Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek oponenta diplomové práce

Autor diplomové práce: **Jan Pilař, Bc.**

Název diplomové práce: **Digitální podpis a digitální certifikáty**

1. **Zadání odborného problému a použití metod řešení v rámci diplomové práce**

   Zadaný odborný problém spočívá v analýze technologie digitálního podpisu a certifikátů, studia příslušné legislativy a vyhodnocení možných budoucích dopadů na implementaci zmíněných technologií v ČR a EU. V praktické části byly představeny praktické ukázky konfigurace dané technologie v prostředí Microsoft Windows.

2. **Konkrétní výsledky diplomové práce**

   Autor nastudoval a představil v práci příslušnou legislativu a budoucí dopady na implementaci technologie digitálních certifikátů a podpisu. Čtenáři byla představena a vysvětlena i samotná technologie digitálních podpisů a certifikátů včetně základního matematického aparátu. V praktické části je čtenáři představeno a přiblíženo nasazení této technologie v operačním systému Microsoft Windows.

3. **Prokázání správnosti navrženého řešení problému**

   Student vysvětlil stávající i budoucí legislativu, představil teoreticky technologii digitálního podpisu a certifikátů. Student implementoval digitální podpis a certifikáty v testovacím prostředí.

4. **Splnění cílů diplomové práce**

   Vytyčené cíle diplomové práce byly splněny.

5. **Kvalita textu diplomové práce**

   Kvalitu textu DP si dovolím označit jak mírně podprůměrnou. Anglický text anotace lze označit jako volný, místy neformální. Student používá formulace, které do textu diplomové práce nepatří - například kritika České justice z důvodu zdlouhavého řešení standardních kauz. Dále student minimálně na dvou místech práce vyslovuje vlastní a ničím nepodložené domněnky. Některá tvrzení by mohla být hlouběji vysvětlena (například na straně 36 student uvádí, že šifry mající klíč delší než 80bit lze považovat za silné).

6. **Připomínky a dotazy k diplomové práci**

   Student se v diplomové práci dopustil několika nepřesností. Například na straně 49 v bodě 6 uvádí, že délka klíče má vliv na životnost certifikátu. Problém stojí jinak. Délka klíče by měla být přímo úměrná životnosti certifikátu, ale navzájem se neovlivňují.

   U obhajoby doporučuji představit bezpečnostní problém týkající se software OpenSSL, který také využívá certifikáty.

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **velmi dobře minus**

Posudek vypracoval:

Jméno, tituly: Zitta Stanislav, Ing.,
Zaměstnavatel: Univerzita Pardubice, FEI

V Pardubicích dne: 1. 6. 2014 Podpis: