Zadání softwarového projektu - PKI Čipové karty

Projektový tým:
Jakub Balada
Ondřej Babuljak
Hedvika Peroutková
Matěj Cáha
Vedoucí:
RNDr. Libor Dostálek
Předpokládaný termín dokončení:
Květen 2007

Specifikace

Cílem projektu bude vytvoření víceúrovňového obslužného software pro PKI čipovou kartu Siemens. PKI čipové karty jsou karty s vlastním čipem, pamětí a operačním systémem využívané například jako bezpečný prostředek pro vytváření elektronického podpisu.

Projekt se bude skládat ze tří částí:

- Knihovna PKCS11
- Knihovna CSP (= kryptografické rozhraní Crypto Service Provider pro prostředí MS Windows)
- Obslužná aplikace pro základní práci s kartou

Komunikaci s kartou zajišťuje knihovna s pevně definovaným rozhraním, které obsahuje funkce na vytváření objektů na kartě, na provádění kryptografických operací, na autentizaci uživatelů, apod.

Implementace projektu bude rozdělena do vrstev, kdy nejspodnější vrstvou bude knihovna PKCS11. Knihovna CSP bude implementována primárně voláním funkcí PKCS11, pouze funkčnost, kterou PKCS11 neposkytuje, bude implementována voláním funkcí komunikační knihovny ke kartě. Obslužná aplikace bude primárně využívat rozhraní CSP, pouze funkce, které CSP neposkytuje, budou vyvinuty voláním funkcí komunikační knihovny ke kartě.

Funkční požadavky

CSP a PKCS11

Na PKCS11 a CSP jsou požadavky přesně specifikované normami a standardy (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf a http://msdn.microsoft.com/library/default.asp?url=/library/en-us/seccrypto/security/entry_points.asp).

Podporované kryptoalgroritmy budou odpovídat kryptoalgortimům, které podporuje čipová karta:

- RSA s maximální délkou klíče 2048 bitů
- DES

- 3DES
- RC2
- RC4
- MD2
- MD5
- SHA-1
- SHA-2

Jiné algoritmy nebudou implementovány (čili veškeré krypto operace budou prováděny na čipové kartě a knihovny/aplikace vyvíjené v rámci projektu budou pouze volat funkce operačního systému pro jejich provedení).

Obslužná aplikace

Obslužná aplikace bude umožňovat základní práci s kartou. Na aplikaci jsou kladeny následující technické a funkční požadavky:

- technické požadavky
    - aplikace bude připravena pro běh pod OS Windows
    - aplikace bude lokalizovatelná
    - aplikace bude připravena v podobě instalačního balíčku, součástí instalace bude registrace CSP do Windows
- funkční požadavky – aplikace bude umožňovat
    - Generování žádostí o certifikát včetně příslušného páru klíčů. Během generování žádosti bude možné vytvořit zálohu klíčů.
    - Import/Export certifikátů
    - Správu PIN a PUK karty (nastavování, odblokování)
    - Využívání paměti karty jako úložného prostoru pro libovolná data. Data mohou být volitelně chráněna PINem.
    - Zobrazení obecných informací o kartě (stav využití prostoru apod.)

Dokumentace

Součástí řešení bude provozní a vývojová dokumentace.