Slovenská technická univerzita
Fakulta informatiky a informačných technológii
Ilkovičova 3, 812 19 Bratislava

Infraštruktúra PKI a vybavenie pre koncových používateľov

Posudok dokumentácie

Autori dokumentácie:

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: *Sikovni*
Bc. Jozef Hamar
Bc. Radomír Škrib
Bc. Martin Mačica
Bc. Peter Mulinka
Bc. Tomáš Smolek

Odbor: PSS
Predmet: Tímový projekt
Šk. rok: 2004/2005

1. Úvod

Obsahom tohto dokumentu je posúdenie dokumentácie prvej etapy práce na tímovom projekte[1] tímu *Choice* v zimnom semestri. Tím *Choice*, podobne ako náš tím, pracuje na projekte *Infraštruktúra PKI a vybavenie pre koncového používateľa*. Posudzovaná dokumentácia je rozdelená do siedmich kapitol. Autori postupne prechádzajú od všeobecnejšieho opisu ku konkrétnej špecifikácii. Viditeľná je snaha spraviť dokument čitateľný aj pre laika, čo chápeme ako dôsledok prípravy na implementáciu prvej časti projektu, web aplikácie demonštrujúcej princípy činnosti PKI. Autori sa taktiež hrubo zaoberajú návrhom tejto aplikácie.

Dokumentácia je posúdená z pohľadu formálneho i pohľadu obsahového. V posudku nerozoberáme do podrobna všetky detaily, ale snažíme sa zhodnotiť celkový dojem z dokumentácie.

[1] Tímový projekt je absolvovaný v rámci inžinierskeho štúdia na FIIT STU

2. Formálna stránka

Dokumentácia je na prvý pohľad rozsiahla. Po prelistovaní pôsobí dobrým dojmom, bez rušivých estetických vplyvov. Členenie dokumentu je prehľadné. Nachádza sa v ňom množstvo obrázkov a schém, čo priaznivo vplýva na celkovú čitateľnosť.

V dokumentácii je vidieť snahu o jasnosť a jednoznačnosť. Každá zavedená notácia je prehľadne a stručne vysvetlená.

Pri čítaní niektorých častí dokumentu sme mali pocit, že nie všetky vety sú správne sformulované. V niektorých prípadoch by zmena slovosledu pomohla jasnejšie vyjadriť myšlienku, ktorú autori chceli prezentovať.

Pre lepšiu ilustráciu uvedieme zoznam položiek, ktoré by sme pravdepodobne riešili iným spôsobom:

- V nadpise témy - „Infraštruktúra PKI vybavenie pre koncového používateľa“ – chýba „a“ ako spojka slov PKI a vybavenie.
- Podkapitoly 3.2.2.x a 3.2.3.x majú v obsahu zlé odsadenie názvu kapitoly, chýba medzera.
- Hlavička je na každej strane „Tímový projekt“ - skôr by sme očakávali meno kapitoly
- Pri čítaní nachádzame množstvo gramatických chýb.
- Nachádzame pojmy, ktoré by si mohli pre menej informovaného čitateľa vyžadovať klarifikáciu, napr. Str.3: pojem „NBÚ“, Str. 8 „Kryptografická karta“, Kap. 3. - pojmy „PIN,ZEP, token, ACA“ atď.
- Niektoré obrázky (Obr. 1, Obr. 3, ...) obsahujú anglické názvy vnútri, avšak tieto nie sú vysvetlené. Taktiež rozlíšenie niektorých obrázkov nie je vhodné na prezentáciu na papieri. Oceňujeme však použitú farebnú tlač.
- Str. 15 spomenuté slovo „užívateľ“ - volil by som radšej „používateľ“ resp. v celom dokumente použil jednotné označenie.
- Kap. 4. EP - Legislatíva – túto kapitolu by sme odporúčali dať ako prílohu.
- Text je príliš rozsiahly pre potreby tohoto predmetu.
- V dokumente, ktorý sme obdržali chýba Príloha A. WSDL špecifikácia SAML rozhrania, v obsahu deklarovaná na Str. 100.

3. Obsahová stránka:

Dokument sa zaoberá danou tématikou na rôznych úrovniach, avšak máme pocit, že podsatata dokumentu je zhrnutá veľmi stručne v kapitole 2.8 a ostatné kapitoly akosi vysvetľujú kontext. Podľa nás mala byť táto kapitola niekde po úvode a všetko by malo smerovať k nej.

Páčilo sa nám vloženie kapotoly 3. opisujúcej praktické nasadenie opisovaných technológií.

Ostatné podnety na zlepšenie uvádzame v bodoch:

- Používanie slova „číslo“ v zmysle hash nie je najšťastnejšie, lebo v odbornej verejnosti je už slovo hash dosť zaužívané.
- obr.2: môže vyvolať dojem, že na výpočet „čísla“ pri vytváraní EP je potrebný tajný kľúč. Taktiež nie je úplne jednoznačné, že „Dokument“ je totožný z prvkom z dvojice (Dokument, „XXX“) .
- Často nachádzame úseky textu takmer zhodné s niektorou uvedenou referenciou bez uvedenie odkazu zdroja, napr. odsek č.2 „Elektronický ... preukaze“. Dostálek strana 11, odsek č.2 „Elektronický ... zločinců“, taktiež Kap 2.6 prvé 2 odstavce. Dostálek 1.10.
- V kap 2.1. na strane 3 je popis zložiek certifikátu, ale nadpis kapitoly je „**Základné** pojmy z oblasti PKI“, podľa nás toto nie sú základné pojmy.
- Str.6-7 Používanie slova „číslo“ v zmysle hash nie je najšťastnejšie, lebo v odbornej verejnosti je už slovo hash dosť zaužívané.
- Str. 4. Je spomenuté, že na zriadenie CA je potrebné 100-150 mil. Sk – ocenili by sme uviesť, odkiaľ je údaj čerpaný.
- Kap. 2.15 -Certifikáty - Je nerozumné, že táto kapitola je až tu. Keď veľa kapitol pred tým sa o nich hovorí.
- Nejasné a často nezrozumiteľné formulácie :
    - Kap. 2.16 „Certifikát je sekvenciou vlastných sát certifikátu...“
    - Str. 28 „Relatívne jedinečné meno“ - Čo to je?
    - Str. 29. „Bližší popis nájdete zaoberajúcou sa jedinečnými menami.“
    - Kap. 2.19.1 „Štruktúru, ktorú vytvárajú CA sa nazýva hierarchia.“

- Kap 2.22 Manažment kľúčov resp. 2.22.1 Získavanie kľúčov obsahuje informácie, ktoré by sme si predpokladali skôr v úvode do problematiky PKI.
- Všeobecne by sme sa rasdšej stretli s opisom funkčnosti kódu ako so samotným kódom.
- Kap. 7. Miesto jedného diagramu s konkrétnym prípadom použítia by sme viac ocenili activity diagram popisujúci celkové správanie.

4. Zhodnotenie

Z dokumentácie máme pocit, že bola písaná horúcou ihlou a jednotliví členovia tímu písali rôzne kapitoly bez znalosti toho, čo píšu iní členovia tímu. Časté používanie textov bez uvedenia citácie taktiež znižuje kvalitu dokumentu. Taktiež si vieme predstaviť, že by celý dokument mohol byť podstatne kratší.

Kapitoly o návrhu web-aplikácie by som úplne vylúčil, pretože spomínaný hrubý návrh je príliš hrubý.

Z uvedeného dokumentu však je možné získať dobrú predstavu o fungovaní procesov súvisiacich s PKI, preto konštujem, že dokument splnil svoj cieľ.

Slovne by sme ohodnotili prácu ako chválitebná.