METODE JAKE AUTENTIFKACIJE U SAVREMENIM RAČUNARSKIM SISTEMIMA

Uroš Racković, *GŠ Vojske Srbije Uprava za vezu i informatiku Beograd, rackovicu@gmail.com*

Rezime: *Autentikaciju korisnika se može izvršiti na tri načina: na osnovi nečega što korisnik zna (lozinka ili PIN), na osnovu nečega što korisnik poseduje (bezbednosni token ili smart kartica), na osnovu nečega što korisnik jeste (fizičke karakteristike). Sva tri autentikaciona mehanizma imaju svoje nedostatke, tako da eksperti iz oblasti zaštite podataka predlažu primenu dva zasebna mehanizma odnosno princip dvofaktorske autentikacije. Implementacija dvofaktorske autentikacije zahteva skup hardver i infrastrukturne promene, pa je najčešće bezbednost svedena na upotrebu jednog mehanizma autentikacije. Ovaj rad opisuje jedan od načina implementacije dvofaktorske autentikacije u Windows operativnim sistemima upotrebom smart kartica.*

Ključne reči: *Autentikacija, Smart kartica, GINA*

METHODS OF STRONG AUTHENTICATION IN ACTUAL COMPUTER SYSTEMS

Abstract: *We can authenticate an identity in three ways: by something the user knows (such as a password or personal identification number), something the user has (a security token or smart card) or something the user is (a physical characteristic). All three authentication mechanisms have drawbacks, so security experts recommend using two separate mechanisms, a process called two-factor authentication. But implementing two-factor authentication requires expensive hardware and infrastructure changes. Therefore, security has most often been left to just a single authentication method. This paper describes one of the ways of implementation two-factor authentication in Windows operating systems by using smart cards.*

Key words: *Authentication, Smart card, GINA.*

UVOD

Savremene računarske mreže se, skoro u potpunosti, zasnivaju na Internet tehnologijama i TCP/IP protokolima. Automatizovani informacioni sistemi zasnovani na Internet tehnologijama imaju brojne slabosti sa aspekta zaštite bezbednosti podataka, što je u velikoj meri prouzrokovano arhitekturom računarske mreže Internet/Intranet tipa [1]:

- TCP/IP protokoli nisu projektovani da zadovolje zahteve za zaštitom informacija
- Internet je mreža sa komutacijom paketa u kojoj se relativno jednostavno pristupa informacijama koje se prenose i moguće je ubacivanje poruka uz nemogućnost kasnijeg određivanja njihovog porekla i sadržaja

Primenom kriptografije realizuju se četiri osnovna bezbednosna servisa: tajnost podataka, provera autentičnosti, provera integriteta primljenih podataka, neporecivost transakcija. Zaštita tajnosti podataka se vrši primenom simetričnih kriptografskih algoritama, dok se ostali servisi realizuju primenom asimetričnih kriptografskih algoritama.

1. MEHANIZMI AUTENTIKACIJE KORISNIKA

Autentikacija entiteta je proces uz pomoć kog je jedna strana uverena (tako što joj je predstavljena odgovarajuća evidencija) o identitetu druge strane uključene u protokol i da je druga strana zapravo učestvovala (bila aktivna u trenutku ili neposredno pre trenutka u kome je evidencija bila predstavljena). Tehnike autentikacije korisnika mogu biti podeljene u tri glavne kategorije u zavisnosti od toga na čemu se evidencija zasniva:

- na nečemu što korisnik zna – primeri uključuju standardne lozinke, PIN (*Personal Identification Number*) kodove, i privatne i tajne ključeve čije znanje se demonstrira u *challenge-response* protokolima
- na nečemu što korisnik poseduje – ovo je tipično nešto što se fizički poseduje, neka tehnička oprema, kao npr. magnetne ili *smart* kartice, kalkulatori za generisanje vremenski promenljivih lozinki
- na nečemu svojstvenom, jedinstvenom za korisnika – ove metode koriste ljudske fizičke karakteristike i nesvesne reakcije (biometrika) gde spadaju prepoznavanje glasa, prepoznavanje ručnih potpisa, otisak prsta, struktura retine,…

Zadnjih godina se pokazalo da autentikacija sa samo jednom od ove tri tehnike nije dovoljno bezbedna, pa se današnji sistemi koji zahtevaju visok nivo sigurnosti uglavnom baziraju na dvo i tro faktorskoj autentikaciji (korišćenje dve ili sve tri navedene tehinke spregnuto). Primeri koji pokazuju ovu tvrdnju su da korišćenje samo lozinki za autentikaciju, omogućavaju potencijalnom napadaču da ukrade lozinku i na taj način lažno autentikuje sebe, ili da ukrade token na kome su kriptografski parametri autentikacije i da na taj način lažno autentikuje sebe. Ovakve vrste prevara su u današnje vreme dostigle enormne cifre, po količini štete (novčane, materijalne) koju prave u razvijenim zemljama sveta. Korišćenje dvokomponentne autentikacije podrazumevalo bi sledeće: ako se na tokenu čuvaju kriptografski parametri autentikacije (ono što se poseduje - token), i ako sam pristup tim parametrima zaštitimo nekom lozinkom (ono što se zna), onda sprečavamo potencijalnog korisnika da pristupi parametrima tokena, t.j. da se autentikuje čak i da ukrade token, jer ne zna lozinku za token [2].

2. AUTENTIKACIJA KORISNIKA NA PLATFORMAMA NA BAZI WINDOWS OPERATIVNIH SISTEMA

Windows operativni sistemi počev od *Windows 2000* podržavaju nekoliko protokola za verifikaciju identiteta korisnika koji tvrdi da poseduje korisnički nalog na sistemu, uključujući protokole za autentikaciju *dial-up* konekcija i protokole za autentikaciju spoljašnjih korisnika koji pristupaju mreži preko Interneta. Međutim postoje samo dva izbora mrežnih protokola:

- Kerberos verzija 5. *Kerberos* verzija 5 autentikacioni protokol je primarni mrežni autentikacioni protokol na računarima sa operativnim sistemom *Windows 2000* ili novijim [3].
- Windows NT LAN Menager (NTLM). NTLM protokol je bio primarni mrežni autentikacioni protokol za operativni sistem *Windows NT 4.0*. Zadržan je i u narednim verzijama *Windows* operativnih sistema pre svega iz razloga kompatibilnosti. NTLM se takođe koristi i za autentikaciju pri logovanju na samostalni računar sa *Windows 2000* operativnim sistemom [3].

Računari sa *Windows 3.11, Windows 95, Windows 98,* ili *Windows NT 4.0* operativnim sistemima koriste NTLM protokol za mrežnu autentikaciju u *Windows 2000* domenima, oni sa *Windows 2000* operativnim sitemom ili novijim koriste NTLM samo za autentikaciju na servere sa *Windows NT 4.0* operativnim sistemom ili kada pristupaju resursima na *Windows NT 4.0* domenima.

Glavni proces autentikacije korisnika je interaktivno prijavljivanje. Interaktivno prijavljivanje je obavezno za *Microsoft Windows Server* 2003, *Windows XP*, *Windows* 2000 i *Windows NT* 4.0 operativne sisteme [3]. Interaktivno prijavljivanje obezbeđuje način za identifikaciju autorizovanih korisnika i određivanje kada im je dozvoljeno da se prijave ili pristupe sistemu.

3. KOMPONENTE INTERAKTIVNOG PRIJAVLJIVANJA

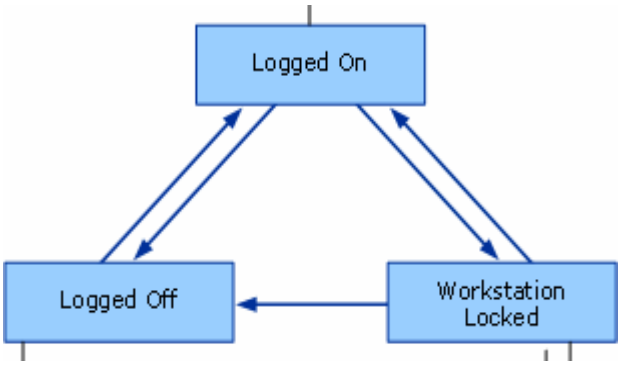
Komponente interaktivnog prijavljivanja na sistem su odgovorne za uspostavljanje sigurne autentikacije

3.1 Winlogon

Winlogon je izvršni fajl (*Winlogon.exe*) odgovoran za upravljanje interakcijom sa korisnikom, on inicira proces prijavljivanja korisnika na *Windows Server* 2003, *Windows* 2000, *Windows XP* i *Windows NT* 4.0. *Winlogon* je odgovoran za sledeće zadatke:

- zaključavanje *desktop*-a
- prepoznavanje standardnih SAS (*Secure Attention Sequence*)
- određivanje SAS rutina
- učitavanje profila korisnika
- kontrola *Screen Saver*-a

Zaključavanje *desktop*-a. *Winlogon* sprečava neautorizovanog korisnika da pristupi sistemu tako što zaključava *desktop* računara. U svakom trenutku, *Winlogon* je u jednom od tri moguća stanja: prijavljeno, odjavljeno ili radna stanica zaključana



Slika 1: Winlogon stanja

Winlogon koristi tri *desktop*-a: *Winlogon*, *Screen-saver* i podrazumevani. Koji će od ova tri koristiti zavisi od stanja u kom se nalazi i aktivnosti korisnika**.**

Prepoznavanje standardnih SAS. *Winlogon* registruje *boot* proces, koji obezbeđuje da nijedan program ne može pristupiti istoj ključnoj sekvenci i kompromitivati proces prijavljivanja imitirajući *Winlogon* i njegove dijaloge.

Određivanje SAS rutina. Kada *Winlogon* prepozna SAS događaj ili GINA (*Graphical Identification and Authentication*) generiše SAS, *Winlogon* poziva jednu od GINA SAS funkcija, koja vrši obradu SAS događaja.

Učitavanje profila korisnika. Posle uspešnog logovanja, *Winlogon* učitava profil korisnika u HKEY_CURRENT_USER redžistri ključ.

Kontrola Screen Saver-a. *Winlogon* prati aktivnosti tastature i miša i određuje kada da se aktivira *screen saver*. Kada se on postavi kao otkazana bezbednost, *Winlogon* tretira radnu stanicu kao zaključanu, GINA prikazuje „računar zaključan“ dijalog. Kada *screen saver* nije postavljen kao otkazana bezbednost, korisnik je u mogućnosti da pristupi *destop*-u bez upozorenja da ponovo unese akreditive.

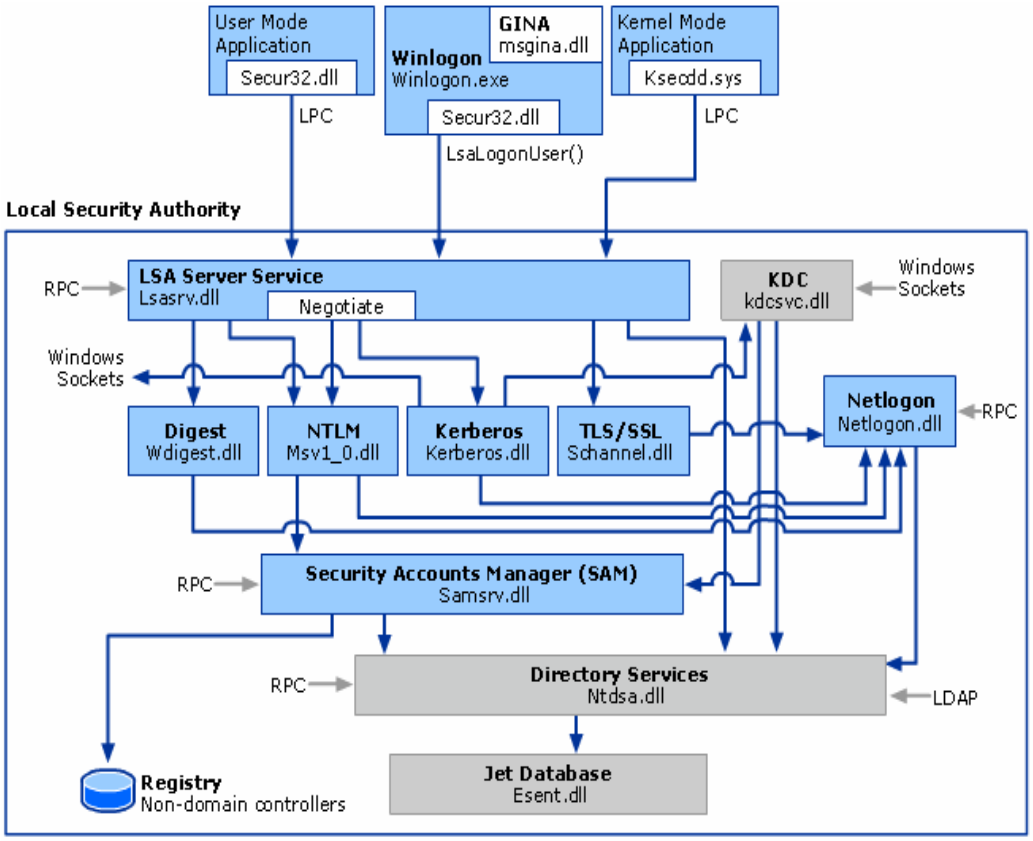
3.2 GINA

GINA je DLL (*Dynamic Link Library*) modul koji funkcioniše u okviru bezbednosnog konteksta *Winlogon*. *Winlogon* učitava GINA pre *boot* procesa. GINA je odgovorna za izvršavanje SAS događaja i aktiviranje korisnikove ljuske (*shell*). U nekim slučajevima GINA može generisati SAS događaje. Za *Windows Server* 2003, *Windows XP* i *Windows* 2000 Msgina.dll je podrazumevana GINA. Može biti zamenjena kako bi podržala specifične i jedinstvene metode autentikacije. Prilagođavanje GINA omogućuje upotrebu autentikacionih hardverskih tokena, kao što su skeneri mrežnjače, posedovanje *smart* kartice i druga rešenja.

3.3 LSA (Local Security Agent)

LSA je zaštićeni bezbednosni podsistem koji pomaže u kreiranju bezbedne interakcije sa korisnikom kod *Windows* operativnih sistema. *Winlogon* i GINA pozivaju LSA da obradi akreditive logovanja. Sledeće komponente se koriste tokom logovanja korisnika u bezbednosnom kontekstu LSA:

- Autentikacioni paketi
- SAM (*Security Accounts Manager*)
- AD (*Active Directory*)



Slika 2: Arhitektura LSA

Kao što slika 2 pokazuje, svi pozivi od *Winlogon*-a se šalju upotrebom Secur32.dll *LsaLogonUser* poziva. Onda LSA server servis određuje koji autentikacioni paket da koristi za logovanje.

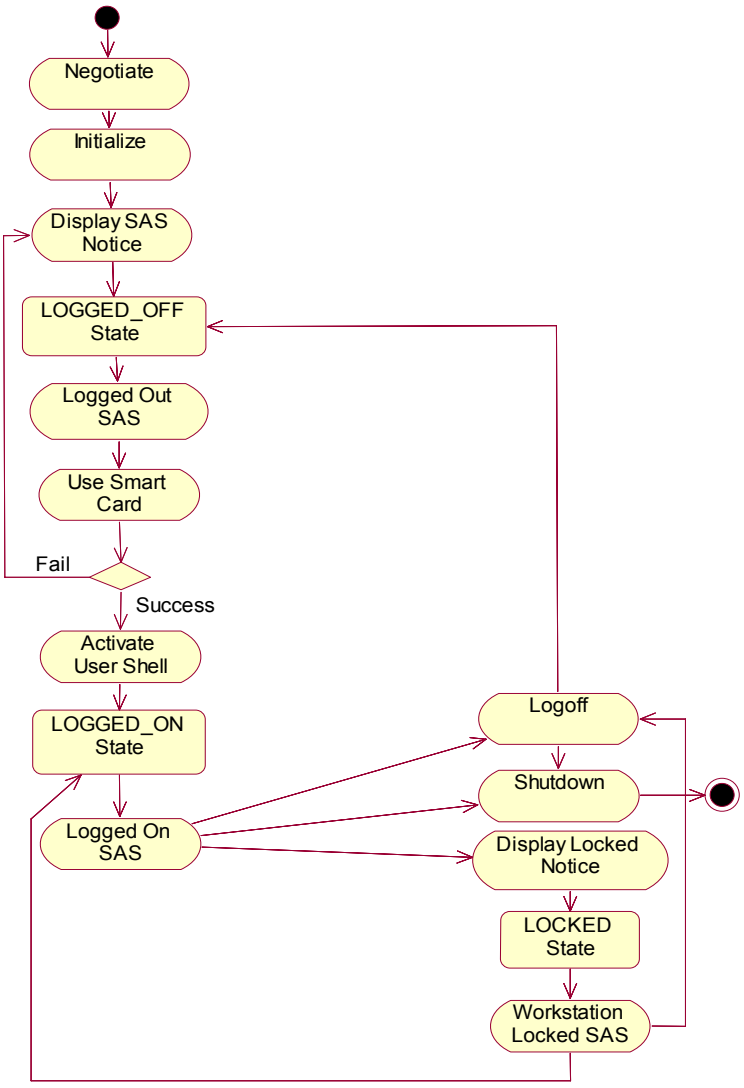
Autentikacioni paketi. Autentikacioni paketi na korisnikovom lokalnom računaru komuniciraju sa serverovim autentikacionim paketom radi autentikacije korisnika. *Windows* primenjuje podrazumevane autentikacione pakete za autentikaciju korisnika a takođe podržava prilagođene autentikacione pakete.

SAM. SAM čuva informacije o lokalnim nalozima korisnika u *Windows* redžistriju. Lozinke se šifruju upotrebom NTLM autentikacionog paketa. Rezultat šifrovanja je heširana lozinka transformisana u šifrovani tekst, niz brojeva i slova koji izgledaju besmisleno. Proces heširanja se obavlja primenom *hash* algoritma. NTLM koristi isti algoritam za šifrovanje i dešifrovanje.

AD. Informacije o nalozima korisnika na domenu su smeštene u AD na kontroleru domena. U okviru određenog domena, svaki kontroler domena ima identičnu kopiju AD domena.

4. IMPLEMENTACIJA VLASTITE GINA KOMPONENTE

Komponenta koju treba zameniti u procesu autentikacije je GINA (msgina.dll). U novoj GINA komponenti moraju biti implementirane sve funkcije podrazumevane GINA, kao i dodatne koje omogućuju komunikaciju sa *smart* karticom. Dijagramom aktivnosti na slici 3 prikazana je kompletna aktivnost nove GINA komponente u okviru autentikacije korisnika na Windows operativnim sistemima.



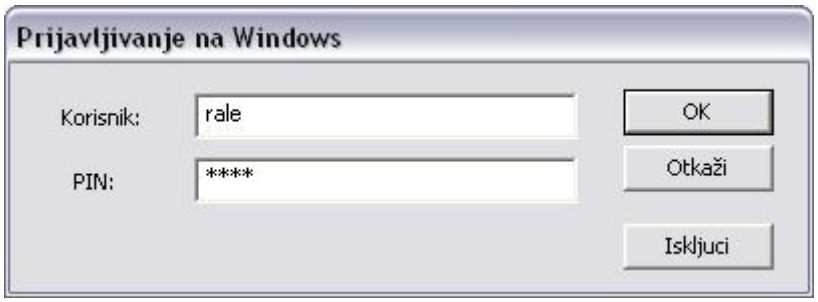
Slika 3: Dijagram aktivnosti u okviru GINA komponente

Kada se računar upali i kada se podigne operativni sistem, *Winlogon* učitava GINA komponenetu i poziva njenu funkciju WlxNegotiate kojom joj daje do znanja koliku funkcionalnost očekuje, a zatim poziva i funkciju WlxInitialize kojom saopštava koliku funkcionalnost od njega može da dobije GINA i u kom se stanju trenutno nalazi (LOGGED_OFF stanje). Posle inicijalizacije, pošto nijedan korisnik još nije prijavljen *Winlogon* poziva GINA funkciju WlxDisplaySASNotice, koja prikazuje prozor kao na slici 4 kojim se traži od korisnika da pritiskom na tastere CTRL+ALT+DELETE inicira proces prijavljivanja.



Slika 4: Inicijalni prozor

Kada korisnik pritisne potrebne tastere, *Winlogon* prestaje sa prikazivanjem prozora i poziva sledeću GINA funkciju, a to je WlxLoggedOutSAS. Ova funkcija prikazuje dijalog kao na slici 5 kojim se od korisnika zahteva da unese korisničko ime i PIN *smart* kartice.



Slika 5: Dijalog za pijavljivanje korisnika

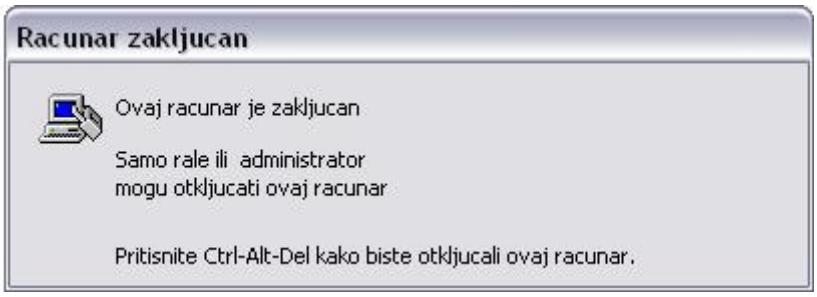
Pošto korisnik unese tražene podatke, WlxLoggedOutSAS poziva funkciju useSmartCard kojom na osnovu PIN-a pristupa *smart* kartici, čita korisničku šifru, a zatim je prosleđuje zajedno sa korisničkim imenom ka LSA pozivom funkcije LsaLogonUser kako bi se izvršila autentikacija korisnika. U slučaju neuspeha proces se ponavlja sa zahtevom da korinik ponovi postupak. Ukoliko je autentikacija korisnika uspešna *Winlogon* poziva funkciju WlxActivateUserShell. GINA sada aktivira korisnikovu ljusku (*shell*) a *Winlogon* prelazi u stanje LOGGED_ON. Ako korisnik pritisne tastere CTRL+ALT+DELETE inicira se SAS na šta *Winlogon* odgovara pozivom funkcije WlxLoggedOnSAS koja prikazuje dijalog kao na slici 6.



Slika 6: WlxLoggedOnSAS dijalog

Na osnovu izabrane opcije korisnika GIINA signalizira odgovor korisnika *Winlogon*-u, koji preduzima sledeće:

- ukoliko korisnik izabere opciju „Zakljucaj“, poziva GINA funkciju WlxDisplayLockedNotice koja prikazuje prozor kao na slici 7 i prelazi u stanje LOCKED čime je računar zaključan.
- ukoliko korisnik izabere opciju „Odjava“, poziva GINA funkciju WlxLogoff i vraća se u stanje LOGGED_OFF čime je korisnik odjavljen.
- ukoliko korisnik izabere opciju „Iskljuci“ računar se gasi.
- ukoliko korisnik izabere opciju „Task Manager“, pokreće Task Manager.
- ukoliko korisnik izabere opciju „Otkaži“, ostaje u istom stanju i korisnik nastavlja sa daljim radom.



Slika 7: WlxDisplayLockedNotice prozor

Implementacija je urađena u programskom jeziku C++ upotrebom *Microsoft Visual Studio .Net 2003* programskog paketa. U komunikaciji sa *smart* karticom korišćen je standard PKCS#11, standard koji kompanija RSA definiše za rad sa kriptografskim tokenima. Da bi *Windows* mogao da koristi novu GINA komponentu potrebno je da se naprave odgovarajuće izmene u *Windows* redžistriju. Naime potrebno je u liniji *\HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT \CurrentVersion\Winlogon* dodati ulaz pod nazivom *GinaDLL* i imenom dll fajla koji sadrži implemenaciju GINA komponente. Prednosti ovako realizovanog metoda autentikacije u odnosu na standardni metod autentikacije u *Windows* operativnim sistemima:

- lozinka je generisana na slučajan način
- lozinka spada u grupu „jakih“ lozinki
- korisnik ne zna lozinku
- korisnik pamti samo PIN *smart* kartice i korisničko ime
- lozinka se čuva u PIN kodom zaštićenom delu memorije *smart* kartice
- PIN može biti samo tri puta pogrešno unet
- korisnik mora da poseduje *smart* karticu sa adekvatnom lozinkom pri prijavljivanju na sistem.

5. ZAKLJUČAK

Ovakvom realizacijom GINA komponenete omogućena je upotreba *smart* kartica i kod operativnog sistema *Windows NT* 4.0 što ranije nije bio slučaj, kao i prijavljivanje korisnika upotrebom *smart* kartica ne samo na domenske naloge, već i naloge koji postoje samo na lokalnom računaru kod novijih *Windows* operativnih sistema [4]. Ovo rešenje ne zahteva izgradnju infrastrukture sa javnim ključem (*Public Key Infrastructure*), što znatno snižava njegovu cenu, tako da je ovo neka vrsta prelaznog rešenja koje u znatnoj meri povećava stepen bezbednosti u odnosu na tradicionalni metod autentikacije zasnovan na korisničkom imenu i šifri.

6. LITERATURA

1. Adolfo Rodriguez, John Gatrell, John Karas and Roland Peschke (2001), “TCP/IP Tutorial and Technical Overview”, IBM
2. Boško Rodić i Goran Đorđević (2004), “Da li ste sigurni da ste bezbedni”
3. Microsoft (2000), “Smart Card Logon”
4. W.Rankl and W.Effing (2002), “Smart Card Handbook”, John Wiley & Sons