Slovenská technická univerzita
v Bratislave
Fakulta informatiky a
informačných technológií

Infraštruktúra PKI vybavenie pre koncového používateľa

Tímový projekt

Posudok dokumentu „Analýza, špecifikácia a hrubý návrh“

Posudok vypracovali:
Členovia tímu č.2 PSS
Bc. Vladimir Balaš
Bc. Martin Kerni
Bc. Štefan Novák
Bc. Peter Procházka
Bc. Ján Olbert
Bc. Pavol Skočík

Autori posudzovanej práce:
Členovia tímu č. 4 PSS
Bc. Jozef Hamar
Bc. Martin Mačica
Bc. Peter Mulinka
Bc. Tomáš Smolek
Bc. Radovan Škríb

Rok: 2004/2005

1 Úvod

Tento dokument je posudkom tímu č.2 PSS „Choice“ na dokument „Infraštruktúra PKI a vybavenie pre koncových používateľov“ vypracovaný tímom č.4 PSS „Šikovní“. Posudzovaný dokument by mal obsahovať v tejto fáze predmetu Tímový projekt nasledovné časti: analýza problematiky, špecifikácia a hrubý návrh riešenia. Posudzovaný dokument je východzím prvkom pre ďalšiu činnosť a smer projektu. Posudok sme sa snažili hodnotiť a posudzovať práve v tomto kontexte.

Úvodom musíme konštatovať, že posudzovaný dokument má niekoľko hrubých nedostakov. Za najvážnejšie považujeme absenciu kapitol pojednávajúcich o špecifikácii a hrubom návrhu. Rovnako negatívne hodnotíme relatívne laxný prístup k samotnej analýze problematiky.

Žiaľ, výsledný posudok je pomerne negatívny a preto aj dúfame, že nebude takto prijatý, ale bude použitý ako základ na zlepšenie. Viackrát sú v posudku uvedené opravené (doplňujúce) informácie k danému problému. V prípade, že došlo k nepochopeniu z našej strany a nejaký problém je neoprávnene vytknutý, sa ospravedlňujeme.

Pre upresnenie uvádzame, že ako východzí bod pre hodnotenie považujeme elektronickú verziu dokumentácie, doručenú pomocou emailu po dohode medzi vedúcimi tímov. K tomu to kroku došlo v dôsledku technických prekážok pri vzniku papierovej verzie dokumentu zo strany hodnoteného tímu. Preto dokument nepokrýva zmeny, ktoré by mohli byť opravené v papierovej verzii oproti elektronickej verzii dokumentu.

Poznámka k typografii v dokumente: Texty uvedené kurzívou v úvodzovkách sú citáty z posudzovaného dokumentu alebo iných prác autorov v zmysle predmetu Tímový projekt.

2 Formálna stránka dokumentu

Po formálnej stránke treba vyzdvihnúť, že dokument je písaný príjemnou formou a má prehľadnú štruktúru. Obsahuje malé množstvo pravopisných a štylistických chýb (nie je ich veľa, ale zopár sme našli). Ako nedostatok hodnotíme nevhodné preklady anglických originálov, ďalej používanie slova „užívateľ“ ako ekvivalent slova používateľ. Skloňovanie skratky CA sa zle číta (napr. CA-y, CA-it) bolo by to prehľadnejšie bez násilného skloňovania.

Z pohľadu formy dokumentu niekoľko postrehov:

- Odkaz na použitú literatúru by mal byť zhodný z indexom v zozname použitej literatúry.
- Nesprávne zalomenie textu v zozname použitej literatúry.
- Číslovanie strán je nevhodné, obsah nemá mať vlastné číslovanie rovnaké ako dokument.
- Slovník pojmov obsahuje niekoľko pojmov, ale neobsahuje vysvetlenie týchto pojmov.
- Každý obrázok má vlastný štýl popisku, zarovnanie aj obtekanie textu.
- Netypické číslovanie obrázkov napr.2.0 alebo 2-1.
- Na str. 10 je uvedený prvý obrázok v dokumente a tento má index 2.0; na str. 11 je opäť obrázok 2.0
- Na str. 13 a 15 je sú dva rôzne obrázky s indexom 2.1 alebo 2-1.
- Odkaz na neexistujúci obrázok, strana 31 - obr. 4.5.1.2
- Z formálnej stránky nie je vhodné aby exitovali kapitoly 3-4 úrovne keď sú iba osamotené, dokument pôsobí dojmom nedokončenosti a nevyváženosti.
- Stana 15 odstavec je centrovaný – nie zarovnaný na strany ako v ostatnej dokumentácii
- Od kapitoly 3.4 a ďalej je text zarovnaný vpravo.
- V kapitole 7 – sa mení riadkovanie z 1 na 1,5
- V kapitole 8 – sú nekonzistentné písma, na rovnakej úrovni sú použité rôzne fonty a štýly.

Ako silné negatíva dokumentu sú absentujúce kapitoly špecifikácia a hrubý návrh. Tak isto chýba zadanie projektu. Práve po prečítaní zadania sa objavujú ďalšie chýbajúce oblasti dokumentu ale viacej v posudku k obsahu dokumentu.

3 Obsahová stránka dokumentu

To to je slabá stránka posudzovaného dokumentu. Vzhľadom na veľkosť problematiky PKI je obsah dokumentu venujúci sa tejto problematiky pomerne malý. Ak už pominieme chýbajúce zadanie, aspoň názov projektu napovie, čo by malo byť obsahom dokumentu „Infraštruktúra PKI a vybavenie pre koncových používateľov“. Celkovo dokument budí dojem, že autori povrchne pristúpili k úlohe v tejto fáze projektu. V dokumente je viacero odborných nedostatkov.

Krátke zhrnutie základných nedostatkov :

- O samotnom PKI je tam popísané pomerne málo, a aj to málo je podané na úrovni populárneho článku a nie ako inžinierska analýza problematiky PKI.
- V dokumentácii používajú pojmy autentizácia a autentifikácia ako keby to boli dva rôzne pojmy a nie synonymá.
- V tejto fáze mali byť odovzdané analýza, špecifikácia a hrubý návrh projektu práve špecifikácia a hrubý návrh absentuje v dokumentácii
- Veľká časť obsahu dokumentu sa venuje autentifikácii, čo je okrajový problém zadania.
- Viacero technológii v rámci PKI je tam iba spomenutých, že existujú, ale nie je analyzované načo sa používajú a aký druh problémov riešia.
- Nepožívanie vhodnej terminológie z cieľovej oblasti.
- Problémy pri pojme jednosmerná funkcia alebo algoritmus
- Nepresné formulácie, problematické na správne pochopenie

Ďalej je dokument rozobratý stručne podľa kapitol.

3.1 Kapitola 1 - Predslov

Z predslovu jeden citát: „*Súkromný kľúč je iba jeden a je našim výlučným vlastníctvom, kým verejný kľúč môžeme poskytnúť viacerým osobám, s ktorými sme v elektronickom styku.*“ Takáto formulácia navodzuje pocit, že existuje pre jeden súkromný kľuč viacero verejných kľúčov. Inak je to pekný úvod do problematiky, veľmi vhodný ako článok do časopisu.

3.2 Kapitola 2

- Kapitola 2.2 – Z kontextu vyplýva, že autori nerozumejú pojmom ktoré sa snažia priblížiť čitateľovi.
- Kapitola 2.2 – V praxi sa používajú viac ako 2 algoritmy na výpočet „hešu“ (kryptografická suma), napr. MD4, MD5, SHA-1, crypt a veľa ich modifikácií.
- Kapitola 2.2 – Tvrdenie „*Keďže ide o jednosmernú funkciu, neexistuje inverzná funkcia. Je veľmi náročné nájsť ku kontrolnému súčtu originálny text. Podľa niekoho dokonca úplne nemožné.*“ Autorom odporúčame zauvažovať o informačnom zákone: „Ak nejakú informáciu v čase spracovania stratíme, neexistuje spôsob ako ju späť získať“, jednosmerné funkcie sú nereverzibilné.
- Kapitola 2.2 - „*Kontrolný súčet nám zaručuje integritu správy, t.j. že správa nebola modifikovaná.*“ - samotný kontrolný súčet nezaručuje integritu správy. Útočník môže vytvoriť aj sám kontrolný súčet.
- Kapitola 2.7 - „*Pri elektronickom podpise je však rovnaký problém s distribúciou verejného kľúča, ako pri asymetrickom šifrovaní.*“ -je to spôsobené asi tým, že elektronický podpis je jeden spôsob ako využiť asymetrickú kryptografiu, a tým pádom zdieľa jeho problémy.

3.3 Kapitola 3

Zdá sa nám, že táto kapitola je sem vložená vzhľadom na to, že bola k dispozícii. Nemá žiadny vzťah k spracovávanej téme a problematike PKI. Pojednáva o autentifikácii používateľov a len okrajovo sa dotkne problematiky PKI, ale aj v tejto oblasti je viacero vážnych nedostatkov.

- „*Napríklad v systéme UNIX sa ukladajú jednocestné znehodnotené heslá, kde jednocestný algoritmus je založený na symetrickej šifre.*“ - logická chyba; symetrická šifra nie je jednocestná ale práve že je bijektívna. UNIXové systémy využívajú zväčša na ukladanie hesiel algoritmus MD-5 alebo crypt.
- Autorom odporúčame, ak sa venujú odbornej problematike bezpečnosti, aby pri preklade pojmu, ktorý doteraz nemá v slovenskej odbornej praxi bežný ekvivalent, v zátvorke uviedli pôvodný pojem. Slovo *„soľ“* asi nie je vhodný preklad, nie je jasná ani jeho funkcia (podobne: *„násada“*).
- „*Gridcard*“ – Nie je to metóda pre jednorázové heslá, ale pre schému výzva-odpoveď

(Challenge-response) typický príkladom na jednorázové heslá je S/Key popisovaný neskôr alebo SecureID.

- Kapitola 3.4 – Popisovaný algoritmus sa nazýva CHAP (Challenge-Handshake Authentication Protocol) a existuje viacero jeho modifikácii (MS-CHAP …).
- Odporúčame miesto slova kľúč, v zmysle miesta kde sú uložené privátne kľúče, používať pojem bezpečné úložisko alebo len úložisko, prípadne token. Vety ako „*Dnešné kľúče sa uchovávajú tak, že nikdy neopustia kľúč.*“ nadobudnú zmysel.

3.4 Kapitola 4

- *„rušiť certifikát“* – Vhodnejšie je používať bežný pojem „zneplatňovať certifikát“.
- Hierarchická štruktúra – Z dôvodu krížovej certifikácie medzi autoritami nie je čisto stromová. Hierarchická štruktúra je len jeden zo spôsobov; v praxi sa vyskytuje a veľmi dobre funguje voľne viazaná štruktúra certifikátov bez certifikačných autorít systému Web-of-Trust (Sieť dôvery) implementovaná v systéme PGP.
- V prípade kompromitácie privátneho kľúča CA – CA neprestane existovať, len stratí dôveru svojich klientov. Keďže certifikácia je obchod s dôverou, je to len možný následok kompromitácie.
- „*Popis komunikácie medzi digitálnymi certifikátmi*“ – certifikáty medzi sebou nekomunikujú, komunikujú subjekty, ktoré vlastnia certifikáty.
- Kapitola 4.4.1, bod 2 – správne znenie by malo byť: „CA zašle smerovaču NY certifikát pražského smerovača“, podanie v dokumentácii „*Cerifikačné autorita pošle Pražskému smerovaču certifikát podpísaný jej súkromným kľúčom*“ je nelogické vzhľadom na to, že pražský smerovač svoj certifikát pozná, prípadne je to nelogický krok na žiadosť od NY smerovača.
- Kapitola 4.4.1, bod 3 – Smerovač ako subjekt neschvaľuje certifikát a verejný kľúč, ale ho overuje.
- Kapitola 4.4.1, bod 5 – asi došlo k zámene bodov 2 a 5.
- Kapitola 4.5 – Pracuje sa tu s pojmom dôveryhodné certifikáty absolutistickom vyhlásení a zároveň sa predpokladá, že WWW prehliadač ako prostriedok v PKI obsahuje dôveryhodné certifikáty – tie, ktoré určuje firma Microsoft (viď príklad v dokumentoch). Pritom práve

produkty Microsoftu neobsahujú pre Slovensko najdôveryhodnejší certifikát – certifikát národnej CA. V kontexte kapitoly čitateľ nadobudne pocit, že tento certifikát nie je dôveryhodný. Chýba upozornenie, že tento zoznam je voliteľný a je daný dôverou subjektu v dané inštitúcie, ktoré poskytujú certifikačné služby.

- Obrázok 4-4 – Zle vyjadrené certifikačné vzťahy. Dôvera CA-A a CA-B je jednostranná.
- Kapitola 4.7 – Odporučil by som autorovi tejto kapitoly, aby prediskutoval skutočnosti uvedené v tejto kapitole s autorom kapitoly 3.4.2.1. Pre certifikačné autority sa bežne používa HSM modul ako úložisko privátnych dát CA, ktoré spĺňa normu NIST FIPS 140 level 3. Odporúčame sa viac držať faktov pre inžiniersku dokumentáciu ohľadom ochrany kľúčov CA a prípadne bežnej prevádzkovej praxe.

3.5 Kapitola 5

- Kapitola 5 – Je veľmi nepresné tvrdiť, že norma X.509 je vo svete Internetu mladá. Norma X.509 vznikla v roku 1988. V roku 1993 bola aktualizovaná na verziu 2 atď.
- Kapitola 5.1 – Certifikáty bývajú kódované viacerými spôsobmi, nielen pomocou DER. Typicky sa používajú: PEM, DER, Base64, PKCS#7 a PKCS#12.
- Kapitola 5.1.1.5 – Bezpečnostný dôvod na skrátenie doby platnosti certifikátu CA je nelogický, pretože certifikačná autorita nepomerne menej krát využíva svoj privátny kľúč. V prípade koreňovej certifikačnej autority to býva rádovo v jednotkách použití ročne.
- Kapitola 5.1.1.5 – Tvrdenie, že platnosť certifikátu CA by mala vypršať až po poslednom ňou vydanom certifikáte je nelogické, lebo podriadený certifikát sa vydáva s prihliadnutím na ostávajúcu dobu platnosti certifikátu CA, kedže tento certifikát bol vydaný skôr a nemôže sa meniť.
- Kapitola 5.3 – Tvrdenie „*Ak súkromný kľúč niekto odcudzil, je možné poslať žiadosť podpísanú týmto kľúčom.*“ naráža na praktický problém, ak mi niekto odcudzí úložisko privátnych kľúčov, asi veľmi problematicky podpíšem žiadosť o zneplatnenie certifikátu. Tento odstavec zároveň ponecháva možnosť nezneplatniť certifikát ak útočník chce zneplatniť certifikát alebo to tak nie je? (Čitateľ ostáva na vážkach.) V bežnej praxi sa bez rozlíšenia prípadov zneplatňuje certifikát už len pri podozrení na možnú kompromitáciu privátnych dát. Neskôr v texte je toto uvedené na pravú mieru, ale čitateľ ostáva

dezorientovaný.

- Kapitola 5.4 – Bývalý majiteľ kompromitovaného certifikátu nemá smolu, lebo najbližšie vydanie CRL obsahuje presný čas (revocationDate) odkedy je certifikát zneplatnený a teda dáta podpísané prislúchajúcim privátnym kľúčom nedôveryhodné. Je na overovateľovi podpisu, aby si overil, či použitý certifikát (privátny kľúč pri podpisovaní) nie je na zozname zneplatnených certifikátov (CRL).
- Kapitola 5.7 – Nie je uvedený primárny dôvod využívania TSA a časových pečiatok, a to zabránenie podvodom pri zneplatňovaní certifikátov.

3.6 Kapitola 6 – Použitá literatúra

- 1 – Chýba popis, v ktorom ročníku a čísle časopisu PC REVUE sa dané články vyskytovali
- 6 – Popisovaná linka https://cert.utc.sk/ca je neplatná (403 - Forbidden).
- 9 - Linka http://www.economy.gov.sk/doc/komentar.htm je neplatná (404 - Not Found).

Je málo pravdepodobné, že popisované neplatné WWW linky by zanikli v priebehu jedného týždňa od odovzdania dokumentácie. Do budúcna odporúčame autorom sa vyvarovať nepresných liniek a WWW odkazov. Prípadne striktnejšie určiť zdroje, ktoré použili pri analýze.

3.7 Kapitola 7 - Slovník základných pojmov

Opätovne sa v dokumente stretávame so slovníkom pojmov. Tentokrát majú slová popísaný aj svoj význam. Problémom je nekonzistencia pojmov v slovníku z pojmami v texte:

- „digitálny odtlačok“ a „elektronický odtlačok“ – slová sú síce z pohľadu slovenčiny alebo bežnej praxe ekvivalentné. Prípadne sa pojmy v predchádzajúcom texte nenachádzajú (Certifikát transakcie).
- Nevhodné preklady anglických pojmov a ich nepochopenie zo strany autorov „*Metóda verejného kľúča (anglicky Public Key Infrastructure – PKI) - pozri Asymetrické šifrovanie*“. Pojmy PKI a Asymetrické šifrovanie spolu nesúvisia. PKI je v jednoduchosti infraštruktúra pre správu a fungovanie implementácie asymetrických šifrovacích algoritmov v praxi.
- Zle vysvetlený pojem „Jednocestný algoritmus“ – v jednoduchosti sa jedná a o funkciu (algoritmus), ktorá nie je bijektívna. „Nekonečný“ obor hodnôt vstupu sa mapuje na konečnú množinu výstupov.

3.8 Kapitola 8

- Iba dve chyby – hash a X.509 nie sú skratky ale pojmy.
- PGP nie je kryptografický balík ale alternatívny prístup k PKI.

Zo skratiek vystupujúcich bežne v dokumente chýbajú napr. RA, CRL, OCSP, TSA.

3.9 Porovnanie s ponukou tímu

Z ponuky tímu č.4 citujeme:

Našou úlohou bude vytvorenie web stránky, kde budeme názorne prezentovať princípy a činnosť Public Key infrastructure (PKI). Na stránke nájdeme základné informácie a vysvetlenie činnosti PKI a kryptografie. Taktiež bude na stránke prezentovaná činnosť PKI v praxi.

Ďalej sa budeme venovať témam s tým súvisiacimi, certifikáty verejného kľúča, a elektronický podpis. Na stránke budeme demonštrovať použitie certifikátov verejného kľúča na podpisovanie a overovanie podpisov elektronických dokumentov u koncových používateľov.

Ako posledný bod bude návrh a implementácia PKI a aplikácia slúžiaca na podpis a overenie elektronického dokumentu u koncového používateľa. Pri návrhu a implementácií budeme dodržiavať platné štandardy, zapísané v dokumentoch RFC2511, RFC2511,RFC2560, RFC2630,RFC2787, RFC2986, RFC3280, RFC3369, zákon NR SR č. 215/2002 Z.z. o elektronickom podpise a vyhlášku NBÚ k zákonu o elektronickom podpise č. 536 až 542/2002.

Z uvedeného vidno, že v ponuke poznali všetky vyhlášky NBÚ k danej problematiky a všetky normy RFC, ale v samotnej analýze tomu už tak nie je – viď. použitá literatúra. Rovnako v ponuke sa zaväzujú k vytvoreniu WWW prezentácie problematiky, v dokumente nie je podobná úloha ani spomenutá. Deklarujú demonštráciu použitia certifikátov, v dokumente nie sú analyzované možné CA nutné na takéto konanie ani iné softvérové prostriedky potrebné na PKI. Tak isto je uvedený posledný bod návrh a implementácia PKI a aplikácia na podpisovanie a overovanie dokumentov, opäť bez analýzy, prípadne špecifikácie požiadaviek na tieto prostriedky v dokumentácii.

4 Záver

Z predchádzajúceho textu vidno, že posudzovaný dokument má viacero rôzne závažných nedostatkov. Väčšina nedostatkov je práve v obsahu dokumentu. Dokument je po formálnej stránke obstojne spracovaný, ale v obsahovej časti absentujú niektoré podstatné kapitoly. Chýbajú kapitoly povinné pre túto fázu ako špecifikácia a hrubý návrh. Pomerne problematicky sa posudzoval tento dokument vzhľadom na negatíva v ňom obsiahnuté, tých niekoľko pozitív, čo sme našli, bolo treba ťažiť.

Celkovo dokument budí dojem, že tím poňal tento míľnik projektu len ako nutnú časť, ktorá nemá veľkú váhu a toto sa odrazilo na kvalite dokumentu. Ak by sme tento dokument zobrali ako referenciu znalostí problematiky PKI tímom č.4, potom môžeme konštatovať nepochopenie základnej problematiky v oblasti. Dúfame, že vyjadrenia v tomto posudku budú brať ako konštruktívne obohatenie svojich vedomostí a výsledné vylepšenie ďalších výsledkov v predmete Tímový projekt ako aj profesionálnom živote.