



**VISOKA POSLOVNA ŠKOLA
STRUKOVNIH STUDIJA
ČAČAK**

MAGISTARSKI RAD

Elektronski studentski indeks

Mentor: _____
Profesor: _____

Student: _____
Br.Indeksa: _____

Mesto, mesec, godina

Elektronski studentski indeks

Xxxxx Xxxxx, Xxxx Xxxx, Fakultet za poslovnu informatiku, Univerzitet Singidunum

Sadržaj — U ovom radu analizirana je mogućnost realizacije studentskog indeksa na bazi smart kartica. Savremene smart kartice poseduju dovoljne memorijske resurse za prihvatanje podataka iz indeksa i podršku za realizaciju zaštitnih mehanizama, kojima se može čuvati integritet podataka na kartici. Puna funkcionalnost ovakvog indeksa može se ostvariti njegovom integracijom u informacioni sistem fakulteta. Prednosti primene predloženog rešenja su u automatizaciji svih aktivnosti oko studenata, od upisa do diplomiranja.

KLjučne reči — *digitalni sertifikati, digitalni potpis, kriptografija, PKI infrastruktura, smart kartice.*

I. UVOD

PRIHVATANJE bolonjske deklaracije na nivou univerziteta dovelo je do izmena u izvođenju nastave, kao i ukupnom funkcionisanju fakulteta. Jedna od najbitnijih izmena jeste zamena klasičnih indeksa, koji su se ranije koristili, novim. Pored indeksa svaki student po upisu na fakultet dobija i svoju ID (identifikacionu) karticu, u papirnatom obliku, koja služi kao jedinstveni identifikator studenta. Kartica na sebi sadrži:

- naziv visokoškolske ustanove,
- fotografiju studenta,
- ime i prezime studenta,
- datum rođenja studenta,
- datum isteka važenja kartice,
- broj indeksa,
- potpis,
- jedinstveni identifikacioni broj.

Ova kartica se trenutno koristi samo za identifikaciju studenata, ali bi njena primena mogla da bude znatno drugačija. U ovom radu se razmatra i predlaže primena elektronskih studentskih indeksa na bazi *smart* kartica. Uvođenjem *smart* kartica i njihovom integracijom u informacione sisteme fakulteta, postigla bi se puna funkcionalnost novih dokumenata. Ovo bi trebalo da bude kartica koja će u svojoj memoriji čuvati bitne podatke vezane za studenta, koji se trenutno nalaze u standardnom papirnom indeksu, kao što su na primer: ocene, podaci o školarini, podaci o overi semestra, potpisi koji su potrebni za overu semestra itd. Dalje, digitalni dokumenat bi se

koristio za automatsku identifikaciju prisutva studenata predavanjima i vežbama, pristup računarskim resursima, za prijavljivanje ispita, plaćanje školarine i sl. Podaci na kartici bi bili zaštićeni od neovlašćenih izmena.

Sve prednosti primene *smart* kartica danas su evidentne iz sistema elektronskog plaćanja, trgovine, bankarstva, državne uprave i sl.

II. PREDLOG NOVOG REŠENJA

Da bi se postigla puna funkcionalnost elektronskog indeksa on bi na sebi trebao da sadrži sledeće podatke:

- digitalni sertifikat univerziteta (root CA),
- digitalni sertifikac fakulteta (intermedium CA),
- fotografiju studenta (jpg),
- ime i prezime studenta,
- JMBG,
- datum isteka važenja kartice,
- broj indeksa (UID veza ka bazi),
- digitalni sertifikat studenta.
- dva tekstualna polja od po 255 karaktera (za rezervu, ukoliko su bude kasnije ispostavilo da je potrebno nešto kasnije ubaciti)

Uz ovakvu digitalnu studensku karticu neophodno je da postoji i server baze podataka koji služi za skladištenje podataka koji se ne nalaze na samoj kartici (ocene, overe semestra, školarine i sl.). Iz razloga bezbednosti instalirao bi se i *back up* server. To znači da podaci koji su se do sada nalazili na kartici ostaju i dalje na kartici, s tim što su podaci od interesa i u bazi podataka. Podaci, koji su se dosad nalazili u klasičnom papirnom indeksu prementili bi se u bazu podataka.

Postoji više pitanja u primeni smart kartica koje treba analizirati:

- Integritet podataka je od izuzetne važnosti za elektronski dokumenat. Kod postojećih, papirnatih dokumenata, ovaj problem nije razmatran, izuzev onemogućavanja fizičkog krivotvorenja same kartice. Osnovno pitanje je ko može da čita koje podatke, a još važnije od toga ko ima pravo da menja i upisuje podatke u indeks;
- Drugi pitanje odnosi se na izbor kartica. U ponudi se nalazi više tipova kartica (kontaktne, beskontaktne, memorijske, sa čipom, sa Microsoft podrškom ili Java, obične ili PKI itd.) i u startu je potrebno izabrati karticu potrebnu za ovakvu svrhu;
- Treće pitanje je na koji način omogućiti da spoljni korisnici veruju u verodostojnost

Igor Franc, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Danijelova 32 Beograd; telefon: 381-11-3093238; e-mail: ifranc@singidunum.ac.yu

Mladen Veinović, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Danijelova 32 Beograd; telefon: 381-11-3093227; e-mail: mveinovic@singidunum.ac.yu

podataka koji se nalaze na kartici (ovde je potrebno uspostaviti CA i odnos poverenja);

rezervu	
UKUPNO:	16578

III. IZBOR SMART KARTICA

Izbor *smart* kartica je od fundamentalne važnosti. Loš izbor bi mogao da ograniči punu funkcionalnost indeksa, a moguće je i da se dobije neperspektivno rešenje, tj. rešenje koje ne bi moglo da prihvati buduće povećane zahteve

Tip kartice (kontaktne(*contact*), beskontaktne (*contactless*) ili kombinovane (*dual interface*)) je veoma bitan, jer on može da ograniči ili dopusti realizaciju željenih funkcija. Poznato je da su zbog velikog broja kartica kontaktne kartice mnogo isplativije, ali se na taj način može izgubiti na funkcionalnosti. Sa druge strane, beskontaktne kartice su daleko fleksibilnije za upotrebu. Kod logovanja na računar neophodno je da kartica bude kontaktana. Ako se zahteva evidencija studenata kod ulaska u amfiteatar, kada je potrebno da se u kratkom vremenskom periodu prihvati veliki broj kartica, beskontaktne kartice bi bile idealne. Beskontaktne kartice omogućavaju i precizno lociranje studenata u zgradi. Nameće se zaključak da su za potrebe univerziteta idealne kombinovane kartice.

Sledeća bitna karakteristika je izbor kartica kompatibilnih sa JAVA ili sa Microsoft okruženjem. Sa stanovišta funkcionalnosti kartica na univerzitetu moguća je primena jedne ili druge platforme. JAVA kompatibilna kartica omogućava razvoj sopstvenog softvera. Ona na sebi ima *Java Virtual Machine* (JVM), koji omogućava izvršavanje raznih vrsta Java apleta. Na internetu postoji veliki broj *Open Source* softvera koji se može preuzeti i implementirati u slučaju JAVA kartica. U slučaju izbora Microsoft kompatibilne kartice dolazi do sveukupne zavisnosti od jednog proizvođača, ali je na raspolaganju niz alata za rad sa ovim karticama. Zbog pitanja bezbednosti podataka na kartici, udaljenog pristupa informacionom sistemu fakulteta i sl, ako se želi potpuna kontrola realizacije, prednost je na strani JAVA kartica.

Treća stvar odnosi se na zahteve za memorijskim resursima. Na tržištu su u opticaju kartice sa različitim memorijskim kapacitetima. Neophodno je što potpunije sagledati sve podatke koji bi se nalazili na kartici, jer se na *smart* karticama ne mogu vršiti povećanja memorijskih resursa. Prema proceni, za ove potrebe bi bilo dovoljno da kartica ima 32k raspoložive memorije, ali za buduće potrebe poželjno je koristiti kartice sa 64k. Ovo se može izračunati (proceniti) iz table 1

TABELA 3: PRORAČUN ZAUZEĆA MEMORIJE NA KARTICI

NAZIV POLJA	VELIČINA B
fotografiju (jpg 100*150 sa 72pix/inch)	10000
ime i prezime studenta,	30
JMBG,	13
datum isteka važenja kartice,	8
broj indeksa (UID veza ka bazi),	15
root CA + 1200 int. CA i 3600 digitalni sertifikat studenta,	6000
2 tekstualna polja od 255 karaktera za	512

Postoji više različitih proizvođača čipova za *smart* kartice, kao što su na primer: Philips, Siemens, Hitachi, SGS-Thomson itd. Ove čipove koriste svi proizvođači i integratori *smart* kartica kao što su: GemPlus, Cybermark Schlumberger itd. U sledećoj tabeli data je specifikacija čipova za *smart* kartice.

TABELA 2: ČIPOVI ZA SMART KARTICE.

Čip	P8WE5032	SLE 66CX160S	H8/ 3113
Proizvođač	Philips	Siemens	Hitachi
Izrada	0.35 μ m	0.6 μ m	0.5 μ m
CPU	80C51	8051	H8/300
ROM (bytes)	32K	31.5K	32K
EEPROM (bytes)	32K	16K	16K
RAM (bytes)	2.3K	2K	2.5K
Arithmetički Koprocesor	Yes	Yes	Yes
Random Number Gen	Yes	Yes	Yes

Kako se predviđa zaštita podataka od neautorizovanog pregledanja i menjanja podataka, neophodno je da se primene kartice koje na sebi već imaju ugrađenu podršku za *Public Key Infrastructure* (PKI). Tehnologija PKI omogućava sledeće: autentičnost (asimetrični sistem), integritet (asimetrični sistem), neporecivost (asimetrični sistem), zaštitu tajnosti podataka (simetrični sistemi). Pored ovoga dodaje se mogućnost digitalnog potpisa i digitalne envelope[3].

IV. KRIPTOGRAFSKA PODRŠKA

Problem integriteta podataka se rešava PKI tehnologijom i digitalnim sertifikatima. Kako na jednom univerzitetu postoji više fakulteta neophodno je uspostaviti hijerarhijski sistem poverenja, gde je root CA na univerzitetu. U slučaju univerziteta bilo bi neophodno uspostaviti kompletnu CA infrastrukturu koju bi činili sledeći elementi:

- root CA (CA kompletnog univerziteta)
- intermedium CA (CA svakog fakulteta pojedinačno)
- RA (Registration Authority), registraciono telo
- sistem za distribuciju sertifikata
- PKI aplikacije.

Na ovaj način bi svaki izdati sertifikat bio potpisan sa dva CA autoriteta koji bi garantovali njegovu verodostojnost. Prvi autoritet je CA fakulteta koji garantuje da je student upisan na fakultet, a drugi CA univerziteta koji bi garantovao da je dati student upisan na fakultet koji pripada datom univerzitetu [2].

RA bi u ovakvoj arhitekturi predstavljao registraciono telo koje bi proveravalo podatke vezane za zahteve za izdavanje digitalnog sertifikata i prosledivalo validne podatke CA koje bi izdavalo digitalni sertifikat.

Sistem za distribuciju sertifikata služi za distribuciju sertifikata do krajnjih korisnika, publikovanje izdatih digitalnih sertifikata kao i publikovanje liste povučenih sertifikata (CRL).

Potrebno je kreirati i određeni broj PKI aplikacija koje bi trebalo da omoguće kako rad sa samom karticom tako i zaštićen e-mail (korišćenjem SMIME) i siguran FTP (File Transport Protocol) tj. transfer podataka na siguran način. Takođe ovakav sistem bi morao da podrži i sledeće mogućnosti[3]: obnavljanje, povlačenje i suspenziju sertifikata.

Za obezbeđivanje tajnosti podataka na elektronskom indeksu mogu se koristiti komercijalno dostupni simetrični šifarski algoritmi, kao što su DES (Digital Encryption Standard), 3DES, AES (Advance Encryption Standard), IDEA ili neki drugi algoritam ove namene[1].

V. PREDNOSTI NOVOG REŠENJA

Prednosti koje bi donelo uvođenje digitalnih studentskih kartica su sledeće:

1. automatska overa semestra ako student ispunjava uslove (ako je sakupio dovoljan broj potpisa i izmirio školarinu)
2. automatsko kreiranje diplome ili uverenja (ako je student završio sve ispite i odbranio diplomski rad)
3. polaganje ispita bez ličnog prisustva studenta (ako je student upisao DLS tj. studiranje na daljinju)
4. lakše evidentiranje prisustva predavanjima/vežbama ili ispitima
5. mogućnost dodatne kontrole pristupa računarima u laboratorijama (student se najavljuje za rad na računaru putem smart kartice)
6. plaćanje usluga (fotokopiranje, štampa, uplata školarine i sl.) kao i dodatnih usluga.

Da bi se studentima omogućilo da se njihov digitalni indeks koristi i kao platna kartica (Debit Card) potrebno je sklopiti ugovor sa nekom od banaka, kako bi se omogućilo obavljanje različitih vrsta novčanih transakcija.

VI. STANJE U SVETU

Većina univerziteta u svetu uvodi ili je već uvela digitalne studentske kartice (Campus Card). Međutim, kod nekih se kartica koristi samo za identifikaciju prisustva, dok se za pristup računarskim resursima koriste korisničko ime i šifra.

Istorijat uvođenja digitalnih kartica na univerzitetima u SAD ilustrovana je sledećom tabelom[4]:

TABELA 3: ISTORIAT UVOĐENJA E-INDEKSA U SAD.

GODINA	NAZIV FAKULTETA/UNIVERZITETA
1972	California State Polytechnic University
1974	University of California - San Diego I Boston College
1977	University of Wisconsin - Stout, University of Kentucky, I SUNY Oneonta
1978	West Chester State Teachers College
1979	Cornell University
1980	Colorado State University
1981	California State University
1983	Brigham Young University Law School, University of

	Utah, University Of California - Los Angeles
1984	Cornell University
1985	University of Texas, Duke University, University Of Calgary
1986	Augustana College, South Dakota State University, John's Hopkins University
1987	Utica College, Laurentian University, Drake University
1988	Trinity College I Queens College
1990	Florida State University, Queens College, Loyola College of Maryland i Hamline University, Baylor University, The Pennsylvania State University
1993	Northwestern University, The University of South Florida, Florida State University, Western Kentucky University, University of Wisconsin La Crosse i Moravian College
1994	University of California, Georgia Military College
1995	Washington University, The University of Michigan, Western Michigan University, State University of New York, Florida Community College, Drew University
1996	University of Pennsylvania
1997	University Of North Carolina - Chapel Hill
1998	The University Of Delaware, Northeastern University, University Of Massachusetts at Amherst, The University of Missouri - Columbia, Stephens College
1999	Pepperdine University, University MealPass, University Of South Florida
2002	The University of Vermont, Saint Michael's College, The University of Houston
2004	Saint Michael's College i Champlain College

VII. AKTIVNOSTI ZA REALIZACIJU

Izabrati kombinovane (*dual interface*) procesorsko-memorijske kartice sa najmanje 32kb memorije i podrškom za RSA kao i PKI. Ispianirati koji će se podaci nalaziti skladišteni na samoj kartici a koji u bazi podataka. (poželjno je da kartica čuva minimum podataka koji su potrebni, a ostatak da se nalazi na serveru baze podataka). U sledećoj tabeli dat je predlog rasporeda podataka.

TABELA 4: PREDLOG RASPOREDA PODATAKA.

POLJE	CARD/BP
Kartica na sebi sadrži:	
digitalni sertifikat univerziteta (root CA)	CARD
digitalni sertifikac fakulteta (intermedium CA)	CARD
Fotografiju studenta (jpg)	CARD
ime i prezime studenta	CARD
JMBG	CARD
datum isteka važenja kartice	CARD
broj indeksa (UID veza ka bazi)	CARD
digitalni sertifikat studenta	CARD
Prva strana indeksa	
JMBG (lični broj)	BP
fotografija	BP
prezime, ime jednog roditelja, ime	BP
digitalni potpis studenta	BP
digitalni sertifikat univerziteta (root CA)	BP
digitalni sertifikac fakulteta (intermedium CA)	BP
datum rođenja	BP
opština rođenja	BP
država rođenja	BP
državljanstvo	BP
naziv upisanog studijskog programa	BP
stručni-akademski naziv	BP
datum upisa	BP
digitalni potpis ovlašćenog lica	BP
broj indeksa (UID veza ka podacima na kartici)	BP
Druga strana indeksa	
semestar	BP
školska godina	BP
naziv predmeta	BP
predavanja	BP
vežbe	BP

<i>seminari</i>	BP
<i>kolokvijumi</i>	BP
<i>ostalo</i>	BP
<i>ispit</i>	BP
broj časova	BP
ocenjivanje znanja	BP
poeni	BP
konačna ocena	BP
datum	BP
digitalni potpis nastavnika	BP
upis semestra	
upisao semestar	BP
školska godina	BP
status	BP
datum	BP
vreme	BP
digitalni potpis ovlašćenog lica	BP
overa semestra	
overio semestar	BP
školska godina	BP
datum	BP
digitalni potpis ovlašćenog lica	BP
podaci o seminarskim	
semestar	BP
školska godina	BP
predmet	BP
naslov	BP
ocena	BP
datum	BP
digitalni potpis nastavnika	BP
podaci o praksi studenta	
semestar	BP
školska godina	BP
ustanova gde se izvodi praksa	BP
područje prakse	BP
časovi rada	BP
predlog ocene i potpis mentora	BP
overa i ocena prakse	BP
dobrovoljni rad	
naziv projekta	BP
vrsta rada	BP
vrednovanje	BP
završni rad / disertacija	
naslov rada	BP
ECPB	BP
datum	BP
ocena	BP
tri člana komisije:	
<i>prvi član</i>	BP
<i>drugi član</i>	BP
<i>treći član</i>	BP
Ostali podaci o studentu	BP

Podeliti uloge, i dati ovlašćenja za unos i izmenu podataka u elektronskom indeksu. Na primer, ocene može da upisuje samo predmetni profesor, podatke o uplati školarine samo služba računovodstva a podatke o overi semestra samo nadležna studentska služba).

Instalirati pouzdan računar koji će biti server baze podataka na kome će se čuvati podaci o studentima koji se ne nalaze upisani na samoj kartici i kao rezervna kopija podataka u slučaju da student izgubi indeks).

Postaviti pri ulasku u svaki amfiteatar po jedan Card Reader.

Postaviti u zgradi fakulteta jedan ATM (Automatic Terminal Machine) terminal koji će biti direktno povezan sa bankom. (*debit card*)[7].

Na svim računarima u računskim učionicama ugraditi čitače kartica i zahtevati kao obavezan parametar pri

logovanju na računar da se digitalna kartica nalazi u čitaču.

VIII. EKSPLOATACIJA

Procedura izdavanja kartice. Kartica se izdaje svakom studentu odmah po upisu na fakultet ili eventualno posle prijave da je kartica izgubljena ili ukradena. U tom slučaju generiše se novi ključ za studenta a stari se proglašava nevažećim to jest ide na CRL (Certificate Revoke List).

Povlačenje kartice iz upotrebe. Kartica automatski ističe kad istekne datum koji je upisan na kartici. Moguće je i da se kartica samo privremeno povuče (na primer zbog zamrzavanja godine).

Zahtevi za uspostavljanje sistema digitalnih studentskih kartica. Da bi uspostavili efikasan sistem digitalnih studentskih kartica potrebni su sledeći elementi:

- CA server (MS Windows 2003)
- Server Baze podataka (MySQL/MS SQL)
- CARD Writer
- CARD Reader
- Aplikacije JAVA/VBS

IX. ZAKLJUČAK

Realizacijom elektronskog studentskog indeksa stvara se efikasan sistem koji olakšava funkcionisanje i poslovanje svakog fakulteta, kako za studente tako i za zaposlene koji rade na administrativnim poslovima. Savremene smart kartice poseduju resurse za prihvatanje velikih količina podataka i mehanizme za očuvanje tajnosti ovakvih podataka. Ovakve kartice su idealne za praćenje prisustva, kretanja na fakultetu i za prijavljivanje za rad u računarskim laboratorijama. U integrisanom informacionom sistemu fakulteta moguće je postići punu automatizaciju svih studentskih aktivnosti, od upisa do izdavanja diplome.

LITERATURA

- [1] A Menezes et al., "Handbook of Applied Cryptography", CRC Press, 1996..
- [2] B. Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996
- [3] S.Bosworth, M.E.Kabay, *Computer Security Handbook*, John Wiley & Sons, Inc., 2002
- [4] www.allcampuscard.com
- [5] www.ucalgary.ca/UofC/departments/RISK/security/id
- [6] www.campuscard.uwa.edu.au/UWA_Campus_Card
- [7] www.stanford.edu/services/campuscard/security.html
- [8] www.student.services.wiu.edu/ess/majorsystems/CSGOLD/index.asp
- [9] www.otiglobal.com
- [10] www.mtroval.ca/campuscard

ABSTRACT

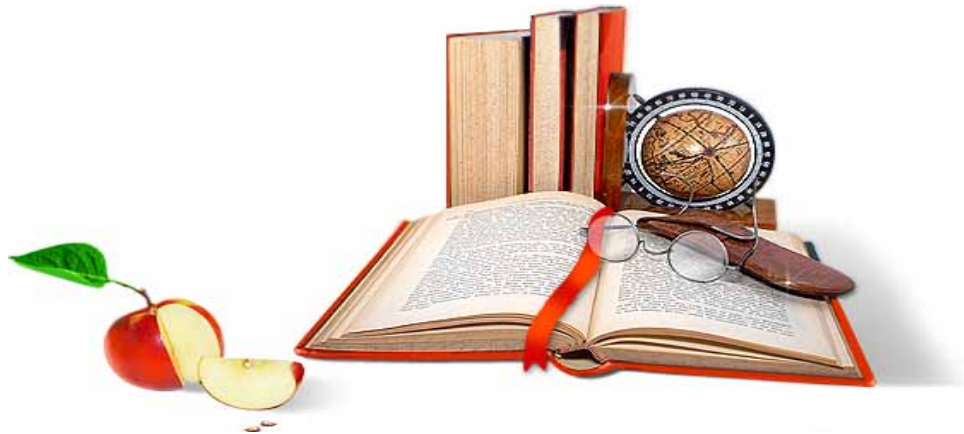
In this paper it has been analyzed possibility of realization student index on basis of smart card. Modern smart cards possess enough memories resource for getting data from indexes and support for realization protected mechanism, with which we can conserve integrity of data on card. Full functionality of such index can fulfil

with his integration in information sistem of faculty.The
main advantage of this solution are in automatization of
all activities about student, from enrollment to graduate.

ELECTRONIC CAMPUS CARD
Xxxx Xxxx Xxxxx Xxxxx

BESPLATNI GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RAD.

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



WWW.SEMINARSKIRAD.ORG

WWW.MATURSKIRADOVI.NET

WWW.MATURSKI.NET

WWW.SEMINARSKIRAD.INFO

WWW.MATURSKI.ORG

WWW.ESSAYSX.COM

WWW.FACEBOOK.COM/DIPLOMSKIRADOVI

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