Posudek práce

předložené na Pedagogické fakultě JU

❑ posudek vedoucího ☑ posudek oponenta
❑ bakalářské práce ☑ diplomové práce

Autor/ka:	**Bc. Stanislav Čeleda**
Název práce:	**Certifikáty a certifikační autority**
Studijní program a obor:	F-VTE-n, k
Rok odevzdání:	2012

Jméno a tituly vedoucího/oponenta:	RNDr. Libor Dostálek
Pracoviště:	Ústav aplikované informatiky
Kontaktní e-mail:	dostalek@prf.jcu.cz

Odborná úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Věcné chyby:
❑ téměř žádné ☑ vzhledem k rozsahu přiměřený počet ❑ méně podstatné četné ❑ závažné

Výsledky:
❑ originální ❑ původní i převzaté ❑ netriviální kompilace ❑ citované z literatury ❑ opsané

Rozsah práce:
❑ veliký ☑ standardní ❑ dostatečný ❑ nedostatečný

Grafická, jazyková a formální úroveň:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Tiskové chyby:
❑ téměř žádné ☑vzhledem k rozsahu a tématu přiměřený počet ❑ četné

Celková úroveň práce:
❑ vynikající ☑ velmi dobrá ❑ průměrná ❑ podprůměrná ❑ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Práce je kompaktní, obsahuje několik sporných formulací:

- 4.1: „K převodu do binární podoby se používá kódování DER nebo BER a následovně ještě Base64. Soubor s digitálním certifikátem je po otevření zobrazen v čitelné podobě, což umožňuje zkontrolovat údaje o jeho předpokládaném majiteli.“ - Certifikát je zásadně jen v DER a otevření souboru kódovaného v DER běžným editorem není opravdu moc čitelné.
- 4.1.1: „Pro tuto normu se používají přípony: .der, .pem ....“ – nikoliv pro normu, ale pro formáty certifikátů.
- 4.1.4: „Pokud má držitel certifikátu vydáno více certifikátu u stejné certifikační autority, je nutné z důvoduzachování podmínky jedinečnosti, rozlišit objekty atributem serialNumber nebodnQualifier.“ – to není úplně pravda, tyto atributy se používají pro odlišení dvou osob, které jinak by měly stejný předmět.

4.4.2: protokoly SSL a TLS nejsou vzájemně kompatibilní 4.4.2: „klient pošle serveru výzvu k navázání spojení pomocí protokolu SSL a zvolí vhodný šifrovací algoritmus, který budou používat“ – právě položka version slouží ke mkompatabilitě

Případné otázky při obhajobě a náměty do diskuze:

Dotaz do diskuse: Jak byla konkrétně zjišťována „důvěryhodnost “ jednotlivých certifikačních autorit?

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:
☑ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:
V Českých Budějovicích 18. 1. 2012