Рекомендации по выбору высокоуровневого интерфейса

При создании собственного приложения, использующего возможности устройств Рутокен, перед разработчиком встает вопрос о выборе оптимального средства реализации криптографических функций. На сегодняшний день наиболее распространёнными высокоуровневыми интерфейсами, предоставляющими мощные возможности по использованию функционала устройств Рутокен прикладными приложениями, являются стандарты **RSALabs PKCS #11** и **Microsoft CryptoAPI**.

Важно помнить, что выбор API должен осуществляться разработчиком в каждом конкретном случае отдельно в зависимости от предъявляемых требований.

Стандарт PKCS #11

Стандарт **PKCS #11** является одним из семейства стандартов криптографии с открытым ключом (PKCS, Public-Key Cryptography Standard), разработанных RSA Laboratories для обеспечения совместимости различных реализаций криптографии с открытым ключом.

Стандарт PKCS #11, также известный под названием Cryptoki (Cryptographic Token Interface Standart), распространяется на «криптографические токены» – устройства, способные содержать криптографическую информацию и выполнять криптографические преобразования, и определяет для них интерфейс прикладного программирования (API). Таким образом, стандарт описывает общий набор команд для выполнения криптографических функций независимо от конкретной аппаратной реализации токена и программной среды.

В основе PKCS #11 лежит объектно-ориентированный подход, который позволяет стандарту все время расширяться, включая в себя вновь появляющиеся как аппаратные, так и программные решения. Кроме того, PKCS #11 предоставляет разработчикам возможность добавлять свои определения для тех алгоритмов, которые еще не вошли в стандарт.

Подробно с текстом стандарта можно ознакомиться на странице https://www.cryptsoft.com/pkcs11doc/.

Достоинства PKCS #11

- кроссплатформенность. PKCS #11 легко реализуется на любых платформах: Windows, Mac OS, Linux, UNIX, Java и т.п.
- простой интерфейс для языка C;
- высокая степень абстракции;
- высокая распространенность среди не-Windows платформ;
- легкая портируемость программного обеспечения на любые платформы;
- поддержка управления несколькими устройствами Рутокен одновременно;
- поддержка одновременного хранения на устройстве Рутокен ключей, сертификатов и объектов данных;
- наличие специальной функции ожидания подключения/отключения токена (C_WaitForSlotEvent).

Недостатки PKCS #11

- недостаточная поддержка стандарта операционными системами семейства Windows и, как следствие, прикладным программным обеспечением под Windows;
- отсутствие вспомогательных функций для работы с сертификатами, в результате чего разбор и изучение сертификата формата X.509 может оказаться достаточно сложной задачей. Однако при работе в MS Windows возможно использование функций Win32 API даже при использовании стандарта PKCS #11;
- отсутствие функции выбора и управления криптопровайдерами. Так как PKCS #11 представляет собой API, а не архитектуру, в случае, если приложению необходимо использовать несколько криптопровайдеров, то оно само должно определять, как с ними работать.

Microsoft CryptoAPI и Cryptography API: Next Generation

Microsoft CryptoAPI (MS CAPI) представляет собой интерфейс прикладного программирования, разработанный корпорацией Microsoft для обеспечения криптографическими функциями разработчиков Windows-приложений и входящий в состав операционных систем Windows. Криптографические алгоритмы реализуются криптопровайдером – независимым модулем, содержащим библиотеку криптографических функций со стандартизованным интерфейсом, а CryptoAPI лишь предоставляет унифицированный интерфейс работы с криптопровайдером. Подобная архитектура позволяет переходить от одного провайдера к другому с минимальными изменениями исходного кода, так как интерфейс (сами функции) не меняется. Подробная информация о CryptoAPI доступна по ссылкам http://technet.microsoft.com/en-us/library/cc962093.aspx и https://msdn.microsoft.com/en-us/library/windows/desktop/aa380255(v=vs.85).aspx.

Начиная с Windows Vista, Microsoft предлагает новый интерфейс **Cryptography API: Next Generation (CNG)**, предназначенный для замены устаревшего интерфейса CryptoAPI. Служба CNG предоставляет набор интерфейсов API для выполнения основных криптографических операций и благодаря своей модульной архитектуре позволяет создавать, обновлять и использовать собственные алгоритмы шифрования в таких приложениях и технологиях, как служба сертификации Active Directory, технологии SSL и IPsec. CNG поддерживает все алгоритмы, предоставляемые CryptoAPI, а также новые алгоритмы, включая алгоритмы шифрования, цифровых подписей, обмена ключами и хеширования, в том числе и алгоритмы на основе эллиптических кривых (ECC). Интерфейс CNG является гораздо более гибким, тем самым обеспечивая разработчикам больший контроль над способом выполнения криптографических операций и совместной работой алгоритмов при выполнении различных операций. Подробная информация о CNG доступна по ссылке https://msdn.microsoft.com/en-us/library/windows/desktop/aa376210(v=vs.85).aspx

Достоинства CryptoAPI

- глубокая интеграция в Windows и прикладное программное обеспечение под Windows;
- простой интерфейс;
- более высокий уровень абстракции по сравнению с PKCS #11;
- легкая портируемость программного обеспечения в пределах ОС Windows;
- автоматический доступ к любому установленному криптопровайдеру.

Недостатки CryptoAPI

- невозможность использования в ОС, отличных от Windows;
- отсутствие возможности управления несколькими устройствами Рутокен одновременно. Так как в CryptoAPI нет понятия физического устройства, то для одновременного использования нескольких устройств Рутокен на одном и том же компьютере потребуется использование особой техники;
- отсутствие специальной функции ожидания подключения/отключения токена (реализация возможна через Win32 API);
- невозможность хранения объектов данных вместе с RSA ключами и сертификатами на устройстве Рутокен;
- установка криптопровайдера требует наличия прав администратора в ОС.