Zaštita privatnosti korisnika pri primeni M-RFID servisa

Ana Lj. Milovanović

***Sadržaj* — U ovom radu predstavljen je osnovni princip rada RFID tehnologije i opisani su osnovni delovi RFID sistema. Prikazano je trenutno stanje RFID tržišta i dato je objašnjenje zašto se teži uvođenju RFID tehnologije u javnu mobilnu telekomunikacionu mrežu. Posebna pažnja posvećena je M-RFID servisu i prikazana su dva predloga zaštite privatnosti korisnika pri korišćenju proizvoda koji su obeleženi tagom. Izloženi su dosadašnji rezultati u procesu standardizacije ove tehnologije.**

***Ključne reči* — Bar code, EPC, mobilni telefon, M-RFID, RFID.**

I. UVOD

RADIO FREQUENCY IDENTIFICATION (RFID) predstavlja sistem za automatsko prikupljanje podataka koji omogućava prihvatanje i prenos podataka u okviru proizvodnih i poslovnih procesa, bežičnim putem, koristeći radio talase. Uvođenjem RFID tehnologije rešen je problem praćenja jedinstvenog proizvoda od njegovog nastanka do krajnjeg potrošača. Standardni *bar code* identifikuje samo proizvođača i proizvod ali ne i jedinstveni artikal. Za razliku od *bar code*-a, RFID tehnologija omogućava funkcionisanje sistema bez direktne optičke vidljivosti i po bilo kakvim vremenskim uslovima kao i istovremeno očitavanje više proizvoda [1].

U ovom radu prikazani su osnovni principi RFID tehnologije i njena primena, predstavljen je M-RFID *(Mobile RFID)* servis i postupak zaštite korisnika pri korišćenju proizvoda koji su obeleženi tagom.

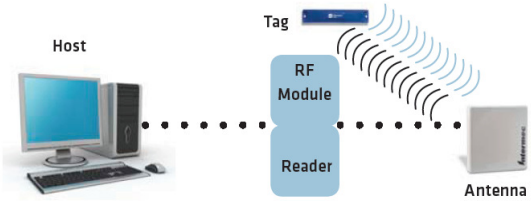
Rad je organizovan kroz sedam poglavlja. U poglavlju II opisani su osnovni principi RFID tehnologije i delovi RFID sistema. Primena RFID tehnologije kao i buduće oblasti primene M-RFID servisa opisane su u poglavlju III. Elementi M-RFID mreže, postupak kupovine proizvoda korišćenjem ove tehnologije kao i predlog dve metode za zaštitu privatnosti korisnika objašnjeni su u poglavljima IV i V. Šesto poglavlje posvećeno je standardizaciji RFID tehnologije, dok je zaključak dat u poglavlju VII.

II. RFID TEHNOLOGIJA

RFID sistem sastoji se od računara, RFID čitača, antene i transpondera-taga, kao što je prikazano na Sl.1. Antena se koristi za pojačavanje signala koji šalje čitač ka tagu i signala koji tag vraća čitaču, čime se povećava domet čitanja taga.

A. Lj. Milovanović, Republička agencija za telekomunikacije; (telefon:20-26-889; e-mail: ana.milovanovic@ratel.org.rs).

RFID čitač šalje signal na antenu u periodu od 50ms. Tada se generiše magnetno polje koje prihvata antena u tagu. Antena je podešena na istu frekvenciju kao i čitač. Primljena energija se smešta u mikro kondenzator u tagu. Kada se završi slanje signala, tag istog trenutka šalje podatke koji su smešteni u njegovoj memoriji. Ovi podaci se prihvataju na anteni čitača i dekodiraju se. Kada se pošalju svi podaci, kondenzator se prazni i resetuje da bi se tag pripremio za sledeći ciklus čitanja [2].



Sl. 1. Osnovni delovi RFID sistema.

A. *RFID tag*

RFID tag sastoji se od mikročipa, antene i opcionog izvora napajanja. Svaki RFID tag sadrži jedinstveni EPC podatak *(Electronic Product Code)*.

EPCglobalTM je udruženje formirano od strane UCC *(Uniform Code Council)* i EAN *(European Article Numbering)* organizacija. Ovo je glavno standardizaciono telo koje se bavi standardizacijom elektronskog koda proizvoda. EPC je otvoreni standard koji omogućava integraciju uređaja različitih proizvođača u jedinstveni sistem. Pored serijskog broja, struktura EPC podatka sadrži oznaku proizvođača kao i klasu proizvoda [3]. Ostale informacije o proizvodu nalaze se u bazama podataka i na serverima koji zajedno čine EPC mrežu.

Tagovi se proizvode u različitim oblicima, veličinama i sa različitim kapacitetima memorije. Postavljaju se na objekte, ambalažu, palete, kontejner ili na sam proizvod. Pored osnovnih podataka, u tagu mogu da se nalaze i instrukcije o daljim postupcima nakon identifikacije proizvoda. Prema vrsti napajanja koju koriste, tagovi se dele na: aktivne, polu-pasivne i pasivne [4].

B. *RFID čitač*

RFID čitač je fiksan ili prenosni uređaj koji može da aktivira i prikuplja signale koje odašilju tagovi. Sastoji se od napajanja, antene i štampane ploče. Naredbe definisane odgovarajućim softverom čitač prima od računara. Kada je sinal taga primljen i dekodiran, prema *Command Response* protokolu, čitač će na ponovljeno slanje signala odgovoriti tagu instrukcijom da prestane sa emitovanjem signala [2].

Ovaj protokol se koristi za rešavanje problema koji mogu da se jave kod čitanja brojnih tagova u kratkom vremenu.

RFID čitači razlikuju se po kompleksnosti, što zavisi od tipa taga sa kojim rade. Kao i tagovi, čitači se razlikuju po dometu koji ostvaruju. Pored navedenih postoje i čitači koji sadrže potenciometar za podešavanje dometa.

III. PRIMENA RFID TEHNOLOGIJE

RFID tehnologija trenutno se najviše primenjuje u transportu i logistici, proizvodnji i kontroli. Neki od primera su: praćenje proizvoda u lancu nabavke, praćenje kontejnera kao i delova koji se kreću kroz pogon u proizvodnom lancu, praćenje poštanskih pošiljki i prtljaga u avio-prevozu, naplata putarine i parkinga, kontrola pristupa vozilima, zaštita vrednih predmeta od krađe. Još neke od tipičnih aplikacija su: sigurnosna kontrola pristupa određenim lokacijama, E-pasoš, elektronska lična karta, obeležavanje životinja,... itd.

Ova tehnologija pobuđuje sve više pažnje, a predviđa se ogroman rast njene primene u narednih nekoliko godina. Velike kompanije na ovom polju prepoznaju ogromno tržište i pripremaju se za njega. Microsoft radi na softverskom delu koji bi trebalo da obezbedi integraciju ovih podataka sa bazama podataka i njihovu povezanost i transparentnost u lokalnim VPN *(Virtual Private Network)* mrežama. Oracle priprema ugradnju podrške za RFID sisteme u svoje baze podataka, IBM i SUN već imaju razvijen softver i infrastrukturu [5].

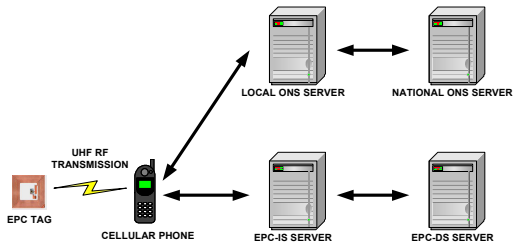
Jedan od najatraktivnijih servisa je svakako M-RFID koji preko javne mobilne telekomunikacione mreže omogućava očitavanje informacija sa proizvoda koji sadrže tag. Čitač je instaliran u mobilni telefon ili PDA *(Personal Digital Assistant)* uređaj. Ovo je sasvim novi pristup jer za razliku od dosadašnjih realizacija RFID tehnologije, tagovi su sada fiksirani dok je čitač pokretan. U budućnosti, kada RFID tagovi postanu dovoljno jeftini i kada se budu nalazili na svim proizvodima koji nas okružuju, korisnik će jednostavnim prinošenjem mobilnog telefona objektu sa tagom moći brzo i jednostavno da očita mnoge korisne informacije. Neki od mogućih servisa su: dobijanje informacije o lokaciji skeniranjem RFID označenog poštanskog znaka; dobijanje informacije o redu vožnje skeniranjem RFID označenog autobuskog znaka; informacije o cenama proizvoda kako u prodavnicama tako i u katalozima; preuzimanje filmova, muzike, rasporeda predstava, lokacije pozorišta i bioskopa skeniranjem RFID označenih filmskih plakata i CD-ova; uspostavljanje poziva ili slanje poruke nakon skeniranja RFID označene vizit karte [6].

IV. M-RFID SERVIS

U ovom radu, pod mobilnim RFID okruženjem podrazmeva se korišćenje RFID mobilnog uređaja u javnoj mobilnoj telekomunikacionoj mreži. Mobilni RFID uređaj tj. mobilni telefon ili PDA mora u sebi da sadrži mobilni RFID čitač koji je u saglasnosti sa EPCTM Class-1 Generation-2 UHF (860-960MHz) standardom [7]. Class-1 Generation-2 tagovi pretežno su namenjeni za obeležavanje proizvoda.

Na Sl. 2. prikazana je mobilna RFID mreža. RFID čitač pristupa podacima preko GSM, CDMA ili WCDMA telekomunikacione mreže.

EPC podatak predstavlja primarni identifikator svakog proizvoda. Ostatak podataka vezanih za proizvod smešteni su u bazama podataka i na serverima EPC mreže. Osnovne komponente mobilne RFID mreže su: RFID tag ugrađen u proizvod, RFID čitač ugrađen u mobilni telefon, lokalni ONS server *(Object Naming Service)*, nacionalni ONS server, EPC-IS server *(EPC-Information Services)* i EPC-DS server *(EPC-Discovery Services)* [8].

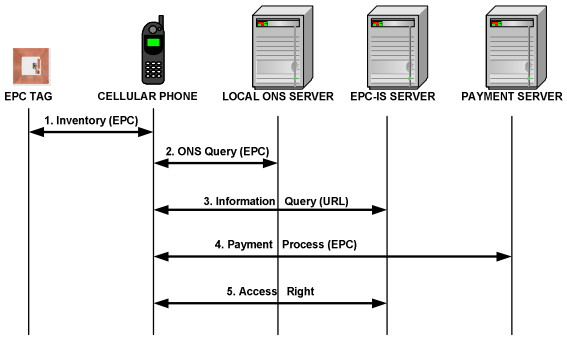


Sl. 2. Arhitektura mobilne RFID mreže.

ONS je globalni server iz koga se na osnovu EPC podatka dobija adresa na kojoj se nalaze željeni podaci na EPC-IS serveru.

EPC-IS je baza podataka koju formira proizvođač. EPC-IS pored EPC podataka sarži detaljan opis proizvoda kao i podatke o datumu proizvodnje, isporuke, transportu, ...itd.

EPC-DS je baza podataka u kojoj se nalazi celokupna istorija EPC taga tj. čuvaju se podaci o svakoj izvršenoj promeni.



Sl. 3. Procedura kupovine proizvoda u M-RFID mreži.

Mobilni RFID čitač preuzima EPC podatak sa proizvoda koji je obeležen tagom. Dalje, EPC podatak potrebno je prevesti u URI *(Uniform Resource Identifier)* (npr. IP adresu ili URL *(Uniform Resource Locator)*) koji će omogućiti pristup lokaciji na kojoj su smešteni konkretni podaci o proizvodu. ONS server daje informacije o odgovarajućem URI na osnovu dobijenog EPC podatka proizvoda. Pomoću dobijenog URI podatka moguće je pročitati konkretne podatke o proizvodu koji se nalaze na EPC-IS serveru. Na Sl. 3. prikazana je procedura kupovine proizvoda korišćenjem M-RFID mreže.

1. Mobilni telefon preuzima EPC podatak od proizvoda.
2. Mobilni telefon šalje EPC podatak ka lokalnom ONS serveru. Lokalni ONS server prevodi EPC podatak u odgovarajuću URL adresu na EPC-IS serveru.
3. Na osnovu dobijene URL adrese mobilni telefon

pristupa EPC-IS serveru i dobija informaciju o željenom prizvodu.

4. U slučaju da korisnik želi da kupi proizvod on zatim pristupa serveru preko koga se odvija procedura naplate proizvoda.
5. Nakon što je izvršena naplata proizvoda, EPC-IS server ili poništava tag prodatog proizvoda ili šalje korisniku šifru koja omogućava direktan pristup RFID tagu.

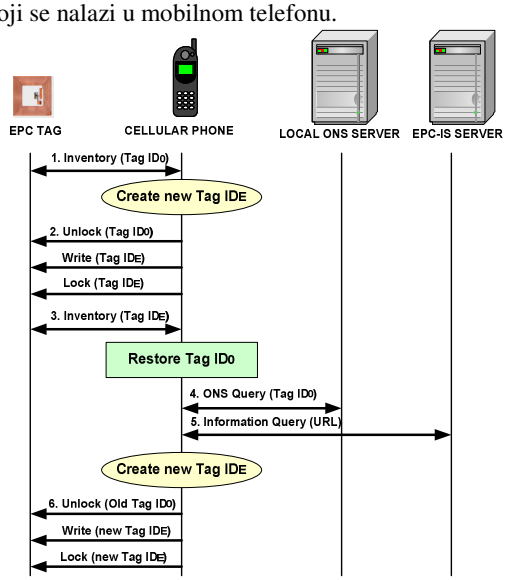
V. PRINCIP ZAŠTITE PRIVATNOSTI KORISNIKA

Jasno je da M-RFID servis može da donese veći stepen mobilnosti, automatizacije i efikasnosti, ali takođe postoji velika zabrinutost vezana za ugrožavanje privatnosti korisnika.

A. Zaštita privatnosti primenom mobilnog telefona

Pomoću mobilnog telefona sa ugrađenim RFID čitačem moguće je promeniti identifikator RFID taga kupljenog proizvoda tj. originalni EPC podatak. Veoma je važno da pri kupovini proizvoda korisnik u svom mobilnom telefonu sačuva šifru koju je dobio od EPC-IS servera, a koja omogućava direktan pristup RFID tagu [9].

Na Sl. 4. prikazan je jedan od načina na koji je moguće promeniti originalni identifikator taga (ID_0). Koristeći kriptografski algoritam, mobilni telefon formira privremeni identifikator taga (ID_E). Ulazne veličine za kriptografski algoritam su originalni idetifikator proizvoda i tajni ključ (K) koji se nalazi u mobilnom telefonu.



Sl. 4. Postupak sakrivanja originalnog identifikatora taga.

1. Mobilni telefon identifikuje originalni identifikator taga (ID_0).
2. Mobilni telefon kreira privremeni identifikator taga (ID_E).
3. Pomoću pristupne šifre, koja se nakon kupovine određenog proizvoda nalazi u mobilnom telefonu, mobilni telefon otključava EPC memoriju taga da bi promenio identifikator.
4. Mobilni telefon upisuje privremeni identifikator (ID_E) u EPC memoriju taga.
5. Mobilni telefon zaključava EPC memoriju taga koristeći pristupnu šifru čime je onemogućena zlonamerna upotreba EPC memorije taga.

Ako kasnije postoji potreba za preuzimanjem informacija sa ONS servera tj. sa EPC-IS servera, potrebno je pomoću iste šifre pristupiti EPC memoriji taga i vratiti originalni identifikator.

Predloženi metod sakrivanja originalnog identifikatora taga uspešno može da reši neke od problema ugrožavanja privatnosti kao što je praćenje proizvoda sa tagom tj. vlasnika takvog proizvoda. Novi tj. privremeno generisani identifikator taga nije registrovan ni u jednom ONS serveru kao ni u EPC-IS serveru tako da je praćenje proizvoda sa ovakvim tagom praktično nemoguće.

B. Zaštita privatnosti posredstvom mobilnog operatora

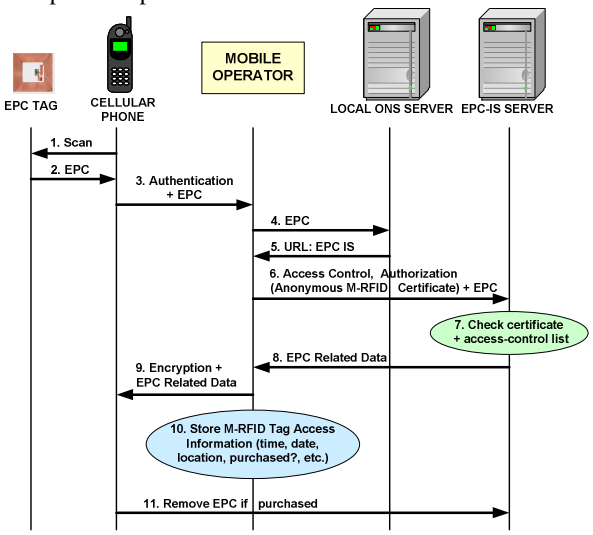
U prethodno izloženom predlogu za zaštitu privatnosti korisnika, mobilni telefon sa ugrađenim RFID čitačem komunicira sa ONS serverom i sa EPC-IS serverom. Takođe, on mora da prepozna originalnu EPC mrežu, da obavi celokupan prenos podataka i da pri tome sačuva privatnost korisnika. Svi ovi procesi previše su komplikovani da bi ih obavljao mobilni uređaj, a i rukovanje ovakvim uređajem bilo bi veoma otežano. Rešenje ovog problema je da pomenute poslove izvršava mobilni operator [10].

Na Sl. 5. prikazan je postupak zaštite privatnosti korisnika posredstvom mobilnog operatora.

1. Mobilni telefon „skenira“ RFID tag proizvoda.
2. Mobilni telefon preuzima EPC podatak od proizvoda.
3. Mobilni telefon šalje EPC podatak mobilnom operatoru. Postupak autorizacije na mobilnu mrežu obavlja se pomoću korisničke šifre.
4. Mobilni operator šalje EPC podatak prema ONS serveru.
5. ONS server vraća URL adresu na kojoj se u EPC-IS serveru nalaze željeni podaci.
6. Mobilni operator pomoću svoje baze podataka generiše lažni M-RFID dokument i šalje ga na URL adresu EPC-IS servera zajedno sa EPC podatkom. Lažni dokument ne sadrži identitet korisnika mobinog telefona ali može da sadrži informacije kao što su starost i pol korisnika, dokaze o pravu pristupa određenim informacijama,...itd.
7. EPC-IS server kontroliše dobijeni M-RFID dokument tj. proverava pravo pristupa određenim informacijama.
8. U zavisnosti od prava pristupa određenim informacijama, EPC-IS server šalje odgovarajuće informacije do mobilnog operatora.
9. Mobilni operator šalje dobijene informacije prema mobilnom korisniku.
10. Mobilni operator u svojoj bazi podataka čuva sve pojedinosti o obavljenom prenosu. Na ovoj način je korisniku omogućen jedostavan pregled podataka o proizvodima kojima je pristupio pomoću M-RFID

servisa. Takođe, čuvaju se datum i mesto kupovine proizvoda.

11. Ako korisnik odluči da kupi određeni proizvod postoji mogućnost da mobilni operator izvrši novčanu transakciju, a da korisnik račun za kupljeni proizvod dobije zajedno sa telefonskim računom. Kada se izvrši proces kupovine korišćenjem M-RFID servisa, mobni operator obezbeđuje da se svi detalji vezani za EPC podatak brišu iz EPC-IS servera. Na ovaj način onemogućeno je praćenje prodatih proizvoda.



Sl. 5. Postupak zaštite privatnosti korisnika posredstvom mobilnog operatora.

VI. STANDARDIZACIJA RFID TEHNOLOGIJE

RFID sistemi klasifikuju se u četiri frekvencijska opsega. Većina zemalja koristi 125kHz i 134kHz za sisteme niske frekvencije, 13.56MHz za sisteme visoke frekvencije, UHF opseg 868-956MHz, a poslednjih godina veoma je aktuelna primena RFID uređaja u opsegu od 2.4GHz. Kako svaka država upravlja svojim frekvencijskim spektrom postoje određene razlike u upotrebi UHF opsega. U Evropi se koristi opseg 865-868 MHz i 869.4-869.65 MHz. Pored razlika u korišćenim frekvencijskim opsezima postoje razlike i u ograničenju snage RFID uređaja [11].

Upotreba RFID uređaja kao i drugih uređaja male snage, u Evropi je regulisana ETSI standardima EN 300 330 , EN 300 440, EN 302 208, kao i CEPT preporukom ERC/REC 70-03. U Tabeli 1. prikazani su frekvencijski opsezi u kojima je dozvoljena upotreba RFID uređaja u našoj državi zajedno sa podacima o snazi tj. magnetnom polju i odgovarajućim ETSI standardom [12].

TABELA 1: FREKVENCIJSKI OPSEZI ZA RFID.

Frekvencijski opseg	***Snaga/Magnetno polje***	***ETSI standard***
13.553-13.567 MHz	42 dBμA/m na 10m	EN 300 330
865-868 MHz	100mW e.r.p.	EN 302 208
865.6-867.6 MHz	2W e.r.p.	EN 302 208
865-868 MHz	500mW e.r.p.	EN 302 208
2446-2454 MHz	500mW e.i.r.p.	EN 300 440
	4W e.i.r.p.	

Postoji sistem standardizacije ISO 15693 koji prestavlja standard za tagove i čitače koji rade na frekvenciji 13.56MHz kao i grupa standarda ISO/IEC 18000 u kojima su definisani svi parametri RFID uređaja u UHF opsegu [11].

ISO/IEC 29143 je prvi standard koji definiše parametre i upotrebu M-RFID čitača.

VII. ZAKLJUČAK

Razvoj RFID tehnologije kao i sve jeftinija proizvodnja opreme omogućili su nastanak mnogih novih servisa od kojih je svakako najatraktivniji M-RFID servis.

Postoji mnogo izazova u stvaranju sigurnog i poverljivog M-RFID rešenja. Izložena dva predloga za zaštitu privatnosti korisnika predstavljaju samo početak razumevanja problema ovog komplikovanog tehnološkog i društvenog pitanja.

LITERATURA

[1] Marcvan Lieshout, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, Claudio Borean, "RFID Technologies: Emerging Issues, Challenges and Policy Options", EuropeanCommision, Joint Research Centre, Institute for Prospective Technological Studies, 2007.

[2] Stephen B. Miles, Sanjay E. Sarma, John R. Williams, "RFID Technology and Applications" , Cambridge University Press, 2008.

[3] Mark Farragher, "Practical use of RFID", FirstFocus BV, 2004.

[4] Vince Pontani, "RFID Tags and Recycling RFID Technology Primer", USA, DoD Logistics AIT Office, 2004.

[5] Dora Karali, "Integration of RFID and Cellular Technologies", Wireless Internet for The Mobile Enterprise Consortium, UCLA-WINMEC-2004-205-RFID-M2M, 2004.

[6] Oliver Falke, Enrico Rukzio, Ulrich Dietz, Paul Holleis, Albrecht Schmidt, "Mobile Services for Near Field Communication", Technical Report, LMU-MI-2007-1, March 2007.

[7] Juan Carlos LópezCalvet, "The reole of RFID in the mobile phone", Telektronikk 3/4.2005., pp. 131-141, 2005.

[8] VeriSign, "The EPCglobal Network: Enhancing the Supply Chain", White Paper, Jun 2005.
Available:www.verisign.com/stellent/groups/public/documents/white_paper/002109.pdf

[9] Haedong Lee, Dooho Choi, Sokjoon Lee, Howon Kim, "A Study on RFID Privacy Nechanism using Mobile Phone", Proceedings of World Academy of Science, Engineering and Technology, vol. 10, Dec. 2005.

[10] Divyan M. Konidala, Kwangjo Kim, "Mobile RFID Security Issues", The 2006 Symposium on Cryptography and Information Security, Hiroshima, Japan, Jan. 2006.

[11] Christoph Seidler, "RFID – Opportunities for mobile telecommunication services", ITU-T Lighthouse Technical Paper, May 2005.

[12] "Pravilnik o vrstama radio-stanica za koje se ne izdaje dozvola za radio-stanicu", Službeni glasnik RS br. 26/07, 2007.

ABSTRACT

This paper presents basic working principles of RFID technology and describes basic parts of RFID system. It shows current state of RFID market and gives explanation for introduction of RFID technology into mobile telecommunication network. Special attention has been given to M-RFID service and two suggestion made for privacy protection while using tag. This presentation discloses results that were made in standardization of RFID technology process so far.

USER PRIVACY PROTECTION IN M-RFID SERVICE

Ana Lj. Milovanović