

# Logit: W1 Report

Malik Koljenović; **06.02.2017**

**Faza:** Dizajn i planiranje

Izrađen je prototip arhitekture sistema za sigurno bilježenje prisustva bazirano na Android NFC platformi uz korištenje NFC kartica kao alternativnog rješenja, te formulisan okvirni plan izrade kao teme za naredni konsultacijski sastanak.

## Zaključci

1. Projekat je podijeljen u tri međuzavisne faze
2. Kao obavezna implementirati će se prva faza projekta
3. Implementacija druge i treće faze projekta zavisna je od vremenskih ograničenja
4. Za prototip sistema u *fazi I* određene su sljedeće komponente:
  - a. Registracija korisnika: verifikacija identiteta i generisanje sigurnog elementa
  - b. Loger: Android aplikacija koja bilježi interakciju (i.e. prisustvo)
5. Aplikacija bilježenja prisustva izrađuje se u svrhu pokazne aplikacije za funkcionalnosti sigurnosnog sistema
6. Odbacuje se raniji prijedlog korištenja QR kodova kao alternativnog rješenja za korisnike koji ne posjeduju Android uređaj sa NFC mogućnostima, umjesto toga predloženo je korištenje NFC smart kartica
7. Rok za implementaciju prototipa faze I je W12 2017
8. Pisani rad u okviru master teze treba pored sistema i dokumentacije uključivati i analizu rizika sistema (kartice, SMI i čitači/aplikacija), te elaboraciju namjene SMI modula

## Faze

1. **SMI modul i Android aplikacija za bilježenje prisustva**
2. **Podrška za fizičke NFC smart kartice (NTAG21x ili DESFire)**
3. **PKI infrastruktura i namjenski HW čitači i**

## Moduli (F1)

1. **SMI (Secure Module Interface)**
  - a. API server na odvojenoj hardverskoj platformi
  - b. obavlja sigurnosno osjetljive operacije
  - c. pohranjuje sigurnosno osjetljive podatke

- d. generiše sigurni element za korisnika
- e. vrši interakciju sa udaljenim korisničkim direktorijem
- f. implementira registraciju i verifikaciju korisnika

## 2. Logger

- a. Android aplikacija za bilježenje NFC interakcija
- b. inicijalizira proces registracije korisnika
- c. održava identitet i sigurni element korisnika
- d. master mod vrši interakciju sa SMI modulom preko API-ja
- e. slave mod radi na principu HCE (*en. Host-Based Card Emulation*)

## Clijevi

1. Ponuditi sigurno i jednostavno okruženje za zadovoljenje korisničkih zahtjeva
2. Minimizirati korisničku interakciju sa sistemom
3. Izgraditi proširivu platformu za sistem sigurne interakcije sa korisnicima
4. Ponuditi jednostavniju i povoljniju alternativu za sigurnu interakciju baziranu na pametnim karticama od zatvorenih komercijalnih rješenja korištenjem dislokacije uloge sigurnog okruženja sa kartice na namjenski SMI modul (*dislocation of concerns?*), ovim se efektivno izuzetno komplikovana JavaCard ili komercijalna aplikacija na kartici zamjenjuje programom visokog nivoa na SMI modulu, a interakcija sa karticom RESTful API implementacijom