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 3.6.1

Руководство программиста

ЖТЯИ.00050-03 90 05

Листов 16

2013

Аннотация

Настоящий документ описывает состав функций и тестовое ПО СКЗИ ЖТЯИ.00050-03 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_6.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_6.chm в полном объеме относятся к дистрибутивам mini.

Файл CSP_3_6.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_6.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_6.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_6.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_6.chm

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.