Microsoft CryptoAPI

CryptoAPI – высокоуровневый интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером (CSP, Cryptographic Service Providers):

- шифрование и дешифрование данных,
- аутентификацию с использованием цифровых сертификатов,
- кодирование и декодирование из формата ASN.1 в приложения на базе Windows.

CryptoAPI поддерживает различные криптопровайдеры, которые самостоятельно реализуют криптографические функции. Так как CryptoAPI используется как обычная библиотека, то от разработчика не требуется детального понимания реализации ни криптопровайдера, ни самой библиотеки.

CAPICOM представляет собой 32-битную библиотеку, которая предоставляет COM-интерфейс и предназначена для использования в ОС Windows Server 2008, Windows Vista, and Windows XP.

Примеры

Примеры использования CryptoAPI доступны на MSDN в разделе Using Cryptography:

1. Создание контейнера и генерация ключей (код)
2. Подпись сообщения (описание процедуры подписи, проверки подписи, пример подписи и проверки подписи сообщения)
3. Кодирование сообщения в PKCS#7 формат (описание процедуры кодирования, декодирования, пример)
4. Шифрование и расшифрование сообщения (описание, пример шифрования, расшифрования)
5. Работа с сертификатами (примеры)
6. Перечисление поддерживаемых криптопровайдером протоколов (пример)
7. Работа с библиотекой CAPICOM.dll (раздел).

Дополнительные источники:

1. Статья на RSDN
2. Руководство разработчика Крипто-Про