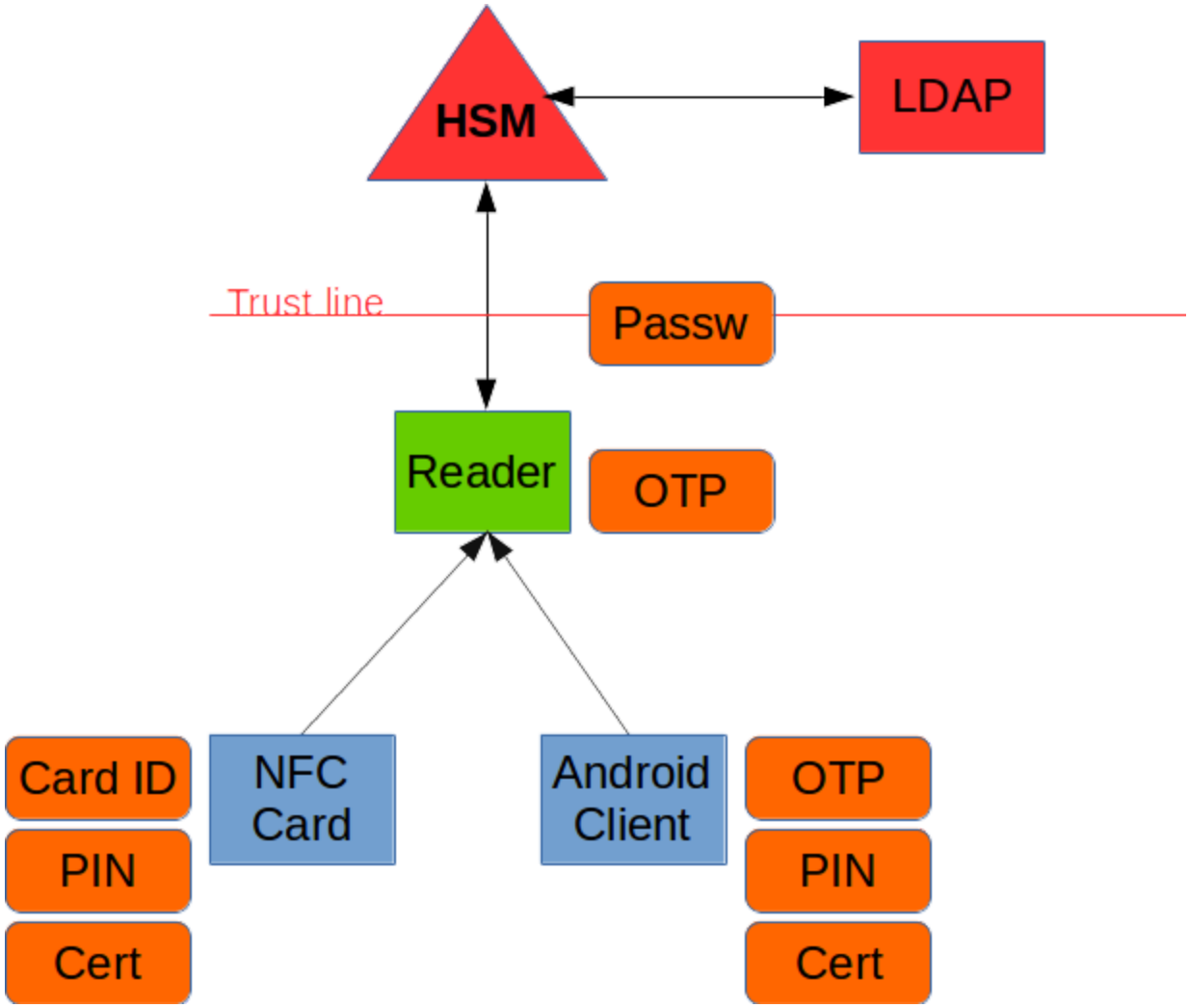
Logit: W2 Report

Malik Koljenović; **19.03.2017**
Faza: Dizajn arhitekture



Sliak 1: Šema logičke arhitekture sistema

Sistem prikazan na slici 1 predstavlja dekompoziciju zatvorenog sistema pametnih kartica sa funkcionalnostima kriptografije javnog ključa i njegovo preslikavanje na distribuirani sistem iste namjene u otvorenom mrežnom okruženju. Osnova sigurnosti sistema pametne kartice zasniva se na nemogućnosti izdvajanja tajne komponente ključa izvan zatvorenog sistema pametne

kartice i sa dodatnom sigurnosnom mjerom tajnog PIN broja predstavlja jednu sigurnosnu cjelinu u okviru sistema dvofaktorne autentifikacije. Ovakva tradicionalna autentifikacijska rješenja sa podrškom za kriptografiju javnog ključa iako široko korištena i dokazana u praksi imaju ozbiljne probleme tehničke i ekonomske prirode. Tehnički problemi ovakvih rješenja ogledaju se u zatvorenosti i fragmentiranosti platforme svakog od proizvođača (Oracle, Gemalto, Infineon etc), kompleksnom interfejsu za programiranje aplikacija i pored postojanja otvorenog operativnog sistema (JavaCard) za pametne kartice, te ograničenim performansama samog čipa. Svi ovi faktori rezultiraju vrlo visokom cijenom koštanja integracije (50-150 KM po korisniku).

Zbog navedenih ograničenja tradicionalnih sistema predložena je izrada sistema ekvivalentnih ili boljih sigurnosnih osobina uz zadržavanje postojećih funkcionalnosti, uz dodatnu mogućnost korištenja generičkih NFC tagova ili bilo kojeg drugog memorijskog uređaja koji se može jedinstveno identificirati na siguran način (***e.g. Android telefon***). U okviru predloženog sistema kao osnovna premisa sigurnosti postavlja se kriptografski zaštićen paket (***Cert***) generisan na lokaciji od povjerenja (***HSM***) koji pored osnovnih informacija o korisniku i njegovog javnog ključa sadrži i njegov privatni ključ, enkriptovan master ključem HSM-a, takav zaštićeni paket može biti dostupan i zlonamjernom korisniku, no beskoristan je bez HSM master ključa, a za njegovu autoriziranu upotrebu neophodno je osigurati dodatne autentifikacijske mehanizme u zavisnosti od potrebnog nivoa zaštite (***PIN, OTP, Card ID, Password, Čitač***). Osobine predloženog sistema nam omogućavaju da ga u poređenju sa sistemom pametne kartice također smatramo zatvorenim sistemom, u smislu da enkripcija osigurava da nekriptovan tajni ključ nikada ne napušta zatvoreni kriptosistem u čijem se središtu nalazi HSM kao element od povjerenja, stoga možemo uspostaviti jasnu paralela sa zatvorenim sistemom pametne kartice. Da bi postigli ekvivalenciju sa sistemom pametne kartice neophodno je još osigurati i element posjedovanja, koji se u slučaju predloženog sistema zamjenjuje sa od strane proizvođača potpisanim jedinstvenim ID brojem NFC taga (***Card ID***, *za NFC tagove*) i jedinstvenim OTP kodom (*za Android uređaje*).

Predloženi sistem biti će realiziran korištenjem HTTPS komunikacijskih kanala sa REST API implementacijom, naknadno je moguće izvršiti potpunu integraciju sa tradicionalnim sistemima korištenjem PKCS#15 emulacije i implementacijom PKCS#11 na HSM strani.

TBC ...