Pametna mobilna naprava z USB razširitvenim modulom kot plačilni terminal

Uroš Sadek[1,2], Bojan Kseneman[1,2], Peter Šamperl[1], Amor Chowdhury[1,2]

[1]*Margento R&D, Gosposvetska cesta 84, 2000 Maribor*

[2]*Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, Slovenija*

uros.sadek@margento.com , bojan.kseneman@margento.com

Transaction solution with smart mobile device with USB dongle extension as payment terminal

The paper presents the concept of a smart mobile device and an USB extension (dongle) as NFC and VOICE transaction solutions. USB dongle supports voice and contactless interfaces to identify customers, while the smart mobile device, running Andorid OS in our prototype solution, manages backend communication channel and user specific application with front-end (GUI).

Such solution is used by Margento service Urbana, and is intended, as mobile payment terminal, to support payment method with Uniform City card Urbana.

1 Uvod

Tendenca na področju plačevanja se giblje v smeri uporabniku prijaznih storitev v smislu enostavnosti, prenosljivosti, zanesljivosti in varnosti. V podjetju Margento R&D d.o.o smo se zato odločili, izdelati razširitveni modul za pametne mobilne naprave, ki se bo uporabljal v okviru projekta Urbana [2]. V prototipni izdelavi smo kot pametno mobilno napravo uporabili Android tablico.

Z uporabo zunanjega modula smo dodali dodatni nivo na področju varnosti sistema. S tem smo se izognili potrebi, da mobilna naprava vsebuje NFC varnostni modul kakor tudi dejstvo, da NFC ni standardiziran in je delovanje le-tega različno pri različnih proizvajalcih. Mobilna naprava bo tako imela vlogo validacijskega terminala.

Članek opisuje sestavni del aplikacije (knjižnico), ki je zadolžena za komunikacijo z razširitvenim modulom ter podatkovnim centrom in omogoča preostalem delu aplikacije zahteve o stanju kartice ter zahtevo za pričetek transakcije. Opisan je tudi razširitven modul.

2 Koncept transakcijskega sistema

Sistem za plačevanje preko pametne mobilne naprave, (tablica, telefon na Slika 1: Tablica z razširitvenim USB modulom) obsega pametno mobilno napravo ter USB razširitveni modul (RM). Slednji omogoča identifikacijo uporabnika preko brezžičnega vmesnika z Urbana kartico, ter preko zvočne komunikacije med razširitvenim modulom in mobilnim telefonom stranke.

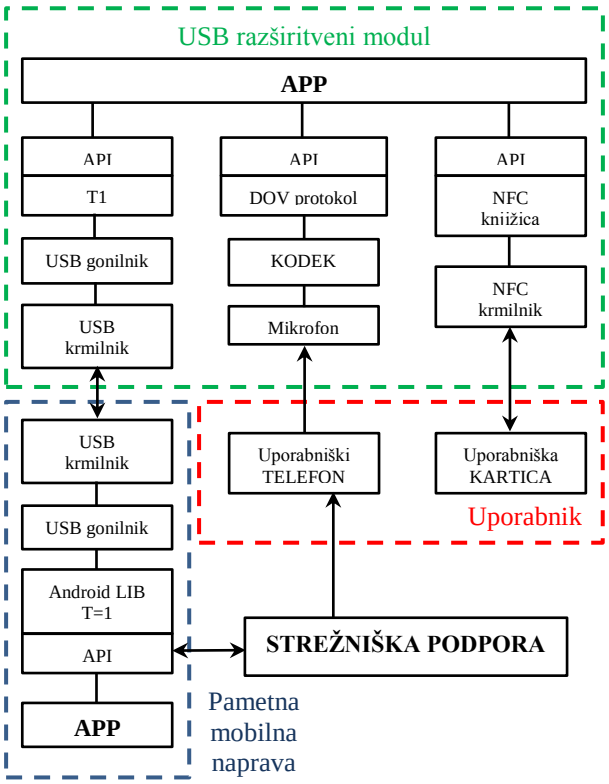
Medsebojno delovanje posameznih naprav poteka v »master-slave« načinu, pri čemer je pametna mobilna naprava »master«, RM pa »slave«. Tako je tudi konfigurirana medsebojna USB komunikacija kjer je konfigurirana mobilna naprava kot 'gostitelj' (host), RM pa kot 'naprava' (device).

Pametna mobilna naprava poganja API (Aplication Interface), ki povezuje RM in plačilno aplikacijo, katera je specifična za uporabnika plačilnega sistema. API mobilne naprave prav tako omogoča vzpostavitev kanala s strežniško podporo (backend-om) ter RM in je tako posrednik izmenjave informacij. S tem se izognemo GPRS modulu na RM. Povezava API-ja mobilne naprave in RM poteka preko modificiranega T=1 protokola.

API za komunikacijo z backend-om se nahaja na RM, ki opravlja servisne transakcije, posodabljanje funkcionalnosti in parametrov, pridobitev črnih list kartic, »batch« transakcije itd. Celotno zgradbo sistema in povezavo med API-ji prikazuje Slika 2.

RM je zasnovan v kompaktni majhni obliki in se vključi direktno v mikro USB vmesnik mobilne naprave. Ker so vse mobilne naprave prešle na standardizirano polnjenje preko mikro USB vmesnika, ki je v času uporabe RM zaseden, vsebuje RM dodatni mikro USB vmesnik. Slednji omogoča polnjenje mobilne naprave v času medsebojnega delovanja z RM.

Slika 1: Tablica z razširitvenim USB modulom



Slika 2: Blokovna shema sistema

2.1 USB komunikacija

USB komunikacija je zelo razširjena in univerzalna serijska komunikacija, prisotna na vsaki pametni mobilni napravi. Zato jo je smiselno izrabiti za prenos podatkov med mobilno napravo in RM.

V našem primeru smo uporabili USB v CDC (Comunications Device Class) načinu, ki se pogosto uporablja v vgrajenih sistemih ter različnih razširitvenih napravah za mobilne naprave.

2.2 API (Aplication interface)

API oziroma aplikacijski vmesnik, povezuje aplikacijo (APP) z različnimi moduli ali zunanjimi vmesniki. Kot na primer API ki povezuje aplikacijo RM za procesiranje transakcij z NFC vmesnikom. Na pametni mobilni napravi povezuje API aplikacijo in RM, ter tudi RM in strežnik v ozadju.

3 USB razširitveni modul

Glavni funkcionalnosti razširitvenega modula sta NFC vmesnik, ki omogoča plačevanje z uporabo brezkontaktne Urbana kartice, ter enosmerni DOV (Data Over Voice) vmesnik, ki omogoča identifikacijo plačnika preko mobilnega telefona s klicem na strežnik v ozadju.

3.1 NFC (Near Field Communication)

NFC je komunikacijska tehnologija srednjega frekvenčnega pasu, ki omogoča izmenjavo podatkov brezkontaktno, na razdalji do 10 cm. Tehnologija temelji na standardu ISO/IEC 14443 ki omogoča komunikacijo med dvema napravama, ali napravo in kartico.

3.2 DOV (Data Over Voice)

Data Over Voice, krajše DOV, temelji na frekvenčni modulaciji FSK (Frequency-shift keying) za prenos digitalnega signala v obliki zvoka. V oddajni napravi se izvede frekvenčna modulacija digitalnega signala, kjer se moduliran signal generira preko zvočnika, ter se sprejme na sprejemni napravi preko mikrofona. Na sprejemni napravi se digitalna informacija izlušči s postopkom demodulacije.

Na razširitvenem modulu se uporablja enosmerna DOV komunikacija, preko katere lahko prenašamo podatke le iz mobilne naprave stranke na terminal. Kar zadovoljuje zahtevam identifikacije stranke.

3.3 Kodiranje podatkov

V skladu z zaščito pred zlorabami, morajo biti zakodirani vsi podatki, ki se prenašajo med napravami.

Prenos podatkov med brezkontaktno Urbana kartico in razširitvenim modulom je, po standardu ISO/IEC 14443, zakodiran z 2KTDES, 3KTDES ali AES128 kodirnim algoritmom, pri čemer se za komunikacijo med kartico in razširitvenim modulom uporablja 3KTDES kodiranje.

Pri DOV komunikaciji med mobilno napravo stranke in razširitvenim modulom, se uporablja EEC (Eliptic Curve Cryptography) kodirni algoritem, ki temelji na asimetričnem kodiranju podatkov z uporabo javnega in zasebnega ključa.

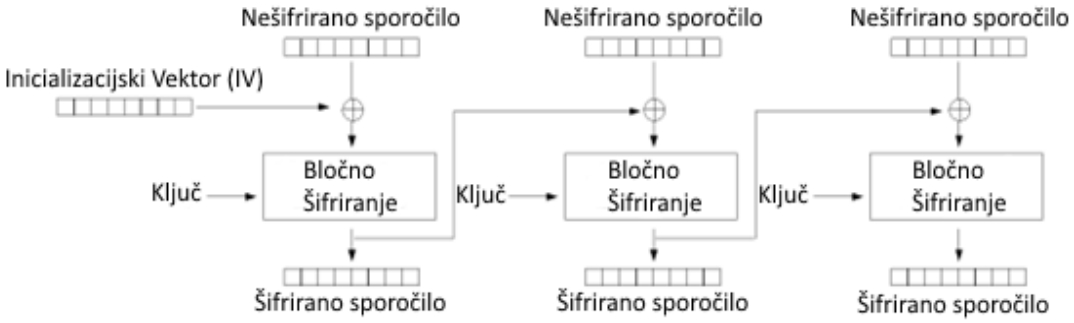
Prav tako so zakodirani podatki ki se prenašajo med razširitvenim modulom ter pametno napravo preko USB vmesnika. Prenos teh podatkov poteka po modificiranem T=1 protokolu, ki temelji na ISO/IEC 7816-3 standardu.

Ključi, ki se uporabljajo za različne kriptografske algoritme so shranjeni na notranjem pomnilniku mikroprocesorja, ki je prav tako zaščiten pred branjem in pisanjem.

3.4 Oddaljeno posodabljanje aplikacije

Aplikacija razširitvenega modula, podpira funkcionalnost oddaljenega posodabljanja aplikacije [1], kot tudi njenih parametrov. Pri oddaljenem posodabljanju se celotna nova aplikacija prenese preko IP povezave in se shrani na notranji FLASH pomnilnik. Ko je prenos aplikacije končan ter uspešno preverjen podpis aplikacije, se trenutno delujoča aplikacija posodobi z preneseno aplikacijo, ki se zažene ob ponovnem zagonu modula.

Uvedba oddaljenega posodabljanja prinese dve glavni prednosti. Terminali so posodobljeni veliko hitreje ob drastično zmanjšanih stroških, ter omogoča enostavno spreminjanje posameznih parametrov in manjše prilagajanje sistema v smislu večje učinkovitosti.



Slika 3: 3K3DES diagram

4 Android API

4.1 Operacijski sistem Android

Operacijski sistem Android spada v skupino odprtokodnih sistemov, ki temeljijo na Linux jedru in je predvsem namenjen uporabi na pametnih telefonih in tabličnih računalnikih. Njegovo sestavo lahko razdelimo na štiri osnovne dele kot to prikazuje Slika 4.

Slika 4: Zgradba operacijskega sistema [3]

Glavna prednost operacijskega sistema glede na ostale je odprtost platforme za razvijalce strojne in programske opreme. To prav gotovo razveseli uporabnike, saj imajo pestro izbiro pri nakupu naprave ter imajo na voljo ogromno brezplačnih aplikacij.

4.2 Komunikacija med razširitvenim modulom in Androidom

Komunikacija med razširitvenim modulom in Android napravo temelji na USB logičnimi kanali oz. cevmi (angl. logical channel, pipe), ki jih definira specifikacija USB OTG [5]. Ta specifikacija omogoča prenosnim napravam, kot so telefoni in tablice, da delujejo v načinu USB gostitelja. Cev med gostiteljem (Android naprava) in logično entiteto (razširitveni modul) imenujemo končna točka. Končna točka je zmeraj enosmerni tip komunikacije, zato jih imamo več.

V našem primeru imamo tri, prva je namenjena pošiljanju podatkov, druga prejemanju in tretja za pošiljanje nizkonivojskih kontrolnih signalov s pomočjo katerih npr. izvedemo ponastavitev (reset) razširitvenega modula.

Nad tem je uporabljen nekoliko prilagojen T=1 protokol [4], ki je standardiziran pod oznako ISO/IEC 7816-3. T=1 protokol je blokovno, gospodar-služabnik (angl. master-slave) orientiran tip komunikacije. Njegov okvir ponazarja Tabela 1: T=1 Okvir. T=1 protokol je izdelan tako, da omogoča avtonomno zaznavanje in odpravljanje napak med prenosom. To zagotavlja dejstvo, da gospodar in služabnik beležita sekvenco (znotraj PCB) lastnih poslanih in prejetih sporočil. V primeru neujemanja sekvenc se zahteva ponovni prenos podatkov. Poleg sekvenc je v uporabi tudi 16-bitni CRC (angl. Cyclic redundancy check) - CCITT, katerega naloga je zagotavljanje integritete sporočil.
T=1 protokol opisuje tri tipe blokov in sicer:

- Informacijski blok ***I***,
- prejemnik pripravljen blok ***R***,
- in nadzorni ***S*** blok.

Nadzorni blok (angl. Supervisory block) se uporablja za izmenjavo kontrolnih informacij med napravama kot npr. usklajevanje sekvenc gospodarja in služabnika. Tega moramo poslati vselej, ko pričnemo z komunikacijo.
Informacijski blok (angl. information block) je uporabljen za prenos podatkov med napravama. Protokol definira, da lahko v posameznem sporočilu prenesemo največ do 254 bajtov podatkov. V primeru da želimo prenesti več podatkov, moramo to sporočilo razdeliti ne več delov, kjer pride do veriženja podatkov.

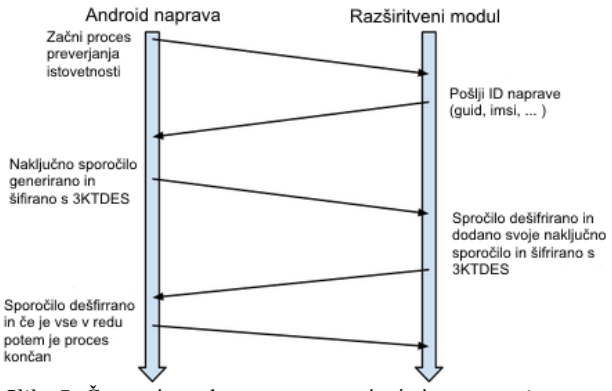
Uvodno polje (obvezeno)			Informacijsko polje(opcijsko)	Zaključno polje (obvezno)
NAD (1 bajt)	PCB (1 bajt)	LEN (1 bajt)	INF (0 do 254 bajtov)	CRC16 (2 bajta)

Tabela 1: T=1 Okvir

Prejemnik pripravljen blok (angl. receiver ready block) se uporablja za pozitivno ali negativno potrditev podatkov. Ta se pošilja v primeru potrditve prejema verižnega sporočila ali v primeru napake npr. neujemanje sekvence, CRC, prejeti napačni blok, itd.

Za varovanje podatkov na komunikacijskem kanalu je uporabljeno 3KTDES [5] (angl. Three Keys Triple Data Encryption) šifriranje v CBC načinu (angl. Cipher Block Chaining). 3K3DES šifriranje je bločno šifriranje, kar pomeni, da šifriramo skupek podatkov v obliki bloka. Velikost posameznega bloka je lahko med 8 in 64 bajti. Vsako sporočilo, ki presega to velikost moramo razdeliti na več blokov. V CBC načinu se nad vsakim blokom vrši bitna operacija XOR s prejšnjim šifriranim blokom, preden se le ta šifriranje. Na ta način je določen blok odvisen od vseh predhodnikov, zato moramo na

začetku uporabiti določen inicializacijski vektor. Grafičen potek procesa šifriranja prikazuje Slika 3. Ključ seje se določi ob začetku komunikacije, v procesu preverjanja istovetnosti (angl. authentication) naprav. Ker gre za komunikacijo tipa gospodar-služabnik, mora proces preverjanja istovetnosti pričeti Android naprava, ki generira naključno skrivno sporočilo dolžine 12 bajtov in ga šifrira s 3KTDES in ga pošlje razširitvenemu modulu. Ta ga dešifrira, obrne (angl. reverse) ter doda svoje naključno sporočilo dolžine 12 bajtov. Vse skupaj nato modul šifrira s 3KTDES in šifrirano sporočilo pošlje nazaj gospodarju. Če lahko gospodar dešifrira sporočilo in če je prvih 12 bajtov po rotaciji enakih poslanim, potem je proces preverjanja istovetnosti uspešen. Gospodar nato novi, skupen ključ seje, pošlje služabniku kot potrdilo uspešnosti procesa preverjanja istovetnosti. Časovni potek procesa je predstavljen na Slika 5.



Slika 5: Časovni potek procesa preverjanja istovetnosti naprav

4.3 Komunikacija med Android napravo in strežnikom

Razširitveni modul sam po sebi ni sposoben komunicirati s strežnikom, kamor se beležijo podatki transakcij in od koder dobimo posodobitve aplikacije razširitvenega modula, zato Android naprava predstavlja vmesni člen med njima. Le ta je sposobna s podatkovnim centrom odpreti varen SSL komunikacijski kanal (angl. socket) preko katere s strežnikom z namenskim protokolom izmenjujeta podatke. Ti podatki se nato z razširitvenim modulom izmenjujejo s pomočjo T=1 protokola.

4.4 Funkcionalnost Android knjižice

Knjižica mora zagotavljati T=1 komunikacijo z razširitvenim modulom ter zagotavljati komunikacijo s strežniško podporo. Prav tako omogoča enostavne klice s strani uporabniškega vmesnika (ločen modul v aplikaciji) za zahtevo transakcije ter informacijo o stanju na kartici.

5 Zaključek

USB razširitveni modul je funkcionalno dodelan produkt, ki bo pripomogel k enostavnejšemu ter varnejšemu načinu plačevanja. Produkt ima širok spekter uporabe in povpraševanja saj je celoten sistem (Android tablica ter RM) cenovno ugoden.

Mobilna aplikacija deluje po pričakovanjih in izpolnjuje zastavljene cilje, vendar je tu treba omeniti veliko ranljivost sistema Android. Aplikacije na sistemu Android je mogoče razvijati v programskem jeziku Java katere glavni problem predstavlja dejstvo, da je možno do razvojne kode priti na zelo enostaven način s procesom povratnega prevajanja (angl. to decompile). Zaradi tega smo se odločili, da bomo uporabili JNI (Java Native Interface) [6]. Ta predstavlja programsko ogrodje, ki Javi omogoča klice funkcij, ki so napisani v drugih programskih jezikih (C, C++, assembler) in obratno. Uporabili smo programski jezik C++, ki poleg dejstva, da je kodo težje povratno prevesti, dodaja še hitrejše in v smislu časovnega izvajanja, natančneje delovanje.

6 Literatura

[1] A. Zajc, A. Koštomaj, Z. Mezgec, A. Chowdhury. *Postopki oddaljenega posodabljanja mobilnih plačilnih terminalov*. *ERK 2008*, Portorož, Slovenija, september, zv. A, str. 145-148.

[2] M. Fras, J. Svečko, A. Chowdhury. *Integralni mestni plačilni sistem (Urbana) in Ljubljanska turistična kartica Urbana. ERK 2010*, Portorož, Slovenija, september, zv. A, str. 354-357.

[3] B. Kseneman, D. Igrec, A. Chowdhury. *Mobilna aplikacija za upravljanje z električnimi porabniki v sistemu pametnih vtičnic. ERK 2012*, Portorož, Slovenija, september, zv. A, str. 323-326

[4] julij 2014, ISO/IEC 7816-3 http://read.pudn.com/downloads132/doc/comm/563504/ISO-IEC%207816/ISO%2BIEC%207816-3-2006.pdf

[5] julij 2014, USB OTG http://en.wikipedia.org/wiki/Triple_DES

[6] julij 2014, JNI http://en.wikipedia.org/wiki/Java_Native_Interface