Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Šimkovič Petr, Bc.** **Oponent:** **Finstrle Luděk, Mgr.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2011/2012**

Téma diplomové práce: **Modul pro asymetrickou kryptografii**

Hodnocení práce:
Student svou prací prokázal, že se plně orientuje v problému. Následně praktickou částí dokázal, že tento problém umí řešit za použití moderních technologií užívaných nejen v bankovním sektoru, který klade nejvyšší nároky na bezpečnost. Řešení je navíc napsáno velmi pěkně a lze jej následně využít beze změn ve větších aplikacích.

Jako drobný nedostatek bych v teoretické části hodnotil, že student předpokládá čtenářovu základní znalost problematiky. Občas by bylo vhodnější některé pojmy nadefinovat (např. asymetrická kryptografie) či zdůraznit bezpečnostní rizika (např. privátní klíč generovaný certifikační autoritou).

Formální úprava diplomové práce je na vysoké úrovni. Práce je napsána stylisticky pěkně a celkový dojem je velmi dobrý, přestože technická zpráva obsahuje několik prohřešků proti pravopisu českého jazyka. Po stránce odbornosti jsem nenašel žádnou chybu a hodnotím práci jako velice zdařilou.

Otázky na diplomanta:
1. Vysvětlete pojem asymetrická kryptografie a její základní rozdíl od symetrické kryptografie.
2. V teoretické části jste uvedl, že privátní i veřejný klíč generuje certifikační autorita. Proč tento postup není vhodný a který postup je brán jako nejbezpečnější?
3. Jak si představujete správu uživatelské části PKI, že ji v demonstračním programu načítáte pouze při inicializaci aplikace.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:
Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 22. 5. 2012 Podpis oponenta diplomové práce