

1	UVOD.....	2
1.1	Zašto pametne kartice ? .....	2
2	PROBLEM KOMPATIBILNOSTI.....	3
2.1	ISO 7816, EMV, i GSM.....	3
2.2	PC/SC Radna grupa .....	3
2.3	Windows-kompatibilni Logo Program.....	<b>Error! Bookmark not defined.</b>
3	KONCEPT PAMETNIH KARTICA NA WINDOWS PLATFORMI.....	<b>Error! Bookmark not defined.</b>
3.1	Davaoci usluga (Service Providers).....	<b>Error! Bookmark not defined.</b>
3.1.1	Kriptografski davaoci usluga (Cryptographic Service Providers)	<b>Error! Bookmark not defined.</b>
3.1.2	Davaoci usluga za pametne kartice (Smart Card Service Providers)	<b>Error! Bookmark not defined.</b>
3.2	Kartice.....	<b>Error! Bookmark not defined.</b>
3.3	Upravitelj Resursa (Resource Manager)...	<b>Error! Bookmark not defined.</b>
3.4	Upravljački programi za uređaje (Device Drivers)....	<b>Error! Bookmark not defined.</b>
3.4.1	Kitovi za razvoj upravljačkih programa (Device Driver Kits) .....	<b>Error! Bookmark not defined.</b>
3.5	Čitači (Readers).....	<b>Error! Bookmark not defined.</b>
4	POBOLJŠANA RJEŠENJA .....	<b>Error! Bookmark not defined.</b>
4.1	Autentikacija klijenta .....	<b>Error! Bookmark not defined.</b>
4.2	Interaktivna autentikacija mehanizmom javnih ključeva.	<b>Error! Bookmark not defined.</b>
4.3	Siguran e-mail.....	<b>Error! Bookmark not defined.</b>
5	PRIMJER SISTEMA TEMELJENOG NA TEHNOLOGIJI PAMETNIH KARTICA .....	<b>Error! Bookmark not defined.</b>
5.1	Arhitektura .....	<b>Error! Bookmark not defined.</b>
5.2	Rad sistema.....	<b>Error! Bookmark not defined.</b>
5.3	Zahtjevi .....	<b>Error! Bookmark not defined.</b>
5.4	Prikaz rada sa sistemom.....	<b>Error! Bookmark not defined.</b>
6	RAZVOJ APLIKACIJA .....	<b>Error! Bookmark not defined.</b>
6.1	Microsoftov pristup.....	<b>Error! Bookmark not defined.</b>
6.2	SDK .....	<b>Error! Bookmark not defined.</b>
6.3	API.....	<b>Error! Bookmark not defined.</b>
6.3.1	CryptoAPI.....	<b>Error! Bookmark not defined.</b>
6.3.2	SCard COM.....	<b>Error! Bookmark not defined.</b>
6.3.3	Win32 .....	<b>Error! Bookmark not defined.</b>
7	ZAKLJUČAK .....	<b>Error! Bookmark not defined.</b>
8	LITERATURA .....	<b>Error! Bookmark not defined.</b>

<http://www.maturskiradovi.net/>

## **1 UVOD**

U današnje vrijeme elektronski oblici plaćanja zamjenjuju zastarjele metode plaćanja «face to face» kao i one temeljene na klasičnom novčanom prometu. Zbog toga raste i potreba za sigurnošću i privatnošću. Sveukupnom globalizacijom kroz Internet i širenjem korporacijskih mreža koje uključuju pristup kako prodavačima tako i davateljima usluga izvan okruženja zaštićenih firewall-a potražnja za rješenjima temeljenim na javnim ključevima postaje sve hitnija.

### **1.1 Zašto pametne kartice ?**

U infrastrukturama javnih ključeva ključna komponentu predstavljaju pametne kartice. One poboljšavaju softverska rješenja kao što su npr. autentikacija klijenta, logiranje i sigurnost elektronske pošte (email-a). U suštini pametne kartice su tačka spajanja za certifikate koji su temeljeni na javnim ključevima i njima pridodane ključeve.

Razlozi tome su što:

- Pametne kartice pružaju zaštićeno skladište za privatne ključeve i druge oblike ličnih podataka
- Pružaju izolaciju sigurnosno kritičnim operacijama koje uključuju autentikaciju, digitalne potpise i razmjenu ključeva iz drugih dijelova sistema
- Pružaju prenosivost privatnih informacija između računara na poslu, kod kuće ili na putu.

Pametne kartice postaju dio Microsoftove Windows platforme. Uz cijenu od oko 20 USD po čitaču i maksimalnom iznosu od 5 USD po kartici, pametne kartice postaju jeftin način za pojačanje sigurnosti unutar firme. Čak i u slučajevima kada se kartice primjenjuju isključivo zbog npr. sigurnije autentikacije razloga u posao se unose sve druge prednosti koje pametne kartice pružaju. Te usluge uključuju funkcije plaćanja, pohranu povjerljivih informacija o korisniku (npr. medicinske informacije ili baze kontakata). Pametne kartice sve ovo pružaju bez potrebe za izmjenom postojeće infrastrukture. Pametna kartica se može prilagoditi svakom korisniku i dodatno

programirati sa više ključeva. Kartice mogu biti korištene za logiranje na PC ili na jednu pa i više mreža kako bi izvele udaljeno logiranje korisnika. Pohranom svih informacija o autentikaciji korisnika pametna kartica može postati pristupna tačka za sve korisnikove račune na lokalnoj mreži, Internetu ili unutar finansijskih institucija.

## **2 PROBLEM KOMPATIBILNOSTI**

Nekompatibilnost aplikacija, kartica i čitača je glavni razlog sporom usvajanju pametnih kartica izvan Europe. Stoga se više napora mora uložiti na poboljšanje kompatibilnosti između proizvoda različitih proizvođača što je preduslov za šire prihvaćanje tehnologije pametnih kartica od strane potrošača.

### **2.1 ISO 7816, EMV, i GSM**

Kako bi promovisali kompatibilnost među čitačima pametnih kartica, International Standards Organization (ISO) je razvila ISO 7816 standard za kontaktne kartice sa integrisanim krugovima. Ove specifikacije prvenstveno su orjentisane na kompatibilnost na fizičkom, električkom i nivou protokola podataka.

Godine 1996. Europay, Mastercard i Visa odnosno EMV definisali su industrijski specifičan standard koji usvaja ISO 7816 i definiše dodatne tipove podataka i pravila kodiranja za upotrebu u području finansijskih usluga.

Evropska telekomunikacijska industrija također usvaja ISO 7816 standard preko standarda za Global System for Mobile Communications (GSM) pametne kartice kako bi omogućili identifikaciju i autentikaciju za korisnike mobilnih telefona.

Iako su sve tri specifikacije (ISO 7816, EMV, and GSM) bile korak u pravom smjeru svaka od njih je bila ili preniskog nivoa ili prespecifična za određenu primjenu da bi dobila široku podršku industrije.

Pitanja kompatibilnosti na aplikacijskom nivou, kao što su Application Programming Interface-ovi (API) nezavisni o uređajima, alati za razvoj i djeljenje resursa nisu bila dotaknuta ovim specifikacijama.

### **2.2 PC/SC Radna grupa**

PC/SC (Personal Computer/Smart Card) radna grupa je formirana 1996 u partnerstvu sa velikim proizvođačima računarske opreme i firmama koje su razvijale pametne kartice: Group Bull, Hewlett-Packard, Microsoft, Schlumberger i Siemens Nixdorf. Osnovni cilj grupe je bio razriješiti pitanja kompatibilnosti. Godine 1997. Radna grupa je objavila prvu verziju specifikacija <http://www.smartcardsys.com/>

PC/SC specifikacije bazirane su na ISO 7816 standardu i kompatibilne su sa EMV i GSM specifikacijama. Postoji široka industrijska podrška ovim specifikacijama kako bi postale nezavisni standard. Od osnivanja i objave početnih specifikacija tom nastojanju pridružili su se i drugi proizvođači kao što su Gemplus, IBM, Sun Microsystems, Toshiba i Verifone.

**---- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE  
PREUZETI NA SAJTU [WWW.MATURSKI.NET](http://WWW.MATURSKI.NET) ----**

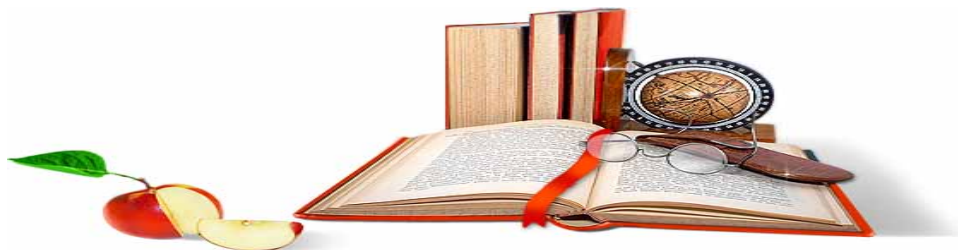
**[WWW.SEMINARSKIRAD.ORG](http://WWW.SEMINARSKIRAD.ORG)**

**RAZMENA LINKOVA - RAZMENA RADOVA**

**RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI MATERIJALI.**

**[WWW.MAGISTARSKI.COM](http://WWW.MAGISTARSKI.COM)**

**[WWW.MATURSKIRADOVI.NET](http://WWW.MATURSKIRADOVI.NET)**



NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO **[SEMINARSKI](#)**, **[DIPLOMSKI](#)** ILI **[MATURSKI](#)** RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NJEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE **[GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI](#)** KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U **[BAZI](#)** NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU **[IZRADA RADOVA](#)**. PITANJA I ODGOVORE MOŽETE DOBITI NA NAŠEM **[FORUMU](#)** ILI NA

**[maturskiradovi.net@gmail.com](mailto:maturskiradovi.net@gmail.com)**