Enkrypcja i dekrypcja w WinAPI

Piotr Kruszewski

Klucz publiczny i prywatny

- Klucz publiczny służy do szyfrowania wiadomości, która może być odszyfrowana tylko przy użyciu klucza prywatnego
- Nie możliwe jest wygenerowanie klucza prywatnego za pomocą klucza publicznego i na odwrót
- Klucz publiczny i prywatny tworzą unikalną parę
- Sposób ten należy do algorytmu szyfrowania asymetrycznego

Cryptographic Service Provider (CSP)

- Biblioteka implementująca Microsoft CryptoAPI zawierające funkcje szyfrujące i deszyfrujące
- Jest modułem który może być używany przez wiele aplikacji

CryptoAPI

Jest to interfejs programistyczny załączony w systemie operacyjnym Windows, dostarcza on użytkownikom funkcji umożliwiających zabezpieczenie aplikacji stworzonej na ten system. Jest on zbiorem bibliotek DLL, pierwszy raz pojawiło się w Windows NT 4.0.

Pozwala nam używać szyfrowania symetrycznego i asymetrycznego, używać autentykacji poprzez certyfikaty cyfrowe, zawiera również kryptograficzny pseudo-losowy generator liczb.

CryptAcquireContext

- Funkcja potrzebna do uzyskania uchwytu do specjalnego kontenera kluczy (baza danych zawierająca wszystkie pary kluczy) z określonego CSP. Zwrócony uchwyt jest wykorzystywany w wywołaniach funkcji CryptoAPI używających wybranego CSP.
- (wskaźnik do uchwytu CSP, nazwa kontenera, nazwa CSP, typ CSP, flagi)

CryptGenKey

- Funkcja generuje losowy kryptograficzny klucz sesji lub parę kluczy (publiczny/prywatny), funkcja zwraca uchwyt do klucza w ostatnim parametrze, który jest następnie użyty w funkcjach CAPI wymagających klucza
- (uchwyt CSP, algorytm do wygenerowania klucza, flagi, uchwyt klucza)

CryptGetUserKey

- Funkcja uzyskuje uchwyt do jednego z dwóch kluczy użytkownika (prywatnego lub publicznego). Używana jest jedynie przez właściciela pary kluczy i tylko gdy CSP i odpowiedni kontener są dostępne
- (uchwyt CSP, AT_KEYEXCHANGE, wskaźnik do zwróconych kluczy)

CryptExportKey

- Funkcja eksportuje klucz lub ich parę z CSP w postaci BLOB’a

CryptCreateHash

- Funkcja inicjuje hashowanie ciągu znaków

Link do kodu

https://github.com/TheNishishiro/EncryptionDecryption