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 3.9

Руководство программиста

ЖТЯИ.00083-01 90 05

Листов 31

2016

Аннотация

Настоящий документ описывает состав функций и тестовое ПО СКЗИ ЖТЯИ.00083-01 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, хеширование и электронная подпись, описывается в файле

CSP_3_9.chm - System Program Interface (CryptoAPI).

Дистрибутивы с приставкой mini представляют собой форму исполнения КС1, реализующую функции СКЗИ, такую, что регистрация в операционной системе не предусматривается. Вопрос целостности данного исполнения должен обеспечиваться разработчиком приложений.

Дистрибутивы с приставкой web представляют собой форму исполнения КС1, реализующую функции СКЗИ, такую, что в ней отсутствуют модули поддержки ключевых носителей.

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

Файл CSP_3_9.chm в полном объеме относятся к дистрибутивам mini.

Файл CSP_3_9.chm относится к дистрибутивам web в части документации, которая определяет функциональность с признаком verify context.

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_3_9.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_3_9.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_3_9.chm

Документация по использованию модулей криптографической поддержки протоколов IKEv1, AH и ESP содержится в файле.

ikespah.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_3_9.chm

Совместно с дистрибутивом поставляются следующие пакеты, позволяющие интегрировать «КриптоПро CSP» версии 3.9 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.

Для встроенных применений должны быть включены компоненты и подсистемы базовой ОС:

LSB 4.0, 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 4.0, 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 3.1, раздел VI. Execution Environment 16. File System Hierarchy

Необходимы следующие разделы со следующими возможностями:

/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.

Для встроенных применений должны быть включены компоненты и подсистемы базовой ОС:

1. Требования к наличию библиотек и пакетов.

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
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
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

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
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
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
libscf.so.1
libsocket.so.1
libthread.so.1
libuutil.so.1
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
libscf.so.1
libsocket.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
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

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).

2. 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'

3. Требования к файловой системе.

Необходимы следующие разделы со следующими возможностями:

/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.

4. Требования к службам.

Необходимо базовое функционирование cron .

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

5. Требования к системе управления пакетами.

Необходимо штатное функционирование системы управления пакетами.

4. Использование программных интерфейсов

Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» v. 3.9 с учетом п.1.5. Формуляра ЖТЯИ.00083-01 30 01 может производиться без создания новых СКЗИ в случае использования вызовов из приведенного ниже перечня в соответствии с документацией.

В случае использования прочих вызовов необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» v. 3.9 с учетом п.1.5. Формуляра ЖТЯИ.00083-01 30 01 возможно без дополнительных тематических исследований

Функция	**Описание**	**Ограничения на использование функции**
Функции инициализации и настройки провайдера		
CryptAcquireContext	Функция CryptAcquireContext() используется для создания дескриптора криптопровайдера с именем ключевого контейнера, определённым параметром pszContainer	
CryptReleaseContext	Функция CryptReleaseContext() используется для удаления дескриптора криптопровайдера, созданного CryptAcquireContext().	
CryptContextAddRef	Управляет счетчиком дескрипторов созданного CryptAcquireContext().	
CryptEnumProviders	Перечисление установленных криптопровайдеров	
CryptEnumProviderTypes	Перечисление установленных типов криптопровайдеров	
CryptGetDefaultProvider	Получение контекста провайдера, установленного в системе по умолчанию	
CryptGetProvParam	Функция CryptGetProvParam() получает	

	параметры криптопровайдера.	
CryptSetProvParam	Функция CryptSetProvParam() устанавливает параметры криптопровайдера.	
FreeCryptProvFromCertEx	Функция используется для удаления дескриптора криптопровайдера, созданного CryptAcquireContext() или через CNG.	
CryptInstallDefaultContext, CryptSetProvider, CryptSetProviderEx, CryptUninstallDefaultContext	Функции управления контекстом провайдера по умолчанию	
Функции генерации и обмена ключами, создание конфигурирование и удаление ключей		
CryptGenKey	Функция CryptGenKey() генерирует случайные криптографические ключи или ключевую пару (закрытый/открытый ключи).	
CryptDestroyKey	Функция CryptDestroyKey() удаляет ключ, передаваемый через параметр hKey. После удаления ключ (дескриптор ключа) не может использоваться.	
CryptExportKey	Функция CryptExportKey() используется для экспорта криптографических ключей из ключевого контейнера криптопровайдера, сохраняя их в защищённом виде.	Разрешено экспортировать только открытые ключи (PUBLICKEYBLOB).
CryptGenRandom	Функция CryptGenRandom() заполняет буфер случайными байтами.	
CryptGetKeyParam	Функция CryptGetKeyParam() возвращает параметры ключа.	
CryptGetUserKey	Функция CryptGetUserKey() возвращает дескриптор одной из долговременных ключевых пар в ключевом контейнере.	
CryptImportKey	Функция CryptImportKey() используется для импорта криптографического ключа из ключевого блоба в контейнер	Разрешено импортировать только открытые ключи (PUBLICKEYBLOB).

	криптопровайдера.	
CryptSetKeyParam	Функция CryptSetKeyParam() устанавливает параметры ключа.	Разрешено использование только со следующими символьными аргументами: KP_CERTIFICATE, KP_CIPHEROID, KP_DHOID, KP_HASHOID.
Функции обработки криптографических сообщений		
CryptSignMessage	Функция CryptSignMessage создает хэш определенного содержания, подписывает хэш и затем производит закодирование и текста исходного сообщения, и подписанного хэша	
CryptVerifyMessage-Signature	Функция CryptVerifyMessage-Signature проверяет электронно-цифровую подпись подписанного сообщения.	
CryptVerifyDetached-MessageSignature	Функция CryptVerifyDetached-MessageSignature проверяет подписанное сообщение, содержащее отсоединенную (detached) подпись или подписи	
CryptDecodeMessage	Функция декодирует, расшифровывает и проверяет сообщение	
CryptDecryptAndVerifyMessage Signature	Функция декодирует и проверяет сообщение	
CryptEncryptMessage	Функция CryptEncryptMessage зашифровывает и производит закодирование сообщения. Аутентичность сообщения не обеспечивается.	
CryptDecryptMessage	Функция CryptDecryptMessage производит раскодирование и расшифрование сообщения. Проверка аутентичности сообщения не производится. *Примечание*: Не допускается автоматический анализ результата работы функции, направленный на проверку корректности сообщения.	

CryptGetMessageCertificates	Функция возвращает хранилище сертификатов и списки аннулированных сертификатов из сообщения	
CryptGetMessageSignerCount	Функция возвращает количество подписавших сообщение	
CryptHashMessage	Функция создает хэшированное сообщение	
CryptSignAndEncryptMessage	Функция создает подписанное и зашифрованное сообщение	
CryptSignMessageWithKey	Функция создает подписанное сообщение	
CryptVerifyDetachedMessageHash	Функция проверяет откреплённый хэш	
CryptVerifyMessageHash	Функция проверяет хэшированное сообщение	
CryptVerifyMessageSignatureWithKey	Функция проверяет подписанное сообщение	
CryptMsgCalculate-EncodedLength	Функция CryptMsgCalculate-EncodedLength вычисляет максимальное количество байтов, необходимое для закодированного криптографического сообщения, заданного типом сообщения, параметрами кодирования и общей длиной информации, которая должна быть закодирована.	
CryptMsgOpenToEncode	Функция CryptMsgOpenToEncode открывает криптографическое сообщение для закодирования и возвращает дескриптор открытого сообщения.	
CryptMsgOpenTo-Decode	Функция CryptMsgOpenTo-Decode открывает криптографическое сообщение для раскодирования и возвращает дескриптор открытого сообщения.	

CryptMsgUpdate	Функция CryptMsgUpdate пополняет текст криптографического сообщения.	
CryptMsgGetParam	Функция CryptMsgGetParam получает параметр сообщения после того, как криптографическое сообщение было раскодировано или закодировано.	
CryptMsgControl	Функция CryptMsgControl выполняет контрольное действие.	
CryptMsgClose	Функция CryptMsgClose закрывает дескриптор криптографичекого сообщения.	
CryptMsgDuplicate	Функция CryptMsgDuplicate дублирует дескриптор криптографического сообщения путем увеличения счетчика ссылок	
Функции работы с алгоритмами хэширования		
CryptCreateHash	Функция CryptCreateHash() инициализирует дескриптор нового объекта функции хэширования потока данных.	Разрешено использование только со следующими символьными аргументами: CALG_GR3411, CALG_GR3411_HMAC, CALG_SHAREDKEY_HASH.
CryptDestroyHash	Функция CryptDestroyHash() удаляет объект функции хэширования.	
CryptDuplicateHash	Функция CryptDuplicateHash() создаёт точную копию объекта функции хэширования, включая все его переменные, определяющие внутреннее состояние объекта функции хэширования.	
CryptGetHashParam	Функция CryptGetHashParam() возвращает параметры объекта функции хэширования и значение функции хэширования.	
CryptHashData	Функция CryptHashData() передаёт данные указанному объекту функции хэширования.	

CryptSetHashParam	Функция CryptSetHashParam() устанавливает параметры объекта хэширования.	Разрешено использование только с символьными аргументами HP_HASHSIZE, HP_OID/KP_HASHOID, HP_OPEN.
CryptSignHash	Функция CryptSignHash() возвращает значение электронной цифровой подписи от значения функции хэширования.	Разрешено использование только с ключевыми контейнерами, полученными ранее с помощью вызова CertGetCertificateContextProperty из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy
CryptVerifySignature	Функция CryptVerifySignature() осуществляет проверку цифровой подписи.	Разрешено использование только с дескрипторами ключей, полученных ранее с помощью вызова CryptImportPublicKeyInfo (CryptImportPublicKeyInfoEx) из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy
Функции работы с сертификатами, списками аннулированных сертификатов, хранилищем сертификатов		
Списки аннулированных сертификатов		
CertAddCRLContext-ToStore	Функция CertAddCRLContext-ToStore добавляет контекст СОС в хранилище сертификатов.	
CertAddCRLLinkToStore	Функция создает ссылку на список аннулированных сертификатов в другом хранилище	
CertAddEncodedCRL-ToStore	Функция CertAddEncoded-CRLToStore создает контекст СОС из закодированного СОС и добавляет его в хранилище сертификатов. Функция создает копию контекста СОС перед добавлением его в хранилище.	
CertEnumCRLsInStore	Функция CertEnumCRLsIn-Store получает первый или следующий СОС в хранилище. Эта функция используется в цикле для того, чтобы	

	последовательно получить все СОС в хранилище.	
CertFreeCRLContext	Функция CertFreeCRLContext освобождает контекст СОС, уменьшая счетчик ссылок на единицу. Когда счетчик ссылок обнуляется, функция CertFreeCRLContext освобождает память, выделенную под контекст СОС.	
CertCreateCRLContext	Функция CertCreateCRL-Context создает контекст СОС из закодированного СОС. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного СОС.	
CertDeleteCRLFromStore	Функция удаляет список аннулированных сертификатов из хранилища	
CertDuplicateCRL-Context	Функция CertDuplicateCRL-Context дублирует контекст СОС, увеличивая счетчик ссылок на СОС на единицу.	
CertFindCRLInStore	Функция CertFindCRLInStore находит первый или следующий контекст СОС в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara. Эта функция может быть использована в цикле для того, чтобы найти все СОС в хранилище сертификатов, удовлетворяющие заданному критерию поиска.	
CertDeleteCertificate-FromStore	Функция CertDeleteCertificate-FromStore удаляет определенный контекст СОС из хранилища сертификатов.	
CertFindCertificateInCRL	Функция осуществляет поиск заданного сертификата в списке аннулированных сертификатов	
CertGetCRLFromStore	Функция CertGetCRLFrom-Store получает первый или следующий	

	контекст СОС для определенного издателя сертификата из хранилища сертификатов. Эта функция также осуществляет возможную проверку СОС.	
CertSerializeCRLStoreElement	Функция сериализации списка аннулированных сертификатов со своими свойствами	
Расширенные свойства сертификата списка аннулированных сертификатов и CTL		
CertGetCRLContext-Property	Функция CertGetCRLContext-Property получает расширенные свойства определенного контекста СОС.	
CertSetCRLContext-Property	Функция CertSetCRLContext-Property устанавливает расширенные свойства определенного контекста СОС.	
CertGetCertificate-ContextProperty	Функция CertGetCertificate-ContextProperty получает информацию, содержащуюся в расширенных свойствах контекста сертификата.	
CertEnumCertificate-ContextProperties	Функция CertEnumCertificate-ContextProperties позволяет перечислить информацию, содержащуюся в расширенных свойствах контекста сертификата.	
CertSetCertificate-ContextProperty	Функция CertSetCertificate-ContextProperty устанавливает расширенные свойства для определенного контекста сертификата.	
CertEnumCRLContextProperties	Перечисление расширенных свойств списка аннулированных сертификатов	
CertEnumCTLContextProperties	Перечисление расширенных свойств CTL	
CertGetCTLContextProperty	Получение расширенного свойства CTL	
CertSetCTLContextProperty	Установка расширенных свойств CTL	
Функции работы с сертификатами		
CertAddCertificate-	Функция CertAddCertificate-	

ContextToStore	ContextToStore добавляет контекст сертификата в хранилище сертификатов.	
CertAddCertificateLinkToStore	Добавляет ссылку на сертификат в другом хранилище	
CertAddEncoded-CertificateToStore	Функция CertAddEncoded-CertificateToStore создает контекст сертификата из закодированного сертификата и добавляет его в хранилище сертификатов. Созданный контекст не содержит никаких расширенных свойств.	
CertEnumCertificates-InStore	Функция CertEnumCertificates-InStore получает первый или следующий сертификат в хранилище сертификатов. Эта функция используется в цикле для того, чтобы последовательно получить все сертификаты в хранилище сертификатов.	
CertFreeCertificate-Context	Функция CertFreeCertificate-Context освобождает контекст сертификата, уменьшая счетчик ссылок на единицу.	
CertCreateCertificate-Context	Функция CertCreate-CertificateContext создает контекст сертификата из закодированного сертификата. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного сертификата.	
CertDuplicate-CertificateContext	Функция CertDuplicate-CertificateContext дублирует контекст сертификата, увеличивая счетчик ссылок на единицу.	
CertFindCertificate-InStore	Функция CertFindCertificate-InStore находит первый или следующий контекст сертификата в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara.	

CertDeleteCertificate-FromStore	Функция CertDeleteCertificate-FromStore удаляет определенный контекст сертификата из хранилища сертификатов.	
CertGetSubject-CertificateFromStore	Функция CertGetSubject-CertificateFromStore получает контекст сертификата из хранилища сертификатов, однозначно определяемый его издателем и серийным номером	
CertGetIssuerCertificateFromStore	Поиск сертификатов издателей заданного сертификата	
CertGetSubjectCertificateFromStore	Поиск сертификата по серийному номеру и издателю	
CertGetValidUsages	Поиск пересечения KeyUsage для массива сертификатов	
CertSerializeCertificateStoreElemene	Сериализация элемента хранилища	
OCSP		
CertAddRefServerOcspResponse	Увеличение счетчика ссылок на OCSP ответ	
CertAddRefServerOcspResponseContext	Увеличение счетчика ссылок на контекст OCSP ответа	
CertCloseServerOcspResponse	Закрытие дескриптора OCSP ответа	
CertGetServerOcspResponseContext	Получение контекста OCSP ответа	
CertOpenServerOcspResponse	Открытие дескриптора OCSP ответа для заданной цепочки сертификатов	
Оконные функции		
CertSelectCertificate	Отображение диалога выбора сертификата по заданным критериям	
CryptUIDlgCertMgr	Отображение диалога управления сертификатами	
CryptUIDlgSelectCertificate	Отображение диалога выбора	

	сертификата	
CryptUIDlgSelectCertificateFrom Store	Отображение диалога выбора сертификата из хранилища	
CryptUIDlgViewCertificate	Отображение диалога со свойствами сертификата	
CryptUIDlgViewContext	Отображение сертификата, списка аннулированных сертификатов или CTL	
CryptUIDlgViewSignerInfo	Отображение диалога с информацией о подписавшем	
CertSelectionGetSerializedBlob	Сериализация сертификата из структуры, используемой для отображения	
GetFriendlyNameOfCert	Преобразование имени сертификата к «читаемому» виду	
Функции проверки цепочек		
CertVerifyCertificate-ChainPolicy	Функция CertVerifyCertificate-ChainPolicy проверяет цепочку сертификатов на достоверность, включая соответствие критерию истинности.	
CertGetCertificateChain	Функция CertGetCertificate-Chain строит цепочку сертификатов, начиная с последнего сертификата, в обратном направлении до доверенного корневого сертификата, если это возможно.	
CertFreeCertificate-Chain	Функция CertFreeCertificate-Chain освобождает цепочку сертификатов путем уменьшения счетчика ссылок. Если счетчик ссылок равен нулю, то память, выделенная под цепочку, освобождается.	
CertCreateCertificate-ChainEngine	Функция CertCreateCertificate-ChainEngine создает контекст HCERTCHAINENGINE, который позволяет изменять параметры механизма построения цепочки сертификатов. Позволяет ограничивать	

	множество доверенных сертификатов.	
CertFreeCertificate-ChainEngine	Функция CertFreeCertificate-ChainEngine освобождает контекст HCERTCHAINENGINE.	
CertCreateCTLEntryFromCertificateContextProperties	Создание CTL на основе свойст атрибутов контекста сертификата	
CertDuplicateCertificateChain	Дублирование контекста цепочки.	
CertFindChainInStore	Функция построения цепочки по заданным критериям из хранилища	
CertFreeCertificateChainList	Функция освобождения массива цепочек	
CertIsValidCRLForCertificate	Функция проверки наличия сертификата в списке аннулированных сертификатов	
CertSetCertificateContextPropertiesFromCTLEntry	Установка свойств в контекст сертификата на основе CTL	
Расширенные свойства сертификата (EKU)		
CertGetEnhancedKey-Usage	Функция CertGetEnhanced-KeyUsage получает информацию о расширенном использовании ключа из соответствующего расширения или из расширенных свойств сертификата. Расширенное использование ключа служит признаком правомерного использования сертификата.	
CryptAcquireCertificatePrivateKey	Функция CryptAcquire-CertificatePrivateKey получает дескриптор HCRYPTPROV и параметр dwKeySpec для определенного контекста сертификата.	
Функции работы с идентификаторами		
CryptFindOIDInfo	Функция CryptFindOIDInfo получает первую предопределенную или зарегистрированную структуру CRYPT_OID_INFO, согласованную с определенным типом ключа и с	

	ключом.	
CryptEnumOIDInfo	Перечисление зарегистрированных идентификаторов и получение информации для них	
Функции работы с хранилищем		
CertOpenStore	Функция CertOpenStore открывает хранилище сертификатов, используя заданный тип провайдера.	
CertDuplicateStore	Функция CertDuplicateStore дублирует дескриптор хранилища, увеличивая счетчик ссылок на хранилища на единицу.	
CertOpenSystemStore	Функция CertOpenSystemStore используется для открытия наиболее часто используемых хранилищ сертификатов.	
CertCloseStore	Функция CertCloseStore закрывает дескриптор хранилища сертификатов и уменьшает счетчик ссылок на хранилища на единицу.	
CertAddStoreToCollection	Добавление хранилища в коллекцию	
CertControlStore	Установка нотификации при различиях в закешированном хранилище и физическом хранилище	
Функции, используемые для работы с открытыми данными и объектами		
CryptImportPublicKey-InfoEx2	Функция CryptImportPublic-KeyInfoEx2 импортирует информацию об открытом ключе в CNG и возвращает дескриптор открытого ключа.	
CryptImportPublicKey-InfoEx	Функция CryptImportPublic-KeyInfoEx импортирует информацию об открытом ключе в CSP и возвращает дескриптор открытого ключа.	
CryptImportPublicKey-Info	Функция CryptImportPublic-KeyInfo преобразовывает и импортирует информацию об открытом ключе в провайдер и возвращает дескриптор	

	открытого ключа.	
CryptExportPublicKey-InfoEx	Функция CryptExportPublic-KeyInfoEx экспортирует информацию об открытом ключе, связанную с соответствующим секретным ключом провайдера.	
CryptExportPublicKey-Info	Функция CryptExportPublic-KeyInfo экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.	
CertCompareCertificate	Функция CertCompare-Certificate сравнивает два сертификата для того, чтобы определить, являются ли они идентичными.	
CertCompareInteger-Blob	Функция CertCompareInteger-Blob сравнивает два целочисленных блоба для определения того, представляют ли они собой два равных числа.	
CryptExportPublicKeyInfoFromBCryptKeyHandle	Экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.	
Функции кодирования/декодирования		
CryptDecodeObject	Функция CryptDecodeObject используются для декодирования сертификатов, списков аннулированных сертификатов (COC) и запросов на сертификаты.	
CryptDecodeObjectEx	Функция CryptDecodeObjectEx используются для декодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты	
CryptEncodeObject	Функция CryptEncodeObject используются для кодирования сертификатов, списков аннулированных сертификатов и	

	запросов на сертификаты.	
CryptEncodeObjectEx	Функция CryptEncodeObjectEx используются для кодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты.	
Получение объектов из удаленных источников		
CryptRetrieveObject-ByUrlA	Функция CryptRetrieveObject-ByUrlA получает объект инфраструктуры открытых ключей по заданному URL.	
CryptRetrieveObject-ByUrlW	Функция CryptRetrieveObject-ByUrlW является unicode версией функции CryptRetrieveObject-ByUrlA.	
Дополнительные функции		
CryptBinaryToString	Функция переводит двоичную строку в строку Base64/HEX.	
CryptStringToBinary	Функция переводит строку Base64/HEX в двоичную строку.	
CertFindAttribute	Функция производит поиск атрибута сертификата по идентификатору.	
CertGetNameString	Функция получает имя владельца или издателя сертификата.	
CertNameToStr	Функция производит раскодирование имени из ASN структуры в DN (RFC1779).	
CertSaveStore	Функция производит запись хранилища сертификатов (включая списки отозванных и доверенных сертификатов) в виде структуры PKCS#7 или бинарного дампа в память или файл.	
CryptFindCertificateKeyProvInfo	Функция осуществляет поиск закрытого ключа, соответствующего открытому ключу сертификата.	
CryptHashPublicKeyInfo	Функция осуществляет ASN1 кодирование и хэширование структуры	

	CERT_PUBLIC_KEY_INFO	
CryptMsgCountersign	Функция вырабатывает добавочную подпись.	
CryptMsgCountersignEncoded	Функция вырабатывает добавочную подпись. (кодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncoded	Функция проверяет добавочную подпись. (декодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncodedEx	Функция проверяет добавочную подпись. (декодирует структуру SignerInfo, как определено в PKCS #7).	