron.

Для работы с отчуждаемыми носителями типа «дискета» и «USB flash drive» необходимо функционирование службы Volume Management.

Требования к системе управления пакетами.

Необходимо штатное функционирование системы управления пакетами.

4. Требования к использованию функций

Необходимо выполнять контроль кодов ошибок, возникающих при отклонениях от штатного выполнения команд.

Таблица 4.1 – Перечень возможных ошибок.

Код ошибки (DEC)	Код ошибки (HEX)	Описание ошибки
536871012	20000064	Мало памяти
536871013	20000065	Не удалось открыть файл
536871014	20000066	Операция отменена пользователем
536871015	20000067	Некорректное преобразование BASE64
536871016	20000068	Если указан параметр '-help', то других быть не должно
536871112	200000C8	Указан лишний файл
536871113	200000C9	Указан неизвестный ключ
536871114	200000CA	Указана лишняя команда
536871115	200000CB	Для ключа не указан параметр
536871116	200000CC	Не указана команда
536871117	200000CD	Не указан необходимый ключ:
536871118	200000CE	Указан неверный ключ:
536871119	200000CF	Параметром ключа '-q' должно быть натуральное число
536871120	200000D0	Не указан входной файл
536871121	200000D1	Не указан выходной файл
536871122	200000D2	Команда не использует параметр с именем файла
536871123	200000D3	Не указан файл сообщения
536871212	2000012C	Не удалось открыть хранилище сертификатов:
536871213	2000012D	Сертификаты не найдены
536871214	2000012E	Найдено более одного сертификата (ключ '-1')
536871215	2000012F	Команда подразумевает использование только одного сертификата
536871216	20000130	Неверно указан номер
536871217	20000131	Нет используемых сертификатов
536871218	20000132	Данный сертификат не может применяться для этой операции
536871219	20000133	Цепочка сертификатов не проверена
536871220	20000134	Криптопровайдер, поддерживающий необходимый алгоритм, не найден
536871221	20000135	Неудачный ввод пароля ключевого контейнера
536871312	20000190	Не указана маска файлов
536871313	20000191	Указаны несколько масок файлов
536871314	20000192	Файлы не найдены
536871315	20000193	Задана неверная маска
536871316	20000194	Неверный хэш
536871412	200001F4	Ключ '-start' указан, а выходной файл нет
536871413	200001F5	Содержимое файла - не подписанное сообщение
536871414	200001F6	Неизвестный алгоритм подписи
536871415	200001F7	Сертификат автора подписи не найден
536871416	200001F8	Подпись не найдена
536871417	200001F9	Подпись не верна
536871418	20000200	Штамп времени не верен
536871512	20000258	Содержимое файла - не зашифрованное сообщение
536871513	20000259	Неизвестный алгоритм шифрования

Код ошибки (DEC)	Код ошибки (HEX)	Описание ошибки
536871514	2000025A	Не найден сертификат с соответствующим секретным ключом
536871612	200002BC	Не удалось инициализировать COM
536871613	200002BD	Контейнеры не найдены
536871614	200002BE	Не удалось получить ответ от сервера
536871615	200002BF	Сертификат не найден в ответе сервера
536871616	200002C0	Файл не содержит идентификатор запроса:
536871617	200002C1	Некорректный адрес ЦС
536871618	200002C2	Получен неверный Cookie какие функции работают с cookie?
536871712	20000320	Серийный номер содержит недопустимое количество символов
536871713	20000321	Неверный код продукта
536871714	20000322	Не удалось проверить серийный номер
536871715	20000323	Не удалось сохранить серийный номер
536871716	20000324	Не удалось загрузить серийный номер
536871717	20000325	Лицензия просрочена

Примечание: кроме кодов, приведенных в таблице, приложение может возвращать код любой системной ошибки.

5. Особенности использования режима усиленного контроля использования ключей

Режим усиленного контроля использования ключей, необходимый для использования в СКЗИ вне тестовой эксплуатации, осуществляет контроль доверенности открытых ключей, срока действия ключей подписи и ключевого обмена, а также корректности инициализации программных ДСЧ. Это накладывает дополнительные требования к выполнению ряда операций, функционал которых предоставляется криптопровайдером.

1) Функции, при выполнении которых предполагается выработка случайных данных (CryptGenKey для временных ключей, CryptGenRandom), будут возвращать ошибку, если программный ДСЧ не был инициализирован с физического ДСЧ и провести инициализацию в данный момент невозможно (например, в системе не установлен ни один физический ДСЧ). Для исправления ошибки следует произвести установку хотя бы одного физического ДСЧ (например, внешней гаммы, аппаратного ДСЧ), после чего произвести инициализацию программного ДСЧ одним из следующих способов:

   а) воспользоваться утилитой csptest:

   # ./csptest -keyset -verifycontext -hard_rng

   б) произвести выработку долговременного ключа с помощью функции CryptGenKey;

   в) произвести вызов функции CryptSetProvParam с флагом PP_USE_HARDWARE_RNG.

2) Функция CryptVerifySignature() принимает на вход дескриптор открытого ключа, с помощью которого производится проверка подписи. При включённом режиме усиленного контроля использования ключей допустимо передавать этой функции дескрипторы следующих ключей:

   а) Дескриптор ключа, извлечённого из контейнера (AT_SIGNATURE, AT_KEYEXCHANGE).

   б) Дескриптор ключа, полученного из сертификата открытого ключа. Для получения этого дескриптора необходимо получить структуру CERT_CONTEXT, содержащую информацию о необходимом сертификате, с помощью функций CertCreateCertificateContext/CertFindCertificateInStore. Затем требуется вызвать функцию CryptImportPublicKeyInfoEx, передав ей указатель на структуру CERT_CONTEXT.pCertInfo.SubjectPublicKeyInfo типа CERT_PUBLIC_KEY_INFO. Функция CryptImportPublicKeyInfoEx вернёт необходимый дескриптор.

3) Функции, использующие долговременные ключи, будут возвращать ошибку, в случае если их срок действия истёк. Срок действия ключей ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012 составляет 1 год 3 месяца. Получить информацию о сроке действия ключа можно с помощью контрольной панели КриптоПро CSP (закладка «Сервис» > Протестировать), либо осуществить вызов функции CryptGetKeyParam с параметром KP_NOTAFTER.

4) Для обеспечения контроля доверенности сертификатов открытых ключей при использовании СКЗИ под управлением ОС Windows при наличии корневого сертификата, установленного в доверенное хранилище КриптоПро локального компьютера («Доверенные корневые сертификаты КриптоПро CSP», "CryptoPro Trusted Roots", CryptoProTrustedStore), осуществляется построение цепочки сертификатов. В случае, если такую цепочку построить невозможно, функция CertFindCertificateInStore, на вход которой передаётся структура CERT_CONTEXT, соответствующая недоверенному сертификату, и функция проверки подписи CMS (CryptMsgControl), в случае если CMS-подпись не содержит указание на доверенный сертификат, будут завершаться с ошибкой. Для того, чтобы избавится от ошибки, необходимо установить необходимый корневой сертификат в доверенное хранилище КриптоПро (см. Руководство Администратора безопасности Windows).