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

Infraštruktúra PKI a vybavenie pre koncových používateľov

Webová prezentácia

Tímový Projekt

Tím číslo 4 PSS:
Bc. Peter Mulinka
Bc. Radovan Škríb
Bc. Martin Mačica
Bc. Jozef Hamar
Bc. Tomáš Smolek

Rok: 2004 / 2005

Vedúci projektu: Doc. Ing. Ladislav Hudec, Csc.

Obsah

1. Zadanie

Infraštruktúra PKI a vybavenie pre koncových používateľov. Pre pedagogické účely vytvorte WEB aplikáciu demonštrujúcu princípy a činnosť PKI. Taktiež demonštrujte použitie certifikátov verejného kľúča na podpisovanie a overovanie podpisov elektronických dokumentov u koncových používateľov. Navrhnite a implementujte PKI a aplikáciu na podpisovanie a overenie podpisu elektronického dokumentu u koncového používateľa. Pri návrhu rešpektujte platné štandardy.

2. Implementácia

V tejto kapitole sa venujeme implementácii jednotlivých častí navrhnutej webovej prezentácie. Webovskú aplikáciu môžeme z hľadiska implementácie rozdeliť na dva celky, ktoré spolu úzko súvisia. Je to implementácia jednotlivých scenárov vo flash-i a implementácia samotnej webovej stránky do ktorej je flash zasadený.

2.1. Implementácia scenárov vo flash-i

Jednotlivé flash scenáre sme vytvorili pomocou nástroja Macromedia Flash MX 2004. Každý scenár je reprezentovaný ako zvlášť scéna. Jednotlivé obrázky a symboly použité v daných scénach sme zobrali z knižnice obrázkov, ktorú poskytuje návrhový prostriedok Microsoft Visio 2003. Výsledné projekty spolu s jednotlivými scénami sa nachádzajú na priloženom cd. Na cd sa nachádzajú aj jednotlivé scény, ktoré je možné prehrať vo flash prehrávači alebo vo web prehliadači, ktorý podporuje prehrávanie flash prezentácií.

2.2. Implementácia webovej stránky

Stránka je vytvorená pomocou HTML štandardu 4.01 Transitional. Na jej tvorbu bol použitý iba textový editor VIM. Každá kapitola je uložená v samostatnom súbore s príponou „html“. Pre zakomponovanie interaktívnych flash animácií do HTML sa použil doporučovaný spôsob od samotného výrobcu flashu, spoločnosti Macromedia. Na priloženom cd nosiči je uložená celá štruktúra webovej stránky aj s flash-mi. Stránku je možné prezerať aj lokálne s internetovým prehliadačom, ktorý podporuje obrázky a prehrávanie flash súborov.

3. Príručka používateľa

3.1. Inštalačná príručka

Vo webovej prezentácii sú použité iba relatívne linky, z toho vyplýva, že je ju možné umiestniť pod hocijaký adresár. Pre jej spustenie je potrebný len internetový prehliadač podporujúci obrázky, flash a kaskádové štýly.

Podporu flash-u možno dosiahnuť nainštalovaním si plugin-u do prehliadača zo stránky výrobcu: www.macromedia.com . Kaskádové štýly a obrázky dnes už podporuje každý slušnejší prehliadač ako napríklad Mozilla, MS Internet Explorer, Netscape alebo Opera.

3.2. Používateľské rozhranie

Webová prezentácia opisujúca infraštruktúru verejného kľúča sa skladá z troch hlavných častí:

- Menu
- Prezentačná oblasť
- Navigačný panel

Menu sa nachádza v ľavej časti prezentácie, je rozdelené do niekoľkých kapitol, pod ktorými sa nachádzajú aktívne linky. Tieto otvoria danú časť prezentácie v prezentačnej oblasti.

Prezentačná oblasť je situovaná v pravej časti prezentačného okna, hneď pod nadpisom. Zobrazuje sa v nej samotný obsah prezentácie.

Navigačný panel sa zobrazí na pravej strane hneď pod prezentačnou časťou. Pomocou neho sa dá prechádzať celou prezentáciou sekvenčne smerom dopredu alebo dozadu. Pre spríjemnenie študovania prezentácie sa medzi linkami „Späť“ a „Ďalej“ nachádza linka „Slovník“, ktorá otvorí nové okno prehliadača a zobrazí v ňom slovník pojmov. Rovnakú linku možno nájsť na začiatku menu pod linkou „Úvod“.

Príloha A: Riadenie projektu

Záznam o 1. stretnutí tímového projektu

číslo stretnutia	1
miesto stretnutia	D109
čas stretnutia	12.10.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

1. dohoda na termínoch stretnutí vrátane nasledujúceho stretnutia
2. Hudec: podrobnejšia špecifikácia požiadaviek, oznámenie o celkových predpokladaných črtách systému
3. zvolenie vedúceho (Jozef Hamar) a zástupcu vedúceho (Tomáš Smolek)
4. Jožo: zadelenie funkcií jednotlivým členom týmu

Zadelenie funkcií

funkcia	**jozef**	**peter**	**rado**	**tomáš**
vedúci	x			
výroba zápisnice			x	
analytik	x	x		
tvorba tímovej stránky				x
dizajn web stránky		x		
Programátor - flash			x	

Záznam o 2. stretnutí tímového projektu

číslo stretnutia	2
miesto stretnutia	D109
čas stretnutia	16.10.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Martin Mačica, Peter Mulinka
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

5. diskusia o TP s vedúcim projektu
6. zmena v zadelení funkcií (viď tabuľka)
7. prezentácia rôznych návrhov stránok nášho tímu (Peter Mulinka), výber jedného návrhu
8. nasadenie vybratého návrhu na nám určené webové miesto (Peter Mulinka)
9. diskusia o vývojovom nástroji pre fázu 1 TP, zadelená úloha na analýzu možností, ktoré poskytuje Flash (Martin Mačica, Radomír Škrib)
10. úlohy: podrobné naštudovanie problematiky Jozef Hamar, Tomáš Smolek

Zadelenie funkcií

funkcia	**jozef**	**peter**	**rado**	**tomáš**	**martin**
vedúci tímu	x			z	
tvorba zápisnice			x		z
analytik	x	z		x	
tvorba tímovej stránky		x		z	
Webovská časť projektu		z		x	
Programátor - flash			x		x
Dokumentácia	x	x	x	x	xx

Záznam o 3. stretnutí tímového projektu

číslo stretnutia	3
miesto stretnutia	D109
čas stretnutia	23.10.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Martin Mačica, Peter Mulinka
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

11. diskusia o TP s vedúcim projektu, doplnenie znalostí (Jozef Hamar)
12. diskusia o prvej časti TP – výber vývojového prostriedku (Macromedia Flash MX 2004)
13. úlohy na nasledovné týždne:
    - špecifikácia návrhov pre prvú časť TP (Jožo, Tomáš)
    - vypracovanie návrhov vo vybranom vývojovom prostriedku (Rado, Martin)
14. spravenie poriadku v súboroch na tímovom ftp (Tomáš)
5. aktualizovanie tímovej stránky (Peter)

Záznam o 4. stretnutí tímového projektu

číslo stretnutia	4
miesto stretnutia	D109
čas stretnutia	2.11.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Martin Mačica, Peter Mulinka
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

15. diskusia o TP s vedúcim projektu, doplnenie znalostí (Jozef Hamar)
16. diskusia o prvej časti TP – prezentácia návrhov
17. úlohy na nasledovný týždeň:
    - dokončenie analýzy (Jožo, Tomáš)
    - vypracovanie návrhov vo vybranom vývojovom prostriedku (Rado, Martin)
    - dokončenie a odovzdanie prvej časti dokumentácie (všetci)
    - vyhľadanie vhodných obrázkov potrebných pre WEB aplikáciu demonštrujúcu princípy a činnosť PKI (Rado, Martin)
4. aktualizovanie tímovej stránky, úvod do dokumentácie (Peter)

Záznam o 5. stretnutí tímového projektu

číslo stretnutia	5
miesto stretnutia	D109
čas stretnutia	9.11.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Martin Mačica, Peter Mulinka
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

18. diskusia o TP s vedúcim projektu, doplnenie znalostí (Jozef Hamar)
19. kontrola úloh zadelených na prechádzajúcom stretnutí (všetky splnené)
20. rozdelenie úloh, ktoré treba spraviť do 12.11. (odovzdanie dokumentácie)
21. úlohy ktoré treba vypracovať do konca týždňa:
    - vyhotovenie analytickej časti dokumentácie (Jožo, Tomáš)
    - vyhotovenie obrázkov potrebných v dokumentácii (Rado)
    - napísanie úvodu do prvej časti dokumentácie (Peter)
    - záverečné dokončenie dokumentácie (Martin)
22. aktualizovanie tímovej stránky (Peter)
23. prebratia a analýza práce konkurenčného týmu

Záznam o 6. stretnutí tímového projektu

číslo stretnutia	6
miesto stretnutia	D109
čas stretnutia	16.11.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Martin Mačica, Peter Mulinka
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

24. diskusia o TP s vedúcim projektu
25. kontrola úloh zadelených na prechádzajúcom stretnutí
    - vyhotovenie analytickej časti dokumentácie (Jožo, Tomáš) – splnené
    - vyhotovenie obrázkov potrebných v dokumentácii (Rado) – splnené
    - napísanie úvodu do prvej časti dokumentácie (Peter) – splené
    - záverečné dokončenie a odovzdanie dokumentácie (Martin, Jožo)
26. rozdelenie úloh, ktoré treba spraviť do ďalšieho stretnutia
    - vyhotovenie a odovzdanie posudku k projektu konkurenčného týmu (Martin, Jožo, Tomáš) – termín 19.11.
    - scenáre (hrubý návrh) k webovskej aplikácii (Rado) – termín 23.11.
    - hrubý návrh stránky kde pobeží webovská aplikácia (Peter) – termín 23.11.
27. aktualizovanie tímovej stránky (Peter)

Záznam o 7. stretnutí tímového projektu

číslo stretnutia	7
miesto stretnutia	D109
čas stretnutia	23.11.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Peter Mulinka
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

28. diskusia vedúcim projektu o tom čo má obsahovať webovská aplikácia
29. preberanie a dopĺňanie navrhnutých scenárov, navrhnuté ďalšie scenáre
30. kontrola úloh zadelených na prechádzajúcom stretnutí
    - vyhotovenie a posudku k projektu konkurenčného týmu (Jožo, Tomáš) – termín 19.11. – splnené
    - posudku k projektu konkurenčného týmu (Martin) – termín 19.11. – nesplnené, odovzdaný až 22.11.
    - scenáre (hrubý návrh) k webovskej aplikácii (Rado) – termín 23.11. – splnené
    - hrubý návrh stránky kde pobeží webovská aplikácia (Peter) – termín 23.11. – splnené
31. rozdelenie úloh, ktoré treba spraviť do ďalšieho stretnutia
    - reakcia na posudok od konkurenčného týmu (Peter) – termín 26.11. 10:00
    - odovzdanie reakcie na posudok (Martin) – termín 26.11.
    - úprava návrhu stránky pre webovskú aplikáciu, návrh menu, tvorba slovníku pojmov (Peter) – termín 30.11.
    - doplnenie hrubého návrhu webovskej aplikácie (Rado) – termín 25.11.
    - naprogramovanie prototypu webovskej aplikácie (Rado, Martin) – termín 30.11
    - návrh scenárov pre overovanie certifikátov a CRL (Jožo, Tomáš)
    - návrh scenára pre časovú pečiatku (Peter)
32. aktualizovanie tímovej stránky (Peter)

Záznam o 8. stretnutí tímového projektu

číslo stretnutia	8
miesto stretnutia	D109
čas stretnutia	30.11.2004 - 9.15
zúčastnení	Jozef Hamar, Tomáš Smolek, Radomír Škrib, Peter Mulinka, Martin Mačica
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

33. prezentácia prototypov prezentácie vedúcemu projektu
34. preberanie a dopĺňanie navrhnutých scenárov
35. kontrola úloh zadelených na prechádzajúcom stretnutí
    - reakcia na posudok od konkurenčného tímu (Peter) – termín 26.11. 10:00 – splnené
    - odovzdanie reakcie na posudok (Martin) – termín 26.11. – nebolo treba
    - úprava návrhu stránky pre webovskú aplikáciu, návrh menu, tvorba slovníku pojmov (Peter) – termín 30.11 – splnené
    - doplnenie hrubého návrhu webovskej aplikácie (Rado) – termín 25.11 – splnené
    - naprogramovanie prototypu webovskej aplikácie (Rado, Martin) – termín 30.11 – Rado – splnené, Martin – čiastočne splenené
    - návrh scenárov pre overovanie certifikátov a CRL (Jožo, Tomáš) – nesplnené
    - návrh scenára pre časovú pečiatku (Peter) – nesplnené
36. rozdelenie úloh, ktoré treba spraviť do ďalšieho stretnutia
    - naprogramovanie všetkých scenárov (Martin, Rado) – termín 7.12.
    - práca na stránke pre webovskú aplikáciu, integrovanie flashu (Peter) – termín 7.12.
    - návrh scenárov pre overovanie certifikátov a CRL (Jožo, Tomáš) – termín 4.12.
    - návrh scenára pre časovú pečiatku (Peter) – termín 4.12.
37. aktualizovanie tímovej stránky (Peter)

Záznam o 9. stretnutí tímového projektu

číslo stretnutia	9
miesto stretnutia	D109
čas stretnutia	7.12.2004 - 9.15
zúčastnení	Jozef Hamar, Radomír Škrib, Peter Mulinka, Martin Mačica
vedúci	Doc. Ing. Ladislav Hudec, PhD.
vypracoval	Radomír Škrib
overil	Jozef Hamar

Záznam stretnutia:

38. prezentácia prototypov webovej prezentácie vedúcemu projektu
39. preberanie a dopĺňanie navrhnutých scenárov, konečná úprava, definovanie štruktúry stránky webovej prezentácie
40. kontrola úloh zadelených na prechádzajúcom stretnutí
    - naprogramovanie všetkých scenárov (Rado) – termín 7.12. – väčšina spravená
    - naprogramovanie všetkých scenárov (Martin) – termín 7.12. – väčšina spravená
    - práca na stránke pre webovskú aplikáciu, integrovanie flashu (Peter) – termín 7.12. – splnené
    - návrh scenárov pre overovanie certifikátov a CRL (Jožo, Tomáš) – termín 4.12. – splnené
    - návrh scenára pre časovú pečiatku (Peter) – termín 4.12. – splnené
41. rozdelenie úloh, ktoré treba spraviť do ďalšieho stretnutia
    - **Peto**
        - skrátiť úvod
        - pridať banner
        - zmeniť štruktúru stránky, pridať posúvanie späť – dopredu, rolovanie a úprava obsahu
        - napísať inštalačnú a používateľskú príručku
    - **Rado**
        - spraviť flash pre časovú pečiatku, ocsp, upraviť existujúce flashe (nahradiť „vygenerovať“, upraviť hierarchiu CA – RA, upraviť flash integrita, vymeniť archív súkromných kľúčov za CRL, pri odvolaní spísať možnosti,)
        - napísanie dokumentácie k implementácii
    - **Tomáš**
        - k nasledovným flashom urobiť doprovodné texty: šifrovanie, certifikácia a CRL (napr. k žiadosti o vydanie popis PKCS10, popísať vlastnosti hashu, popísať štruktúru žiadosti a certifikátu atď)
    - **Martin**
        - spraviť prezentáciu pre časť CRL, použitie a overenie certifikátov
        - obsah prezentácie, zhotovenie dokumentácie

- **Jožo**
  - doprovodné texty k nasledovným flashom: použitie a overovanie certifikátov, zneplatnenie certifikátov
  - prečítať a zaradiť OCSP

42. aktualizovanie tímovej stránky (Peter)

Príloha B: Obsah CD nosiča

Ponuka	dokumenty\ponuka.doc
Analýza PKI	dokumenty\analyza.doc
Posudok k analýze konkurenčného tímu	dokumenty\posudok.doc
Posudok konkurenčného tímu k analýze	dokumenty\posudok_OdXchoice.pdf
Reakcia na posudok konkurenčného tímu	dokumenty\reakcia_na_posudok.doc
Dokumentácia k implementácii Webovej aplikácie	dokumenty\prezentacia.doc
Prílohy k zápisom o stretnutí	dokumenty\rôzne
Webová prezentácia ilustrujúca princípy PKI	prezentacia\