Общее описание

Назначение продукта

PKI-Core применяется для встраивания электронной подписи, шифрования и двухфакторной аутентификации в приложения C++ с использованием аппаратной реализации российских криптографических алгоритмов в USB-устройствах Рутокен ЭЦП 2.0 и Рутокен PINPad.

Библиотека совместима с удостоверяющими центрами, в том числе российских производителей, и может применяться в информационных системах, в которых используются цифровые сертификаты и инфраструктура PKI.

Условия работы

Аппаратные требования

Intel-совместимые процессоры

- x86
- x86_64

Программные требования

Операционные системы, на которых проводилось тестирование:

- Windows 7
- Windows 8, 8.1
- Windows 10
- Windows XP

Состав

В состав PKI-Core входят:

1. Динамическая библиотека rtPKCS11ECP, реализующая стандарт PKCS#11 с поддержкой российского профиля.
2. Динамическая библиотека pki-core, реализующая высокоуровневые криптографические форматы (X.509, PKCS#10, CMS).
3. Статическая либа импорта
4. Заголовочный файл

Функциональность

Библиотека позволяет:

- Получать список всех подключенных к компьютеру USB-устройств Рутокен ЭЦП и Рутокен PINPad
- Получать информацию об устройстве
- Осуществлять логин на устройство
- Осуществлять логаут с устройства
- Получать список всех ключевых пар ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 на выбранном устройстве
- Аппаратно генерировать ключевую пару ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 на выбранном устройстве
- Получать метку ключевой пары
- Устанавливать метку для ключевой пары
- Формировать запрос на сертификат в формате PKCS#10 для выбранной ключевой пары (поддерживаются расширения, необходимые для получения квалифицированного сертификата)
- Импортировать на устройство сертификат формата X.509, переданный в виде base64-строки
- Удалять выбранный сертификат с устройства
- Получать информацию, содержащуюся в сертификате X.509 (DN, keyUsages, extendedKeysUsages и т.п.), с поддержкой расширений квалифицированного сертификата.
- Выдавать информацию о сертификате в виде текста для печати
- Получать список сертификатов, хранящихся на устройстве. Опционально можно задать поиск только тех сертификатов, которые связаны с закрытым ключом
- Осуществлять подпись строки в формате CMS. Опционально строка может быть перекодирована из base64 и подписан бинарный массив.
- Шифровать данные в формате CMS
- Производить вычисление хеш-функции от данных по алгоритму ГОСТ Р 34.11-94

Поддерживаемые устройства

В библиотеке поддерживаются устройства:

- Рутокен ЭЦП 2.0
- Рутокен PINPad

Поддерживаемые стандарты

- Используются криптографические алгоритмы, соответствующие российским стандартам ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94.
- Наборы параметров для этих алгоритмов соответствуют RFC 4357
- Выработка ключа согласования по схемам VKO GOST 34.10-2001 (RFC 4357) и VKO ГОСТ Р 34.10-2012 (RFC 7836)
- Поддерживаемые форматы защищенных сообщений соответствуют RFC 3851 и 3852, использование российских алгоритмов в этих форматах соответствует RFC 4490.
- Сертификаты и списки отзывов реализованы в соответствии с RFC 3280.
- Упаковка открытых ключей алгоритмов ГОСТ реализована в соответствии с RFC 4491.
- Работа с USB-токенами реализована в соответствии со стандартом PKCS#11 v. 2.20