Posudek na diplomovou práci Ondřeje Těthala
Realizace modulu CSP pro tokeny s rozhraním PKCS#15

Úkolem diplomanta bylo zmapovat a zanalyzovat způsob používání čipových karet zejména z pohledu jejich nasazení pro PKI realizovaného na platformě Windows. Provést analýzu důvodů, proč není současný software pro manipulaci s kartami univerzální, tj. proč s každým typem karty spolupracuje pouze software dodávaný buď jeho výrobcem, nebo společností, která realizovala speciální (a vždy velice drahou) sadu kartových aplikací. Dále měl za úkol navrhnout způsob realizace univerzálního modulu CSP (modul nezbytný pro spolupráci systému Windows s čipovými kartami, které jsou schopné provádět některé kryptografické funkce), který by uměl spolupracovat alespoň s těmi typy karet, které splňují požadavky normy PKCS#15.

Podle mého názoru se diplomant zhostil všech těchto úkolů výtečně, provedl důkladnou analýzu způsobu, jakým software, zejména bezpečnostní moduly operačního systému, komunikují s aplikacemi uloženými na kartě, jakým způsobem jsou a mohou být potřebné údaje ukládány na kartě a jak tuto komunikaci i způsob ukládání dat upravují příslušné technické normy.

Výsledek jeho analýzy byl bohužel neradostný. Některé normy specifikují podstatné detaily jen hodně volně nebo umožňují více variant, nechávají tak volný prostor výrobcům a v mnoha případech dokonce nespecifikují nezbytné parametry vůbec. Jednotliví výrobci pak tyto normy dodržují pouze tam, kde se jim to hodí, takže výsledkem je to, že i karty s označením kompatibility s normou PKCS#15 nejsou z velké části navzájem kompatibilní.

I přesto se diplomant pokusil navrhnou „univerzální" modul CSP a to se mu povedlo, alespoň pro třídu karet splňujících několik v práci uvedených požadavků na kompatibilitu s normou. Hlavní přínos práce však spočívá ve výše zmiňované analýze, ze které jasně vyplývají důvody, proč rozšíření Smartkaret v PKI nedosáhlo takového stupně, jaký se ještě před několika lety předpokládal.

Poznámky a otázky:

str. 3 dole: Je skutečně „session" klíč jiný pro každou zprávu?

obr 2 na str. 8: možná by bylo dobré znázornit, že i samotná karta je uložištěm certifikátů (není ekvivalentní s uložišti, která si vytváří systém) a uložištěm klíčů (je ekvivalentní s uložišti, která si vytváří systém).

str. 11 – podle čeho si aplikace vybírá CSP a kontejner, které použije pro vytvoření kontextu?

Doporučuji, aby práce byla uznána jako diplomová a přijata k obhajobě.

V Praze, 15.5.2006

RNDr. Vojtěch Jákl