

Slovenská technická univerzita

Fakulta informatiky a informačných technológií

Ilkovičova 3, 812 19 Bratislava

Infraštruktúra PKI a vybavenie pre koncových používateľov

Posudok

Autori projektu:

Tím č.2 PSS: *Choice*

Bc. Vladimír Balaš
Bc. Martin Kerni
Bc. Štefan Novák
Bc. Peter Procházka
Bc. Pavol Skočík
Bc. Ján Olbert

Autori posudku:

Tím č. 4 PSS: *Šikovni*

Bc. Jozef Hamar
Bc. Radomír Škrib
Bc. Peter Mulinka
Bc. Tomáš Smolek

Odbor: PSS

Predmet: Tímový projekt

Šk. rok: 2004/2005

1. Úvod

Obsahom tohto dokumentu je posúdenie výsledného produktu tímu *Choice* demonštrujúceho činnosť PKI vytvoreného v rámci tímového projektu. Tím *Choice*, podobne ako náš tím „Šikovní“, pracoval na projekte *Infraštruktúra PKI a vybavenie pre koncového používateľa*. Posudzovali sme výslednú dokumentáciu, aktuálnu stránku z 3.6.2005, na ktorej sa nachádza samotná web prezentácia, web stránku s certifikačnou autoritou a program na podpísanie súborov a overenie podpísaných súborov.

2. Výsledná dokumentácia

Pri posudzovaní výslednej dokumentácie sme sa zamerali len kapitoly 8 a vyššie, keďže ostatné kapitoly už boli predmetom predchádzajúceho posudku.

2.1. Formálna stránka

Dokumentácia je po formálnej stránke na veľmi dobrej úrovni. Nemáme voči nej žiadne výhrady.

2.2. Obsahová stránka

V kapitole 8 chýba kapitola o testovaní implementovaného produktu, či už sa to týka webovej prezentácie, či softvéru používaného na podpisovanie a overovanie podpisov. Ďalšou kapitolou, ktorá v danom dokumente chýba je kapitola o implementácii. Dôvodom je pravdepodobne, že samotná implementácia je vlastne popísaná v kapitolách A a B, ale zišlo by sa napísať aspoň pár riadkov o implementácii softvéru použitého na podpisovanie dokumentov a overovanie dokumentov.

Musíme pochváliť príručku ku konfigurácii OpenCa ako aj používateľskú príručku ku web prezentácii a pre softvér na overovanie a podpisovanie. Tieto časti sú veľmi dobre a prehľadne spracované. Postup inštalácie je popísaný takým spôsobom, že aj človek menej znalý danej problematiky bude schopný pomocou neho daný produkt nainštalovať. Návod na použitie je podrobne popísaný a jednotlivé kroky sú doprevádzané názornými obrázkami.

Celkovo je dokument po obsahovej stránke veľmi dobre spracovaný, obsahuje až na vyššie uvedené časti všetky potrebné informácie.

3. Projekt

3.1. Web prezentácia

Táto časť prešla od posledného posudzovania výraznými zmenami k lepšiemu. Ako veľmi pozitívne hodnotíme rozdelenie prezentácie na dve časti. V predchádzajúcom posudku bola vyčítaná absencia obrázkov, ale v novej verzii je už prezentácia doplnená o názorné obrázky, čo výrazne zvýšilo čitateľnosť textu.

V základnom kurze je dosť nešťastne volená časť *Príklad PKI*, kde je obrázok so zobrazenou hierarchiou CA a klientov. Ďalšia pripomienka smeruje na tento obrázok, kde chýba umiestnenie samotnej registračnej authority, ktorá by v konečnom dôsledku mala komunikovať s klientom a následne s CA. Takisto koreňová autorita by nemala priamo s klientom komunikovať aj keď to samozrejme nie je zakázané. Bolo by vhodnejšie vložiť obrázok s príkladu PKI do časti certifikačná autorita. Podobnú pripomienku máme k obrázkom umiestneným v podrobnom kurze v časti Infraštruktúra PKI, kde tiež chýba samotná RA.

Prezentácia ako celok je veľmi dobre spracovaná.

3.2. OpenCA

K tejto časti nemáme žiadne podstatné pripomienky, keďže produkt vznikol úpravou už existujúceho softvéru. V preklade sa občas vyskytol text bez diakritiky. Po funkčnej stránke pracuje všetko ako má.

3.3. Softvér na overovanie a podpisovanie

Používanie softvéru je veľmi intuitívne. Uvítali by sme možnosť uloženia elektronického podpisu a reťazca certifikátov do súboru, ale na prezentovanie princípu elektronického podpisovania je to viac ako postačujúce. Program dokázal pracovať aj s nami dodaným certifikátom s tým, že ho správne nedokázal overiť.

4. Zhodnotenie

Celkový dojem s produktu je veľmi dobrý. K žiadnej časti nemáme žiadne podstatné výhrady. Produkt plní všetky požadované úlohy. S vytvoreným softvérom dokáže pracovať aj laik, a práve pre tých bol aj určený. Web prezentácia poskytuje v čitateľnej forme dostatočné informácie o problematike PKI.