UNIVERSITATEA TITU MAIORESCU

FACULTATEA: INFORMATICĂ
DEPARTAMENT: INFORMATICĂ
Programa de studii: INFORMATICĂ
DISCIPLINA: INTELIGENȚĂ ARTIFICIALĂ

IA – *Testul de evaluare nr.* 17

Mecanisme și Politici de Securitate

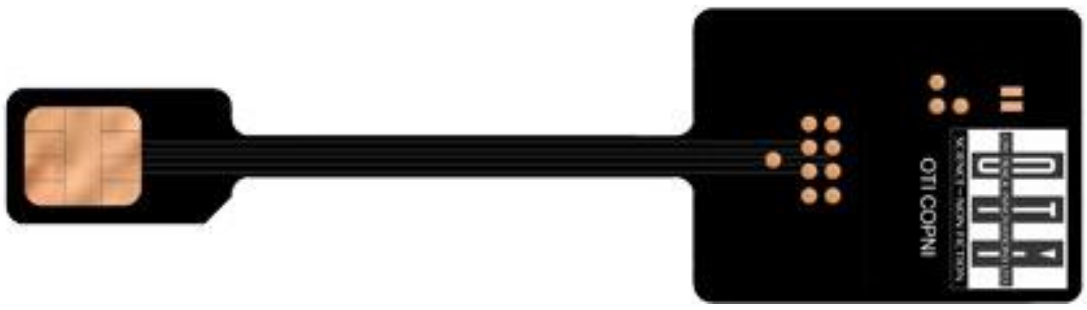
Grupa	Numele și prenumele	Semnătură student	Notă evaluare

Data: ____/____/_____

CS-I dr.ing.
Lucian Ștefăniță GRIGORE

Conf.dr.ing.
Iustin PRIESCU

Ș.L.dr.ing.
Dan-Laurențiu GRECU



Cuprins

1. INTRODUCERE

Dezvoltarea infrastructurii de telecomunicație, precum rețelele de telefonie și Internet, a fost întâmpinată în societate printr-o adopție pe scară largă a terminalelor mobile ce folosesc această infrastructură. Cel mai important aspect al acestor schimbări tehnologice fundamentale îl reprezintă posibilitatea oricărui individ de a purta asupra lui un dispozitiv electronic cu funcționalitatea și performanța unui calculator personal, prin care poate rămâne conectat la lumea digitală după bunul plac. Deși inițial aceste capabilități au fost privite cu neîncredere și conservatorism de o parte a populației, beneficiile și oportunitățile conferite de tehnologia informației și telecomunicații au fost recunoscute în scurt timp și constituie acum o preocupare de bază în rândul agenților economici, autorităților publice, dar și cetățenilor.

Unul din șocurile pozitive aplicate de către rețeaua de Internet economiei mondiale l-a constituit facilitatea de a efectua plăți online. Trebuie menționate în acest context modele de business online consacrate, precum Amazon, eBay sau Paypal, care au știut sa exploateze apetența consumatorului pentru dublul confort garantat de utilizarea cărților de plăți (credit/debit) în locul banilor lichizi, în conjuncție cu dezvoltarea unui sistem sigur de plăți online, ce permit ca datele personale de plată să fie transmise de clienți și acceptate de comercianți în condiții de maximă siguranță. Acest model economic a fost deja integrat în operațiile desfășurate de bănci și de rețelele de carduri (VISA, Mastercard etc), definind un criteriu de relevanță a piețelor financiare.

Portofelul digital este următorul nivel întrezărit în dezvoltarea modelelor de plăți online. Conform acestui concept, rolul portofelului clasic, în care stocăm bani lichizi, carduri și alte artefacte de plată, va fi luat de un dispozitiv mobil precum prea-popularul smartphone. Pentru a atinge acest stadiu, a fost nevoie ca telefoanele smart să fie echipate cu tehnologia necesară de a se substitui cardurilor de plăți, astfel încât să nu fie nevoie de înlocuirea întregii infrastructuri de plată existente în momentul de față la comercianți și bănci.

Astfel, un smartphone folosit pe post de portofel de digital trebuie să poată comunica printr-un protocol de unde radio cu terminalele de plată (POS), dar trebuie să fie prevăzut și cu tehnologia necesară pentru a emula funcționalitatea unui (sau mai multor) card de plată, ceea ce presupune stocarea și vehicularea în condiții de maximă securitate a informațiilor confidențiale de plată ale utilizatorului autorizat.

Tehnologia ce permite comunicarea unui telefon mobil cu un terminal de plată (sau cu un alt telefon mobil) se numește NFC (Near-Field Communication). NFC constă într-un transmițător de date pe bază de unde radio, ce poate iniția transmisii de date contactless (fără a fi nevoie de contact) cu alte dispozitive capabile de NFC la o distanță de câțiva centimetri. Majoritatea producătorilor de smartphone și de tablete au început să integreze în dispozitivele lor circuite NFC.

Elementul securizat este complementar transmițătorului NFC, întrucât reprezintă un mediu securizat de stocare a datelor confidențiale și de execuție a aplicațiilor de plăți. Elementul securizat este o combinație dintre un circuit integrat, un sistem de operare și aplicații software, concept cunoscut drept „sistem pe cip” (system-on-chip). Putem face analogia următoare: elementul securizat este calculatorul propriu-zis, pe când transmițătorul NFC reprezintă modemul sau placa de rețea ce îi permite primului să comunice cu exteriorul.

Deși există o suită de soluții tehnice disponibile pe piață ca elemente securizate, dezvoltarea sistemelor de plăți pe această platformă a rămas până acum în apanajul celor care controlează circuitul financiar, producătorilor de telefoane mobile sau rețelelor de telefonie mobilă, datorită unor limitări tehnologice impuse artificial de birocrația digitală a sistemelor de criptare și comunicații. Rolul acestui raport tehnic este să prezintă opțiunile pe care le au dezvoltatorii independenți de aplicații de plăți, din punct de vedere al elementelor securizate.

2. ELEMENTUL SECURIZAT (SE)

Un element securizat (SE) este un sistem de calcul specializat inviolabil sub formă de circuit integrat (cip) care este utilizat într-un dispozitiv electronic (smartphone, card bancar, acte de identitate, cartele acces) pentru a oferi un mediu sigur de stocare a informațiilor confidențiale (date, aplicații) necesare pentru a sprijini diverse modele de afaceri.

SE pot exista în mai multe forme (factori de formă), inclusiv UICC (SIM), embedded SE și smart microSD. Arhitectura SE prevede memorie separată pentru fiecare aplicație, pentru a elimina interacțiunile dintre ele.

Cipurile SE se împart în două categorii:

- *Detașabile* (eng. removable): smart card de tip UICC sau microSD;
- *Înglobate* (eng. embedded): embedded Secure Element (eSE).

2.1 Caracteristici principale

Portabilitate: Dacă înlocuim dispozitivul ce conține SE, aplicațiile utilizatorului ar trebui să fie portabile și pe noul dispozitiv. Această continuitate în servicii reprezintă o provocare pentru embedded SE în particular, pentru ca SE detașabile pot fi pur și simplu scoase din vechiul aparat și instalate în celălalt.

Securitate: Pentru a-și merita titulatura, SE trebuie să conțină funcționalități cât mai avansate de menținere a securității datelor și aplicațiilor. De exemplu, criptarea datelor ne asigură că nu sunt interceptate pe parcursul transmisiei lor printr-un canal oarecare de comunicație. SE sunt prevăzute și cu mecanisme de a stopa execuția unor aplicații ce pot compromite datele private (exemplu, date de plată) stocate.

Multi-aplicație: Arhitectura SE permite acestora să stocheze mai multe aplicații, provenind de la diferiți furnizori de servicii (bănci, lanțuri de magazine, companii de transport etc). Fiecare aplicație beneficiază de propriul ei spațiu pe SE, ceea ce permite separarea și izolarea strictă a informației critice, după sursă și scop.

Remote management: Programele software și datele ce populează SE trebuie să poată fi modificate de la distanță, de fiecare dată când este necesar.

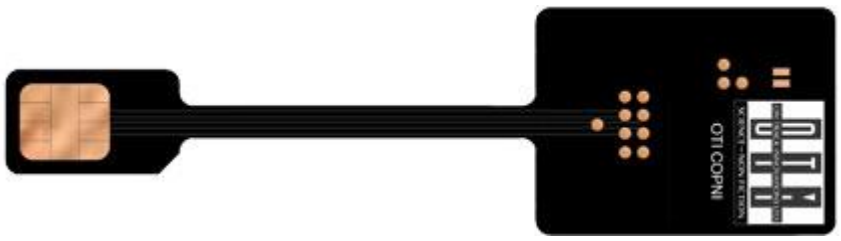


Figura 1: Element securizat (stânga) și transmițător NFC atașat (dreapta)

2.2 Elementul Securizat ca Smart card

Istoricul elementelor securizate se confundă în mare măsură cu cel al smart cardurilor, deoarece fac parte din această clasă de produse, singura diferență fiind că prezintă sisteme de securitate suplimentare.

Termenul de „smart card” este folosit pentru a descrie o cartelă (card) de plastic cu un microprocesor înglobat și o memorie destul de mare care să poată stoca programe software dezvoltate de compania care a emis cardul. Structura fizică a unui smart card este specificată prin standarde internaționale: cartela de plastic trebuie să aibă dimensiunile 85.60mm x 53.98mm x 0.80mm și trebuie să se poată îndoi într-o bună măsură fără să sufere daune. Un circuit imprimat și un cip cu circuit integrat (microcontroler) sunt înglobate pe card. Întrucât siliciul nu rezistă bine la îndoiri, cipul

trebuie să fie mic în comparație cu suprafața cartelei. Circuitul imprimat este o plăcuță aurită subțire care oferă contactele electrice cu exteriorul și protejează cipul de stres mecanic și electrostatic.

Majoritatea cardurilor cu cip sunt construite din straturi (sau substraturi) produse din materiale diferite, care împreună dau cardului un anumit ciclu de viață și funcționalitate. În ziua de azi, cardurile sunt făcute din PVC, poliester sau policarbonați. Mai întâi sunt tipărite straturile cardului și laminate la presă. Următorul pas este golirea și ștanțarea, iar apoi înglobarea cipului și adăugarea datelor pe card. Fabricarea unui card se poate petrece în aproximativ 30 de pași, prin utilizarea a până la 12 articole diferite, de la materialele brute până la software. Rezultatul este un pachet unitar care se prezintă utilizatorului drept un simplu dispozitiv electronic.

Pentru a servi scopului urmărit, un smart card trebuie să conțină memorie și procesor de calcul. Unele dintre ele conțin doar memorie, dar la acestea nu ne putem referi drept „smart” și nu fac obiectul acestui studiu.

Datorită formei și dimensiunii, cardurile smart nu au o sursă de putere internă, deși au nevoie de energie electrică pentru a opera. De aceea, ele operează doar în prezența unui Dispozitiv de Acceptare a Cardurilor (CAD) care furnizează alimentarea necesară. Majoritatea cardurilor smart intră în contact fizic cu CAD, pe când altele nu, dar ambele categorii au practic aceeași arhitectură internă și nu pot fi tratate separat.

O caracteristică fundamentală a cardurilor smart este limbajul în care sunt programate. Similar cu evoluția calculatoarelor personale, există o schimbare de paradigmă de la programarea smart card în limbaj de asamblare la limbaje de nivel înalt, precum Java.

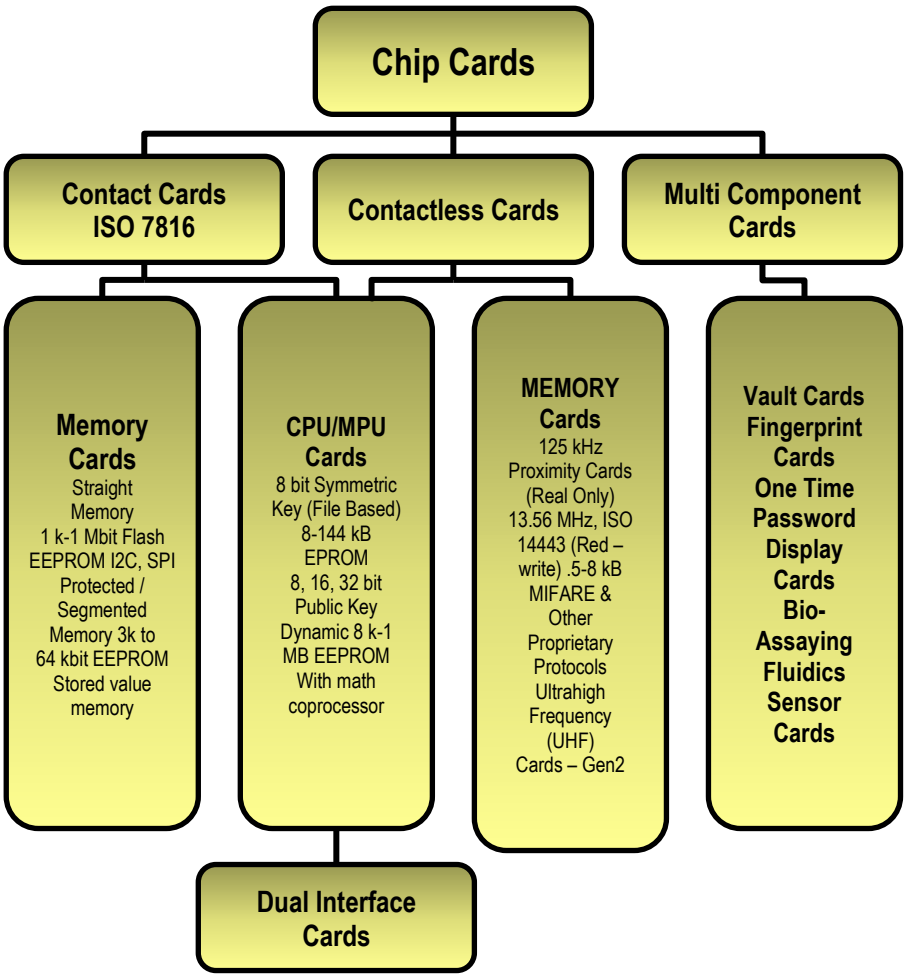


Figura 2: Clasificarea elementelor securizat ca sisteme pe cip

Primul dispozitiv care a prevestit apariția smartcard poate fi consemnat încă din 1974, când jurnalistul francez Roland Moreno a prezentat un potențial sistem de plăți inovativ, sub forma unui

dispozitiv electronic ce putea să stocheze date (cu caracter financiar), atașat unui inel la purtător. În același an au apărut primele astfel de carduri, denumite „epoxy”, dar forma lor nu era plană. De altfel, în zilele noastre producătorii din industria smart card au revenit la această idee pentru a dezvolta ceea se cheamă Java Ring.

În 1975, compania franceză CII-Honeywell-Bull produce primul card în formatul curent al cardurilor de credit, cu cip și contacte electrice pe o parte. Primele comenzi de la clienți au fost livrate doi ani mai târziu.

Marea varietate de smart carduri din care putem alege poate fi clasificată în funcție de:

- modalitatea în care se citesc sau scrie datele;
- tipul sistemului pe cip utilizat pe card și capabilitățile sale.

Elementul securizat poate fi oricare dintre aceste tipuri, atâta timp cât alegem un smart card care este prevăzut cu toate măsurile de securitate impuse de aplicație. De asemenea, este imperios necesar să analizăm factorul de formă pe care trebuie să îl îmbrace elementul securizat, dintre cele detaliate într-una din secțiunile următoare.

2.2.1 Carduri de Contact

Sunt cele mai populare tip de smart card. Au contacte electrice pe exterior cu care se pot conecta la un cititorul de carduri în care sunt introduse. Conectorul este atașat de un cip încapsulat pe card. Aceste carduri costă mai mult odată cu puterea de procesarea, memoria și flexibilitatea, dar costurile tehnologice reprezintă doar 15% din total. Restul reprezintă cheltuielile cu infrastructura, emiterea, programarea și dezvoltarea resurselor umane.

2.2.2 Carduri cu multiprocesor CPU/MPU

Denotă cardurile care au capabilități de procesare dinamică a datelor. Memoria este alocată în secțiuni independente pentru fiecare funcție sau aplicație, iar acest lucru este gestionat de un controler dedicat pentru memorie și de sistemul de operare al cardului. Devine astfel posibil ca diferite funcții și aplicații ce provin de la diferiți emițători să fie stocate în siguranță pe card. De exemplu, permite dezvoltarea unui card de plăți care să servească totodată și drept card de acces în anumite clădiri. De această multifuncționalitate beneficiază atât emitenții cardurilor, care-și pot promova produsele într-un cadru mai diversificat, dar și utilizatorii.

Accesul la capacitate de procesare a datelor, prin CPU și MPU, se traduce printr-o multitudine de configurații posibile ale sistemului pe cip, cum ar fi suport pentru criptografie cu chei publice (Public Key Infrastructure – PKI), care necesită coprocesor matematic și mașini virtuale.

2.2.3 Carduri Contactless

Reprezintă cardurile smart care utilizează o frecvență radio (RFID) pentru a comunica cu cititorul de carduri. Așadar, nu este nevoie de contact fizic, ci doar de trecerea cardului prin proximitatea cititorului. Se folosesc cel mai des drept carduri de acces în clădiri securizate. Dezavantajele cardurilor contactless constau în funcțiile limitate de criptografie și de organizare a memoriei, spre diferență de cardurile cu microprocesor, cât și atingerea distanței de proximitate între card și cititor.

Cardurile contactless au o memorie limitată și funcționează la o frecvență de 126 MHz. Există și un tip special de astfel de carduri, Gen 2 UHF, care operează la frecvențe între 860-960 MHz. Cele care oferă funcții atât de citire cât și de scriere au fost prima oară folosite pentru transportul public și comunicau la 13 MHz prin standardul ISO 14443. Există mai multe variații pe specificațiile acestui standard, notate cu A, B, C, pentru a desemna diferiți producători, astfel: A este pentru NXP-Philips, B este pentru toți ceilalți producători iar C este pentru cipuri produse de Sony.

2.3 Ciclul de viață

Producerea unui element securizat constă din mai multe etape:

1. Procesorul este produs și testat de o companie care produce cipuri. O serie de fabrică (fabrication key – FK) este adăugată pentru a proteja cipul de la modificarea frauduloasă până

la etapa următoare. Fiecare cip are un FK unic și care este derivat dintr-o cheie master a fabricantului.

2. Cipul este montat pe o cartelă de plastic, iar FK este înlocuit cu o altă cheie. Acest procedeu este menit să protejeze cardul de modificări ulterioare prin instaurarea unui cifru personalizat și dezactivarea instrucțiunilor de acces fizic la memoria de date.
3. Entitatea care emite cardul (ex: bancă) scrie fișierele de date și aplicațiile pe card, precum și identitatea deținătorului cardului (ex: client).
4. Clientul utilizează cardul de plăți în viața de zi cu zi. Accesul la informația de pe smart card este limitată de politicile de securitate ale elementului securizat.
5. În caz de necesitate, cardul poate fi invalidat prin blocarea codurilor PIN sau activarea unui lock. În primul caz se dezactivează toate instrucțiunile, pe când în al doilea caz se vor dezactiva toate, mai puțin cele pentru depanarea și analiza incidentelor survenite.

Ciclul de viață al elementelor securizate pe bază de Java Card diferă ușor în etapele 3 și 4, încât rămâne posibilitatea de a descărca date și aplicații pe card de mai multe ori.

2.4 Smart card power-up

În momentul în care introducem un smart card cu element securizat într-un cititor de carduri sau terminal gazdă, circuitul nu este imediat activat, întrucât există riscul să nu fie bine introdus și astfel să distrugem cardul. Odată ce se detectează faptul că smart cardul a fost introdus corect, dispozitivul care acceptă carduri sau echipamentul mobil gazdă vor alimenta SE la un voltaj normal de operare și este adus în stare de așteptare. În acel moment, o comandă RST este trimisă prin linia contactului C2 de pe fața cardului. Semnalul RST rămâne în stare joasă pentru o anumită perioadă, după care comută pe înalt. Acest lucru semnalizează elementului securizat că poate începe secvența de inițializare.

Secvența de inițializare se încheie atunci când cardul transmite un semnal de Answer to Reset (ATR). Scopul principal al acestui semnal este să indice statusul secvenței de pornire a SE și transmite informațiile de care are nevoie cititorul pentru a optimiza viteza de transfer între cele două entități care comunică. Lungimea totală a secvenței ATR este limitată la 33 bytes, conform structurii specificate în ISO 7816-3

3. FACTORII de FORMĂ ai ELEMENTULUI SECURIZAT

În această secțiune vom descrie diferitele forme fizice pe care le poate îmbrăca elementul securizat. Fiecare astfel de factor de formă este caracterizat de propriile avantaje și dezavantaje, iar conștientizarea acestor aspecte este crucială pentru dezvoltarea de aplicații dependente de platformă.

3.1 Elementul securizat UICC

UICC este un smart card care conține aplicațiile ce autentifică terminalele mobile (telefon mobil, smartphone, tablete etc) la o rețea de date mobilă. Cel mai cunoscut exemplu este SIM. Cartelele UICC sunt distribuite de operatorii de rețea mobilă (MNO) care dictează și cadrul tehnologic al acestora.

Atunci când un furnizor de aplicații dorește să instaleze ceva pe SE, trebuie să ceară acordul MNO. De aceea, sistemul de operare al UICC poate avea diferite domenii de securitate pentru diferiți furnizori de aplicații.

Avantajele UICC

- are acces direct la funcționalitatea terminalului mobil și primește informații de la tastatură;
- interacționează cu utilizatorul fără să fie nevoie de instalarea unui software special pe telefon;
- transmite date printr-o interfață Single-Wire Protocol + Host Controller Interface;
- asigură interoperabilitatea respectând specificații tehnice ca ETSI Smart Card Platform și GlobalPlatform;
- permite portarea informațiilor personale ale utilizatorului când este instalat în alt terminal;
- respectă standardele de securitate impuse de bănci și alți furnizori de servicii
- poate fi partiționat în mai multe domenii de securitate independente, pentru a găzdui aplicații ce provin din surse diferite;
- există un canal de comunicare tip Over-the-Air (OTA) între serverul de administrare și UICC, prin protocoalele SMS, CAT-TP și RAM/FRM pe HTTPS;
- este posibilă proviziune OTA astfel încât unele aplicațiile descărcate pot să dezactiveze SE când terminalul este pierdut sau furat, cu scopul de a proteja datele confidențiale de pe acesta;
- mereu online (disponibil) și accesabil prin interfețe ISO;
- utilizează Card Application Toolkit (CAT), definit în ETSI TS 102 223, pentru a dialoga cu dispozitivul în care e instalat sau aplicațiile acestuia.

Dezavantajele UICC

- necesită un telefon cu capabilități NFC și SWP;
- necesită un acord de business între MNO și ceilalți furnizori de servicii;
- distribuirea și certificarea aplicațiilor trebuie planificate în funcție de ciclul de viață al UICC și strategia de piață a MNO. Un UICC poate rămâne activ într-un terminal mobil pentru mai mulți ani, spre deosebire de cărțile de plăți.

3.2 Element securizat embedded (eSE)

eSE reprezintă un chipset separat pe dispozitivul mobil și este înglobat pe placa de circuite integrate în faza de producție. Este conectat la receptorul contactless (CLF) printr-o interfață standard precum SWP, dar și DCLB sau NFC-WI. Acest element securizat este distribuit și controlat de producătorii de telefoane mobile.

Avantajele eSE

- pot fi utilizate pe dispozitive mobile care nu folosesc UICC/SIM și prezintă un cost mai redus decât smart cardurile microSD;
- nu au nevoie de același nivel de standardizare precum SE detașabile întrucât nu pot fi instalate în alte dispozitive.

Dezavantajele eSE

- nu există posibilitatea de portabilitate când schimbăm terminalul. În schimb, trebuie ca aplicațiile să fie dezinstalate de pe vechiul terminal și reinstalate pe cel nou;
- trebuie ca eSE să fie certificat pe fiecare nou dispozitiv;
- aplicațiile trebuie adaptate la protocolul de comunicație utilizat între SE și terminalul gazdă;
- procesele de certificare și validare pot avea un grad sporit de complexitate atunci când folosim interfețe proprietare, întrucât SE este lipit pe placa de circuite integrate;
- ciclul de viață depinde de ciclul de viață al terminalului gazdă. Nu există opțiunea de a înlocui SE independent de terminal;
- este necesar un mecanism de ștergere urgentă și completă a datelor atunci când dispozitivul este pierdut, vândut sa furat, pentru a proteja informațiile utilizatorului;
- gestionarea comunicării prin SWP cu UIC este o sarcină complexă, cu multe probleme de interoperabilitate.

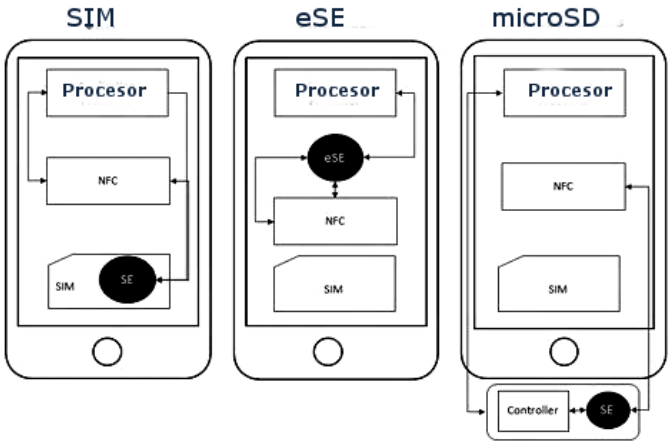


Figura 3: Factori de formă ai SE

3.3 Smart card microSD

SE poate fi stocat și în interiorul unui card tip microSD, întrucât arhitecturile lor de calcul coincid. Termenul „smart microSD" a fost definit de asociația SD. Valoarea adăugată a acestui factor de formă o reprezintă potențialul lui de a fi utilizat independent de MNO și producătorii de dispozitive mobile.

Există două tipuri de SE tip microSD card:

- NFC microSD complet, care are propriul controller NFC și propria antenă;
- NFC microSD, care este conectat la un controller NFC și la antenă printr-o legătură SWP.

Asociația SD standardizează doar NFC microSD și tot ei definesc interfața dintre dispozitiv și microSD când se trimit pachete de tip APDU, precum este definit în specificațiile ASSD [64].

Avantajele microSD

- furnizorii de aplicații pot distribui carduri microSD către clienți fără a implica în acest proces MNO sau producătorii de dispozitive mobile. Aplicațiile de pe microSD pot fi transferate de pe vechiul telefon pe cel nou fără a fi nevoie să le descărcăm din nou;
- Smart microSD permite ca furnizorul de aplicații să fie posesorul de drept al SE;
- furnizorii de servicii pot personaliza suprafața cardului microSD utilizat ca SE.

Dezavantajele microSD

- cele mai multe terminale mobile dețin un singur slot pentru carduri microSD, iar acestea sunt de cele mai multe ori utilizate pentru carduri care extind memoria dispozitivului pentru

stocarea unor date de tip fotografii. Ar putea deveni inconfortabil pentru utilizator să schimbe cardurile microSD în momentul în care dorește să beneficieze de servicii NFC, mai ales când slotul respectiv nu este ușor de accesat în majoritatea terminalelor. O soluție ar fi ca microSD folosit ca SE să conțină și memorie de utilizator suplimentară, pentru a îndeplini și funcția de stocare a datelor acestuia, dar aceasta implică un cost mai mare;

- emițătorul de SE microSD (furnizorul de aplicații) poate să permită și altor furnizori de aplicații să folosească SE sau există posibilitatea ca multe carduri microSD să coexiste în același dispozitiv pentru a suporta aplicații dintr-o gamă largă de surse;
- nu există niciun standard prin care aplicațiile de pe microSD să interacționeze direct cu utilizatorul;
- problemele de interoperabilitate apar relativ la modul în care se realizează accesul terminalului la microSD, întrucât specificațiile ASSD nu au fost adoptate la nivel larg. Putem implementa pe microSD și soluții proprietare care utilizează comenzile pentru stocare în memorie definite de protocolul SD.

3.4 NFC microSD complet

NFC smart microSD complet oferă posibilitatea de a accesa servicii NFC dispozitivelor care nu sunt prevăzute cu interfață NFC, neavând nici controller NFC, nici antenă.

Avantaje NFC microSD complet

- microSD conține atât cipul NFC cât și SE;
- poate fi utilizat în dispozitive și terminale care nu sunt prevăzute deloc cu capabilități NFC.

Dezavantaje NFC microSD complet

- în funcție de tehnologia dispozitivului, antena poate fi acoperită de alte componente (baterie, capac metalic etc), care pot interfera cu semnalul și pot întrerupe comunicația;
- operațiile NFC se pot comporta imprevizibil când un NFC smart microSD complet este introdus într-un dispozitiv care este prevăzut deja cu NFC, prin controller și antena. Din păcate, există anumite bariere tehnologice (cum ar fi drepturile la proprietate intelectuală) care nu permit derularea unor teste de compatibilitate care să ducă la conceperea unei soluții stabile pentru această situație.

3.5 NFC microSD combo

Smart microSD este distribuit de furnizorul de servicii, independent de MNO. Tot furnizorul de servicii se ocupă și de gestionarea SE.

Avantajele smart microSD combo

Există mai puține probleme de interoperabilitate când utilizăm acest SE într-un dispozitiv mobil, întrucât utilizează capabilitățile NFC ale telefonului, care se presupune că au fost testate și calibrate pentru a funcționa în condiții diverse;

Dezavantaje

Necesită un terminal cu capabilități NFC, interfața SD și legătură de date tip SWP.

4. ARHITECTURA INTERNĂ

Întrucât un smart card precum elementul securizat are forma unei cartele subțiri cu cip înglobat, acest lucru impune o serie de provocări în proiectarea arhitecturii interne. Cu toate acestea, soluția adoptată a fost de a scala în jos arhitectura cipurilor convenționale în loc de dezvoltarea unor noi arhitecturi.

În fapt, arhitectura internă a unui smart card cu microprocesor este proiectată în același spirit cu calculatoarele personale. Putem astfel constata prezența blocurilor structurale de bază ale calculatoarelor: CPU, ROM, RAM, porturi I/O și EEPROM pentru stocare (în loc de disc magnetic).

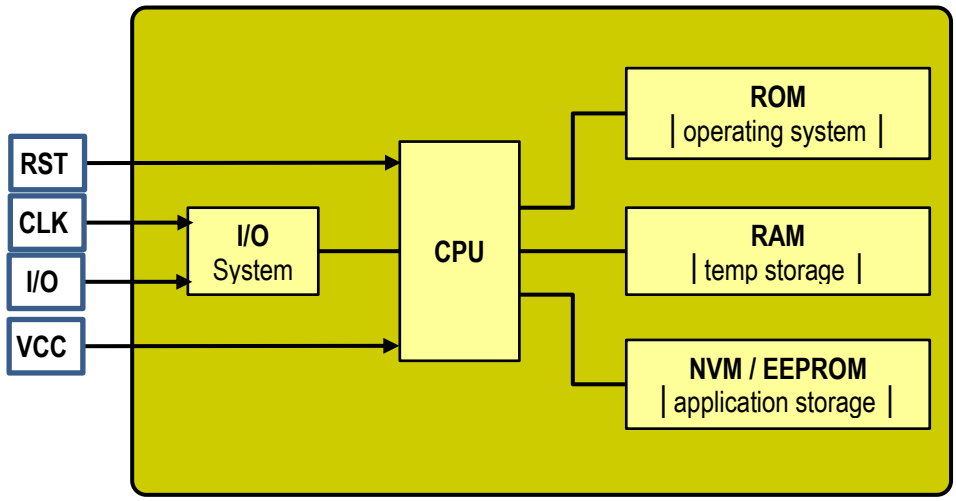


Figura 4: Arhitectura internă a elementelor securizate

4.1.1 Unitatea centrală de procesare (CPU)

CPU pentru smart card este implementat ca un microcontroler de 8, 16 sau 32 biți, dar care nu prevede facilități precum multi-threading, multi-tasking și altele. Instrucțiunile de cod mașină sunt executate la viteze de aproximativ 1 MIPS, iar de calculele matematice precum cele din criptare/decriptare se ocupă un co-procesor.

Pentru CPU sub forma unui microprocesor pe 8 biți se utilizează o magistrală de adrese pe 16 biți, ceea ce face posibil ca aceste carduri să acceseze un maximum de 64 KB de memorie.

4.1.2 Co-Procesor MATEMATIC

Elementele securizate sunt prevăzute cu un coprocesor matematic care să efectueze operațiile exponențiale și modulare pe numere întregi ce apar în cursul procedurilor de criptare și decriptare.

4.1.3 Sistemul de memorie

Există trei tipuri de memorie pe placa de circuit a elementului securizat:

RAM (Random-Access Memory) – Reprezintă memoria de lucru și este volatilă, adică poate stoca date doar cât timp este alimentată. Este utilizată de CPU pentru a încărca și rula aplicațiile existente pe SE. De obicei are dimensiuni de magnitudinea a 1KB, mai mici în comparație cu celelalte memorii, întrucât este realizată pe o tehnologie mai costisitoare și ocupă mai mult spațiu fizic per byte de date. În plus, nu este nevoie ca SE să aibă acces la multă memorie RAM, având în vedere că este folosită doar pentru calcule rapide și generarea de semnale răspuns.

EEPROM (Electrically Erasable PROgrammable Memory) – Reprezintă memoria de stocare și este non-volatilă, spre diferență de RAM, ceea ce înseamnă că nu își păstrează conținutul atunci când iese de sub alimentare. Aplicațiile pot rezida și pot rula de pe această memorie, dar este mai înceată și poate fi citită/scrisă de un număr limitat de ori (magnitudine 100.000). Așadar, această memorie este folosită pentru stocarea datelor și programelor, întocmai ca un hard-disk de pe calculatoarelor personale. Sistemul de operare furnizează mecanisme pentru protecția fișierelor, prin restricționarea

selectivă a accesului către EEPROM. Capacitatea EEPROM poate varia în funcție de aplicația implementată, dar în zilele noastre se folosesc de obicei astfel de memorii de aproximativ 64-128KB.
ROM (Read-Only Memory) - Reprezintă memoria în care rezidă sistemul de operare și alte componente critice ale elementului securizat, precum algoritmii de criptare. Sistemul de operare este încărcat pe ROM în timpul procesului de fabricație, de către producător. Acest software mai este denumit și mască ROM (ROM-mask). Capacitatea memoriilor ROM poate varia de la câțiva KB la câteva sute, în funcție de complexitatea sistemului de operare ce se vrea instalat. Deși sistemul de operare este stocat in ROM, acesta poate fi aprovizionat cu noi aplicații ce vor fi salvate pe EEPROM, dar nu există posibilitatea efectuării de upgrade la sistemul de operare. O excepție reprezintă cazul când extensiile acestuia sunt descărcate pe EEPROM, dar această practică este mai rară. Dezvoltarea codului sursă pentru diferite aplicații necesită o bună cunoaștere a setului de instrucțiuni ale CPU, în cazul în care se dorește programarea acestuia la low-level. Alternativa constă în utilizarea tehnologiei Java Card, care permite dezvoltarea de appleturi într-un subset la limbajului Java și rulează pe elementul securizat într-o mașină virtuală Java.

4.1.4 I/O

Se efectuează printr-un singur port I/O care este controlat de procesor. Comunicația de date este standardizată sub forma protocolului APDU. Datele se transferă într-o manieră serială, bit cu bit. Viteza de transfer este de obicei de 9600 biți pe secundă, dar există și carduri cu viteze mai mari.

4.1.5 Dispozitive de Interfațare (IFD)

Un smart card ca elementul securizat are nevoie de alimentare și un semnal de tact pentru a rula programe, însă nu este prevăzut cu niciunul dintre acestea. Semnalele în cauză trebuie furnizate printr-un dispozitiv de interfațare, de obicei un cititor dedicat, care intră în contact cu cardul, sau din circuitul electronic al dispozitivului gazdă, în cazul terminalelor mobile cu element securizat înglobat. Asta înseamnă că fără alimentare, un element securizat nu este decât un dispozitiv de stocare, întrucât memoria EEPROM este singurul circuit care „funcționează” permanent.

Pe lângă furnizarea semnalelor de alimentare și de ceas, cititorul de carduri sau controlerul terminalului gazdă se ocupă și de deschiderea unui canal de comunicație între aplicația software și sistemul de operare al cardului. De obicei, aceste dispozitive pot atât citi, cât și scrie, adică permit unei aplicații externe, cu drepturile potrivite de securitate, să modifice informația de pe card la care are acces.

Canalul de comunicații cu un smart card este half-duplex, ceea ce înseamnă că datele pot parcurge magistrala fie dinspre IFD spre card, fie dinspre card spre IFD, dar nu în ambele direcții în același timp. Receiverul trebuie să eșantioneze semnalul de pe linia serială la aceeași rată cu care transmițătorul îl trimite, pentru ca să fie recepționate datele în mod corect. Această rată se numește bitrate sau baud rate. Atât la transmitere, cât și la recepție, datele sunt stocate într-un buffer din memoria RAM. Întrucât aceasta are o capacitate mică, mesajele conțin pachete mici de date, de ordinul zecilor de bytes.

În tabelul următor se poate vedea o comparație între o serie de smart carduri clasice, ce pot fi programate în limbaj de asamblare și nu dispun de resurse semnificative. Cardurile Java prezintă specificații tehnice mai bune, dar personalizate de fiecare producător pentru piața cărora li se adresează.

Smart Card	Word size	ROM	EEPROM	RAM	Voltage	Clock	Write/erase cycles	Transmission rate
Infineon SLE 44C10S	8-bit	9K	1K	256b	2.7 - 5.5V	5 MHz	500 000	9600 baud
Orga ICC4	8-bit	6K	3K	128b	4.7 - 5.3V		10 000	
GemCombi	8-bit		5K		4.5 - 5.5V	13.6 MHz	100 000	106 kbaud
DNP Risona	8-bit		1K		5V	3.5 MHz		9600 baud

AmaTech Contactless	8-bit		1K		5V	13.6 MHz	100 000 cycles	
Schlumberger Cyberflex	8/16-bit	8K	16K	256b	5V	1-5 MHz	100 000 cycles	9600 baud

4.1.6 Mecanisme de Securitate

Toate datele și parolele stocate pe elementul securizat se găsesc în EEPROM sub formă de sarcină electrică. Teoretic, ar putea fi șterse sau modificate printr-un voltaj de o valoare neobișnuită, dar elementele securizate sunt protejate la atacuri fizice prin mai multe tehnici. De exemplu, acest tip de atacuri ar putea fi detectate prin includerea unor senzori ambientali care trebuie configurați la o anumită toleranță și pattern de fluctuație al semnalului primit din exterior. Alte tipuri de atacuri pot fi supraîncălzirea circuitului integrat la temperaturi ridicate sau bombardarea memoriei EEPROM cu lumină ultravioletă pentru a dezactiva protecția. Tot la categoria atacurilor fizice intră și situația în care smart cardul este desfăcut iar procesorul detașat, la nivel microscopic, cu scopul de a depista tehnologia folosită pentru protecție. Elementele securizate sunt apărate și împotriva acestor tipuri de intruziuni, prin modul în care sunt fabricate și asamblate.

Un alt atac susceptibil operațiilor cu date confidențiale este Analiza de Putere Diferențială (DPA), o metodă statistică de a trece de un algoritm criptografic prin compararea unei ipoteze cu rezultatul pentru a extrage cheia de criptare dintr-un astfel de sistem de calcul ca un element securizat. O altă tehnică similară este Analiza de Putere Simplă (SPA), care analizează direct datele referitoare la energia electrică vehiculată, pentru a determine atât acțiunile întreprinse de sistemul de operare al elementului securizat, dar și pentru a intercepta datele confidențiale.

Mai multe tehnologii au fost dezvoltate pentru a proteja elementele securizate la astfel de atacuri fizice, mai ales contra SPA și DPA:

- barieră tehnologică – Tehnologia de fabricație pe 0.6 microni reduce în mare măsură atât dimensiunea cât și consumul de putere al elementelor securizate, ceea ce conduce la diferențe relativ în parametrii de operare. Asta face mult mai dificil pentru metode ca SPA și DPA să distingă între fluctuațiile cauzate de card și cele cauzate de date;
- fluctuații de ceas – Facilitatea de Clock Software Management conduce la o cadențare software variabilă, în timp ce o aplicație oarecare rulează;
- comportament imprevizibil – Un timer intern cu capabilitatea de a genera întreruperi și un generator de numere imprevizibile (aleatoare) sunt folosite pentru a impune variații imprevizibile în modul în care e executat software-ul, ceea ce va conduce și la schimbări în structura consumului de putere;
- design robust – Modularizarea permite alte variații ale hardware-ului, inclusiv personalizate de utilizator, care să fie produse repede și eficient, ceea ce facilitează un răspuns rapid în fața atacurilor;
- memorie multi-aplicații – Sistemul de control al accesului la memorie ajut sistemul de operare să gestioneze într-un mod securizat stocarea datelor secrete ce provin din surse diferite;
- rutine low-level – Un set extins de mecanisme de securitate și funcții de firmware permit unei aplicații să detecteze și să răspundă în mod potrivit apariției unor condiții ce indică posibilitatea unui atac.

Aceste condiții includ moduri de operare invalidă, opcoduri greșite, adrese eronate și violarea integrității cipului; reacțiile posibile includ întreruperi, resetarea programului, ștergerea instantanee a datelor din RAM și reprogramarea câmpului EEPROM.

5. COMUNICAREA cu ELEMENTUL SECURIZAT

Un element securizat și un dispozitiv de citire carduri comunică între ele prin mici pachete de date denumite APDU (Application Protocol Data Units). În ciuda faptului că orice dispozitiv extern care comunică cu smart cardul se constituie într-un punct de vulnerabilitate și interceptare, persoanele neautorizate vor întâmpina dificultăți în atacarea sistemului datorită următoarele caracteristici:

- rată de transfer (bit) scăzută, de aproximativ 9600 bps, care folosește o linie de transmisie bi-direcțională și serială ce respectă standardul ISO 7816/3;
- mod half-duplex pentru transmiterea informației, ceea ce înseamnă că datele vor călători într-o singură direcție a magistralei în orice moment;
- transmisia de date respectă un protocol sofisticat, descris mai jos.

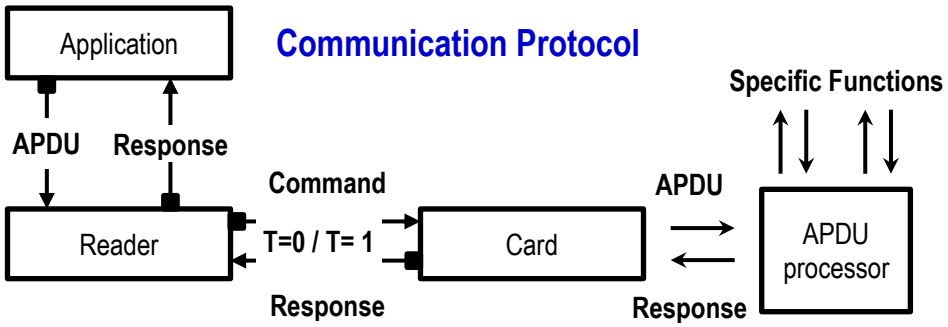


Figura 5: Protocolul de comunicații de date al SE

Elementul securizat și dispozitivul de citire folosesc un protocol de autentificare activă reciproc pentru a se identifica unul pe celălalt. SE va genera un număr aleatoriu pe care îl va trimite la CAD, care va cripta numărul cu o cheie de criptare partajată înainte de a-l returna către acesta. SE va compara rezultatul cu criptarea proprie. O altă posibilitatea este ca perechea de dispozitive să efectueze inversul acestei operații.

Odată ce comunicarea a fost stabilită, fiecare mesaj vehiculat pe magistrală va fi verificat printr-un cod de autentificare a mesajului. Acest număr este calculat din datele propriu-zise, o cheie de criptare și un număr aleatoriu. Dacă datele au fost modificate (din varii motive, inclusiv erori de transmisie), mesajul trebuie retransmis. Există și posibilitatea, în cazul în care cipul are destulă memorie și putere de procesare, ca datele să fie verificate prin semnătură digitală.

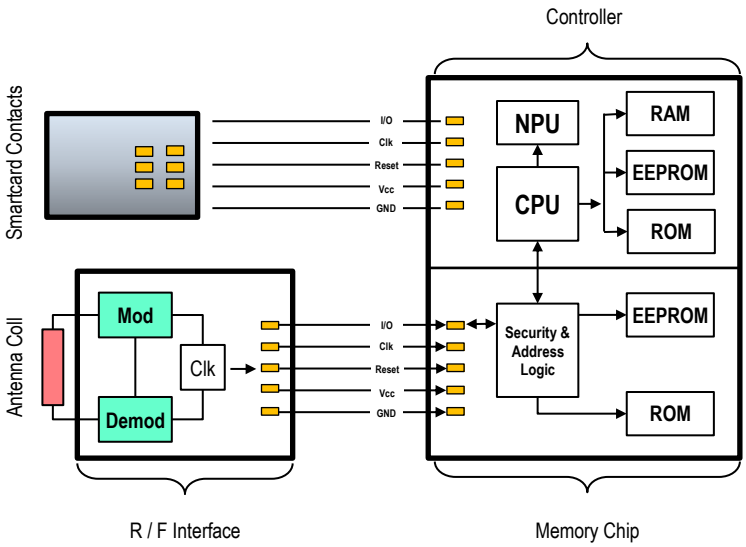


Figura 6: Diagrama bloc a componentelor interne și de I/O

Pentru criptarea mesajelor se folosesc metode consacrate, precum DES (Data Encryption Standard), 3DES și sistemul cu chei publice RSA, ceea ce permite chei în lungime de 56, 168 sau respectiv 1024 biți. Din păcate, în ultima vreme s-a dovedit că aceste chei pot fi sparte, un exemplu fiind dat de Anderson și Kuhn asupra elementului securizat Dallas DS5002FP, printr-o metodă de bruteforcing.

În continuare, vom descrie pe scurt magistralele și protocoalele de comunicație care pot asigura legătura între SE și interfața NFC, cunoscută sub denumirea de „contactless frontend” (CLF), dar și între SE și microprocesorul central al dispozitivului mobil.

Pentru comunicarea între un SE și CFL se pot folosi următoarele protocoale, pentru:

- UICC: Single-Wire Protocol (SWP) sau Host Control Interface (HCI);
- microSD: SWP/HCI;
- eSE: SWP/HCI, I2C, SPI, NFC-WI, DCLB

Deoarece SWP poate fi folosit pentru oricare din cei trei factori de formă, acesta este recomandat a asigura o interoperabilitate cât mai mare.

Un HCI care activează la nivelul superior este de obicei utilizat în conjuncție cu SWP, dar ar putea fi combinat cu oricare alt protocol fizic. Avantajul utilizării HCI este că permite dezvoltarea de aplicații sub incidența diferitelor standarde de interoperabilitate.

Pentru comunicarea între un SE și procesorul mobil se pot folosi următoarele protocoale, pentru:

- UICC: ISO7816;
- microSD: protocolul SD;
- eSE: cea mai populară soluție este ca CLF să ruteze comunicațiile între SE și procesorul mobil, ceea ce înseamnă că eSE trebuie deja să suporte un protocol adecvat de comunicare cu CLF.

Indiferent de conexiunea fizică și de protocolul adaptat, este necesar ca aplicațiile ce rulează pe procesorul mobil să poată interacționa cu aplicațiile de pe SE prin protocolul APDU. În imaginea de mai jos este modelul OSI pentru stiva de protocoale necesare la transmisia de date a SE:

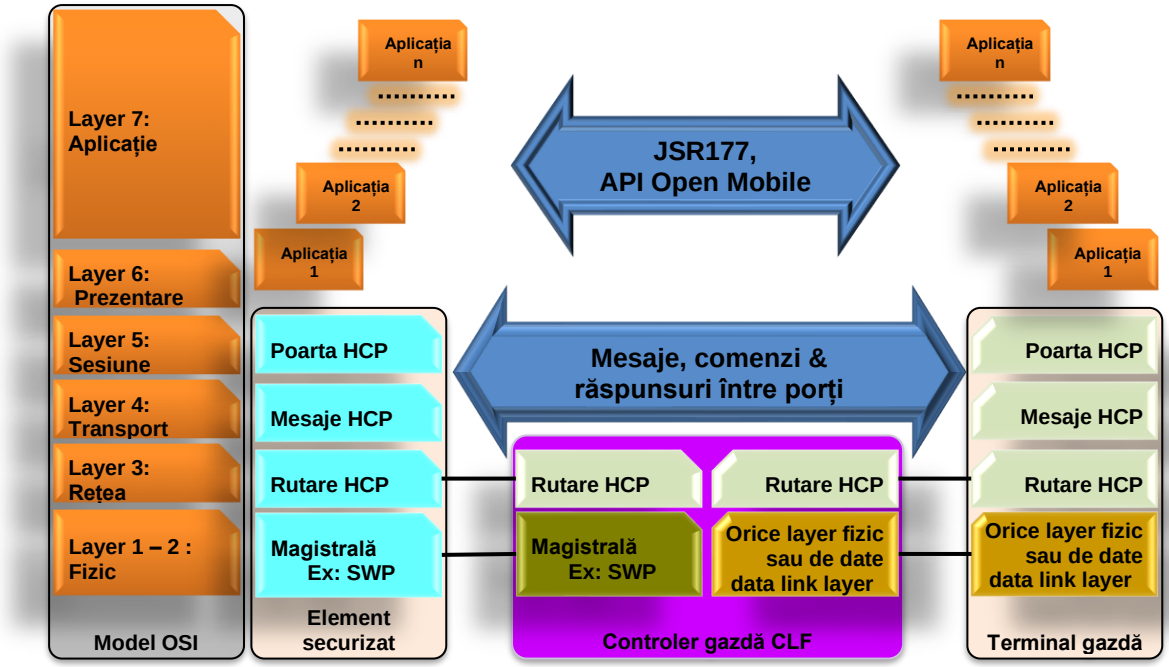


Figura 7: Model OSI transmisie date SE

5.1 SWP

SWP este de departe cea mai adoptată magistrală pentru interfațarea CLF cu SE, dar și un protocol obligatoriu care trebuie suportat de UICC și microSD.

SWP este un protocol bazat pe contact direct, care este folosit mai departe pentru a facilita comunicația contactless. Unul din pinii cardului UICC (C6) este conectat la CLF pentru suport SWP. Este un protocol duplex, la nivel de biți, ceea ce înseamnă că este posibil ca transmisia și recepția să se efectueze în același timp. CLF se comportă ca master, iar UICC ca slave. CLF furnizează UICC cu energie electrică, ceas de sincronizare a transmisiei, date și semnal pentru gestionarea magistralei. Datele transmise sunt reprezentate ca stări binare ale voltajului și curentului de pe un singur fir.

În afară de alocarea pinilor, specifică fiecărui factor de formă SE, protocolul SWP este detaliat încă din versiunea 2011 a documentului NFC Stepping Stones [1].

5.2 SPI

Interfața Periferică Serială (SPI) este utilizată pentru comunicația între CLF și eSE. Suportă viteze de transfer de ordinul zecilor de Mbps.

Această interfață nu poate fi utilizată pentru UICC și microSD.

SPI este o interfață serială sincronă cu scop general, creată de MOTOROLA în anii ’80, și care a fost adoptată și de alți producători de cipuri între timp. A fost proiectată pentru a permite unui microcontroler să comunice cu dispozitive periferice precum memorii EEPROM.

Magistrala SPI operează în mod full duplex, conform unei relații master-slave. Masterul este responsabil pentru inițierea cadrelor de date.

O Implementare multi-slave poate fi executată conform exemplului de mai jos:

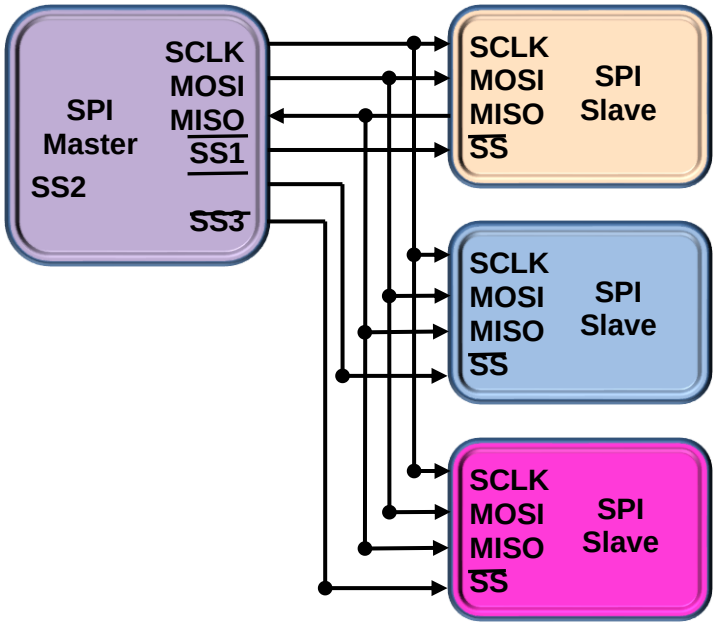


Figura 8: Magistrala SPI: Un singur master, mai mulți slave

Protocolul SPI prevede patru semnale:

- Clock/tact (SCLK1);
- Master output, Slave input (generat de Master (MOSI));
- Master input, Slave output (generat de Slave (MISO));
- selecția Slave (SS)

Figura de mai sus arată cum sunt rutate aceste semnale în configurația multi-slave. Masterul generează semnalul de tact și apoi selectează slave-ul cu care dorește să comunice.

5.3 I²C

Precum SPI, interfața Circuit Inter-Integrat (I²C) este utilizată pentru a permite CLF să comunice cu eSE, dar nu poate fi folosită în cazul microSD sau UICC. Asigură rate de transfer de maxim 400 Kbps.

I²C este o magistrală serială sincron dezvoltată de Philips, tot în anii '80, cu același scop ca și SPI, de a interconecta procesoare și a fost folosită foarte mult în televizoare. Mai este cunoscută și drept interfața cu două fire, întrucât necesită doar un semnal de date (SDA) și un semnal de clock/tact (SCL), precum în imagine

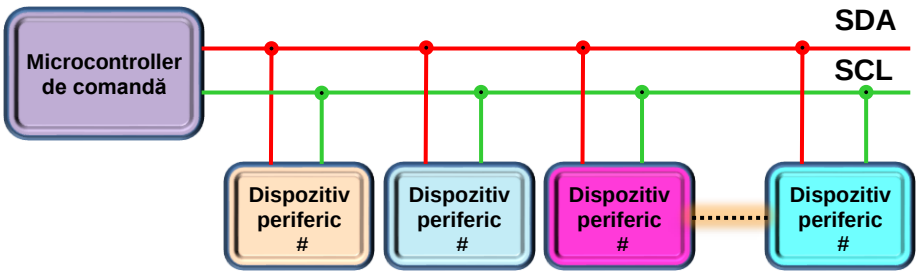


Figure 9: Interfața dublu-fir I²C

Controlerul master generează semnalul de clock (SCL) și trimite datele (SDA), cu excepția semnalului de confirmare, care este generat și transmis de slave, pentru a indica recepția datelor. Dacă nu se primește mesajul de confirmare, comunicația poate fi oprită sau repornită.

Mai multe dispozitive slave pot fi conectate la aceeași magistrală I²C, fiecare având propria sa adresă. Această adresă este codificată pe 8 biți, compusă dintr-o parte fixă (definită de producător) și o parte configurabilă hardware, precum și un bit de citire/scriere care definește direcția comunicației (0 pentru scriere, 1 pentru citire).

Transferul de date începe cu un bit de start, urmat de adresa pe 8 biți, confirmare, byte de date, un nou bit de confirmare și se termină cu un bit de stop, precum în figura următoare:

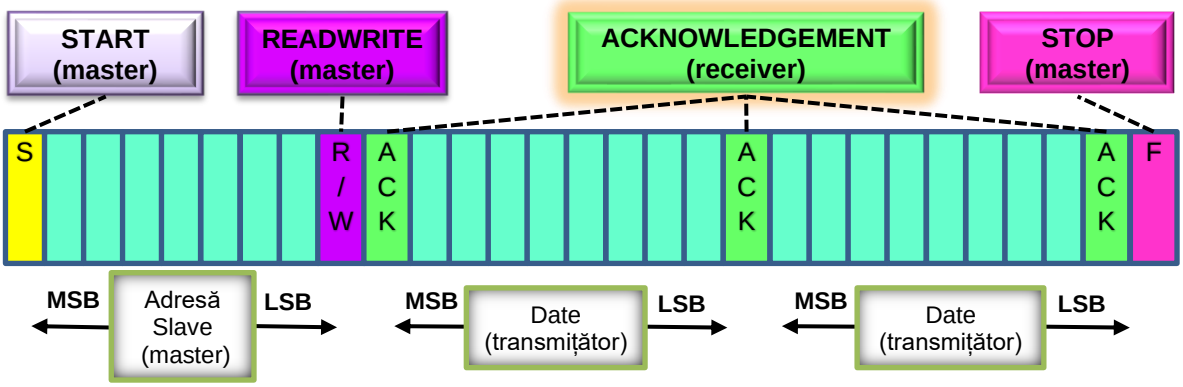


Figura 10: Comunicarea prin magistrala I²C

5.3.1 SPI vS. I²C

Cele două magistrale au fost adesea comparate, întrucât concurează pe aceeași nișă. În tabelul de mai jos sunt enumerate pentru fiecare dintre ele câteva argumente pro și contra:

	SPI	I²C
Aplicații	Fluxuri de date între procesoare	Transferuri ocazionale de date,

		Configurare de dispozitive slave
Rate de transfer	>> 10 Mb/s	< 400 Kb/s
Complexitate	3 linii de magistrală Circuistică complexă Multe pinuri pe cip	2 fire Nu se scalează cu numărul de dispozitive
Mod de adresare	Hardware (selecție cip)	Schemă internă de adresare
Comunicație	Fără mecanism de confirmare, Doar pentru distanțe scurte	Asigură integritatea datelor și detecția coliziunilor, mecanism de confirmare
Specificații	Nu există oficial	Există oficial
Licență	Free	Free

5.4 NFC-WI (aka ECMA 373, S2C)

Magistrala bus NFC-WI a fost definită prin standardul ECMA-373 și poate fi utilizată pentru comunicarea între CLF și SE doar în cazul embedded SE.

În urma standardizării sistemelor NFC, NFC-WI specifică o interfață gen dublu-fir între cele două componente, care sunt denumite „transceiver” și respectiv „front-end”. Sistemele care implementează NFC-WI pot fi augmentate și cu un front-end wireless pentru NFCIP-1, precum este ilustrat în următoarea figură:

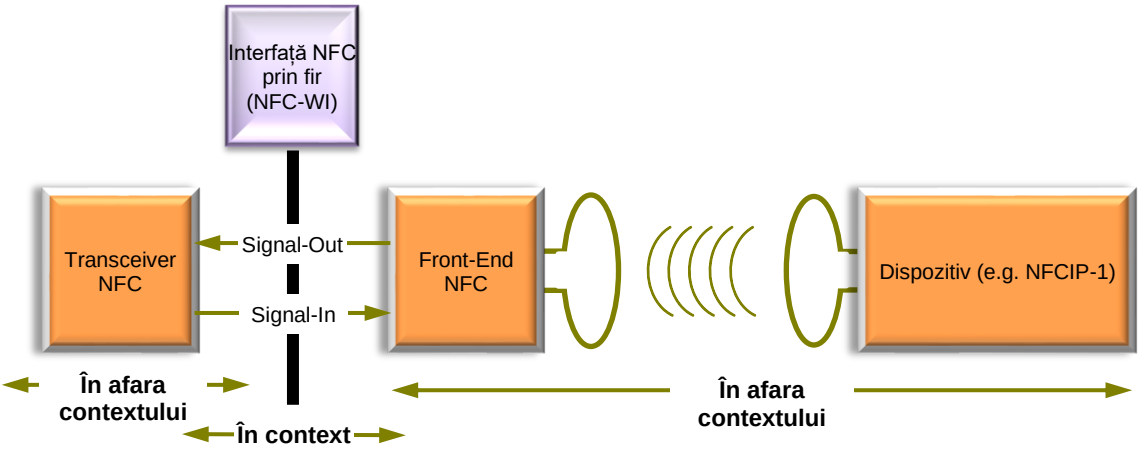


Figure 11: Interfața NFC-WI

Protocolul NFC-WI este limitat de ISO14443 tip A în modul de emulare a cardului. Tipul B al ISO14443 și mod cititor nu sunt suportate de acesta. Semnalul de tact are o rată de aproximativ 13 MHz.

Semnalele de intrare (In) și cele de ieșire (Out) sunt codificate prin scheme la nivel de bit precum Manchester sau Modified Miller și se combină în mod diferit cu tactul, în funcția de rata de transfer, astfel:

- rata 126 kb/s (F Clock/128):
  - semnalul Out este codificat în Modified Miller ȘI combinat cu F Clock;
  - semnalul In este codificat în Manchester SAU combinat cu F- Clock/17;
- rata 212 kb/s (F Clock/64):
  - semnalul Out este codificat în Manchester SAU EXCLUSIV combinat cu F- Clock/17;
  - semnalul In este codificat în Manchester;

- rata 424 kb/s (F Clock/32):
  - aceeași schemă de codificare precum F Clock/64

5.5 USB INTRA-CIP

USB intra-cip este definit în specificațiile ETSI TS 102 600 și poate fi utilizat între procesorul terminalului și SE (sau UICC) pentru rate de transfer de până la 12 Mbps half duplex. Acest protocol nu este disponibil pentru smart card micro SD.

Oficial, USB intra-cip reprezintă interfața de viteză ridicată între un terminal mobil și un UICC standardizat de ETSI. UICC care suportă această tehnologie au început să fie comercializate pe scară largă doar recent. Standardul USB intra-cip a fost definit în 2006 și constituie o extensie la specificațiile USB 2.0

Este o variantă de putere redus a interfeței USB standard, dedicată comunicației între componentele sistemelor embedded printate pe aceeași placă de circuit, dar cu o restricție de distanță între cipuri de aproximativ 10 centimetri.

Intra-cip USB constă în două fire:

- IC_DM: Linia de date D-;
- IC_DP: Linia de date D+.

Adițional, sunt necesare și semnale de alimentare [IC_VDD] și împământae [GND].

Există trei categorii diferite de USB intra-cip:

- ICCD: Dispozitive tip Card cu Circuite Integrate, care permit emularea interfației legacy de UICC și transferul de APDU tip ISO 7816-4 APDU la viteze înalte;
- EEM: Modelul de Emulare Ethernet, care suportă TCP/IP și UDP/IP, precum și transferul pachetelor IP, precum este definit în ETSI TS 102 483;
- stocare: Pentru emularea dispozitivelor de stocare a datelor.

5.6 DCLB

Digital Contactless Bridge (DCLB) este o interfață deschisă (license-free) dezvoltată de Infineon pentru interconectarea CLF cu SE, ce poate atinge viteze de transfer de până la 850 Kbps. Acest protocol se referă la eSE, nu și la UICC sau microSD.

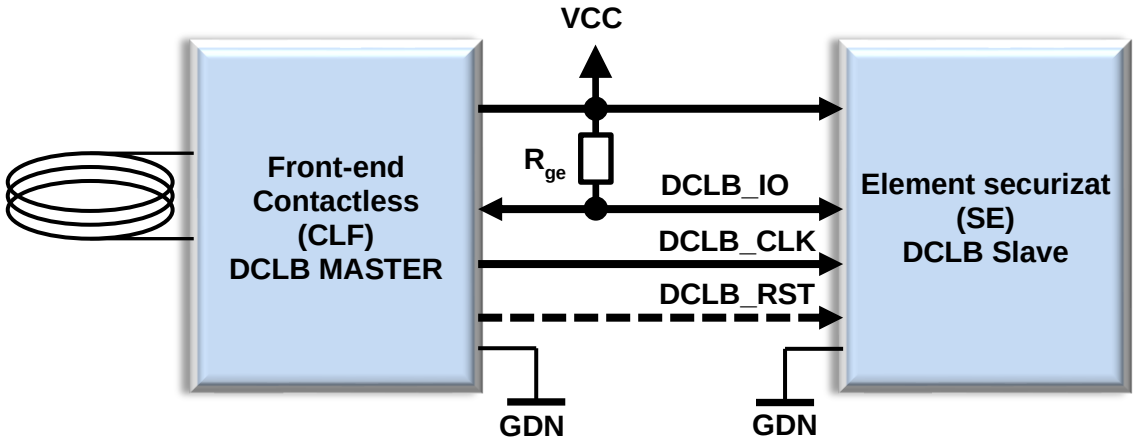


Figure 12: Interfața DCLB

Magistrala DCLB lucrează cu trei semnale:

- DCLB_Clock;
- DCLB_RST;
- DCLB_IO.

5.7 SD

Magistrala Secure Digital (SD) poate fi utilizată pentru interconectarea procesorului mobil la SE doar în cazul factorului de formă microSD. Această interfață a fost definită în 2000 de specificațiile SD emise de Asociația Cardurilor SD.

Cardurile de memorie SD sunt proiectate special pentru a îndeplini cerințele de securitate, performanță, capacitate și protecția mediului impuse de noile dispozitive electronice audio/video. Formatul SD include cinci familii de carduri, disponibile în trei factori de formă. Familiile sunt: format original, Standard-Capacity (SDSC), High-Capacity (SDHC), eXtended-Capacity (SDXC).

Există de asemenea SDIO, care combină funcții de input/output cu stocare de date, dar și smartSD (smart card microSD) care suporta extensiile ASSD. Aceasta din urmă este folosită pentru SE.

5.7.1 Accesarea Elementului Securizat

Asociația SD a actualizat de curând soluția fizică pentru interfațarea prin SWP, pentru a fi compatibilă cu vitezele foarte ridicate precum UHS-II. Astfel, se definește un nou PIN pentru semnalul SWP (SWIO), iar pinul de alimentare Vdd2 este la comun cu interfața UHS-II pentru operații NFC. Pentru adresarea conținutului cardului microSD a fost adaugată și interfața HCI. Diagrama noii configurații poate fi observată în figură:

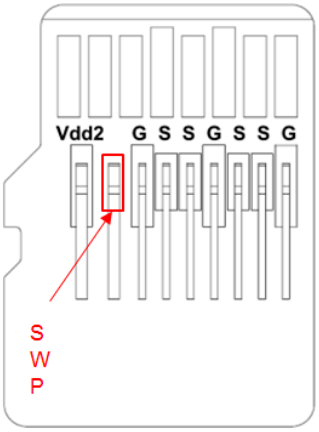
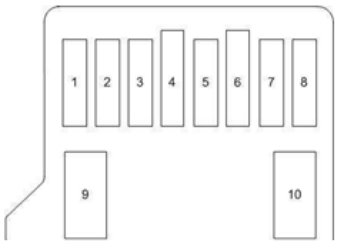


Figura 13: Suport SWP în microSD

SDA a dezvoltat și o configurație alternativă care suportă anumite implementări legacy. Astfel, pinul SD3.X este refolosit pentru transfer contactless, ceea ce înseamnă că timpul către comercializare este mai scurt, deoarece conectorii sunt deja disponibili în circuit.



Pin#	Name	Type	Description
9	SWIO	I	Single Wire Protocol Interface
10	V_{DD2}	S	Supply voltage

Figura 14: Configurație alternativă pentru suport SWP în microSD

6. Exemple de Elemente Securizate

În ceea ce urmează, sunt descrise caracteristicile tehnice a trei elemente securizate care sunt comercializate în acest moment de producători consacrați din industrie. De notat că modul în care funcționează anumite tehnologii proprietare ce asigură securitatea datelor nu au fost dezvăluite public.

6.1 ST33 (ST Microelectronics)

ST33 este o clasă de microcontrolere cu acces serial care incorporează cea mai nouă generație de procesoare ARM pentru sisteme înglobate. Este destinat aplicațiilor mobile securizate, precum comunicații mobile, aplicații Java Card, plăți electronice prin NFC și, în general, ca element securizat.

Nucleul RISC SecurCore SC300 pe 32 biți este construit pe un nucleu Cortex M3, cu caracteristici adiționale de securitate care să protejeze împotriva a diferite feluri de atacuri din exterior.

Procesorul lucrează la o frecvență de 22,5 MHz și permite o densitate foarte bună a codului, întrucât implementează setul de instrucțiuni Thumb-2. Sistemul este prevăzut cu o memorie Flash rapidă, cu capacități de până la 1280 Kbytes și o memorie RAM de până la 30 Kbytes. ST33 este prevăzut cu 3 timere pe 16 biți, dintre care unul poate fi configurat pentru control și monitorizare.

Elementele securizate ST33 comunică printr-o interfață serială compatibilă cu standardul ISO/IEC 7816-3 și pot fi conectate la dispozitivul NFC prin interfață SWP, pentru aplicații ce implică SIM/NFC. Este disponibilă și o interfață SPI Slave pentru comunicarea cu aplicațiile ce nu se găsesc pe SIM, dar funcționează disjunct cu comunicația prin ISO/IEC 7816.

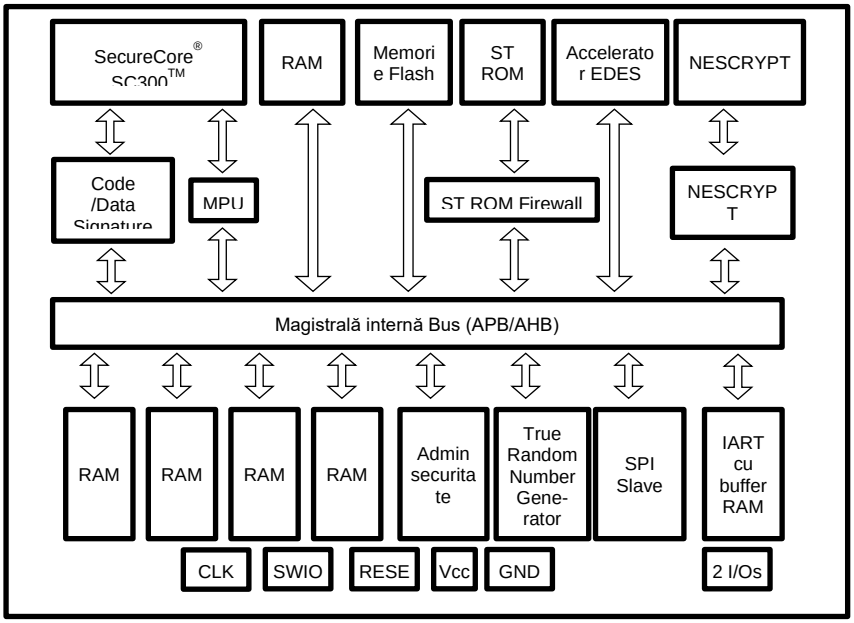


Figura 15: Diagrama bloc a SE ST33

Funcțiile avansate de criptografie sunt suportate prin accelerare hardware. Perifericul EDES implementează algoritmul DES, în timp ce cripto-procesorul NESCRYPT se ocupă de algoritmul cu chei publice. Sistemul deține mecanisme de securitate a datelor precum active shield, unitate de protecție a memoriei, ISO 3309 CRC și generator de numere aleatorii.

Familia dispozitivelor ST33F funcționează în plaja de temperaturi ambientale [–25:+85] °C, acceptând tensiuni de alimentare de 1.8V, 3V și 5V. Proiectarea aplicațiilor cu consum eficient de energie este posibilă prin utilizarea modurilor de economisire a energiei prevăzute, care sunt compatibile cu specificațiile GSM și ETSI.

6.2 SLE 97400 SE/SD (INFINEON)

SLE97400SE/SD este un element securizat înglobat (eSE) pentru dispozitive mobile, tablete și alte terminale, bazat pe tehnologiile Infineon Integrity Guard și Solid Flash și este distribuit cu aplicația CIPURSE deja integrată. Această familie de produse este proiectată pentru aplicații securizate critice, precum plăți electronice, controlarea accesului și autentificare.

Arhitectura SLE97400SE/SD prevede un microcontroler securizat pe 16 biți, 400 Kbytes de memorie Flash și 8Kbytes de RAM. Funcțiile de criptare AES și 3DES sunt executate cu ajutorul accelerării hardware.

Pentru integrarea în infrastructura contactless existentă, suportă emularea MIFARE Classic (1K și 4K). Magistrala de comunicație utilizată de SLE97400SE/SD este DCLB. Varianta SLE97400SD oferă o interfața dual ce poate fi folosită atât în mod contact (ISO/IEC7816), cât și contactless (ISO14443 A/B).

SLE97400SE/SD este conform specificațiilor definite prin Global Platform 2.2.1. Sistemul de operare instalat pe acest sistem este Java Card 3.0.1 clasic, care poate fi ușor updatat și upgradat. Dispozitivul operează în gama de temperaturi [-25:85] °C.

6.3 P5CN072 (PHILIPS)

P5CN072 este un controler smart card securizat cu dublă interfață, realizat de compania Philips pe platforma SmartMX, oferind aceleași caracteristici în modurile contact sau contactless ca toate celelalte produse dezvoltate pe această platformă.

Acest element securizat este dotat cu 160 Kbytes de ROM, 2608 bytes de RAM și 72 Kbytes de EEPROM, care poate fi folosit atât pentru stocarea datelor, cât și a programelor. Memoria non-volatilă constă din celule de memorie de mare fiabilitate care garantează integritatea datelor.

Funcționalitatea cipului este definită de utilizator din sistemul de operare înglobat, în mod contact (ISO/IEC 7816) sau în mod S^2C, ceea ce oferă același nivel de securitate, funcționalitate și flexibilitate pentru cele două interfețe. În telefoanele mobile, tehnologia S^2C asigură comunicația cu dispozitive NFC într-un mod securizat.

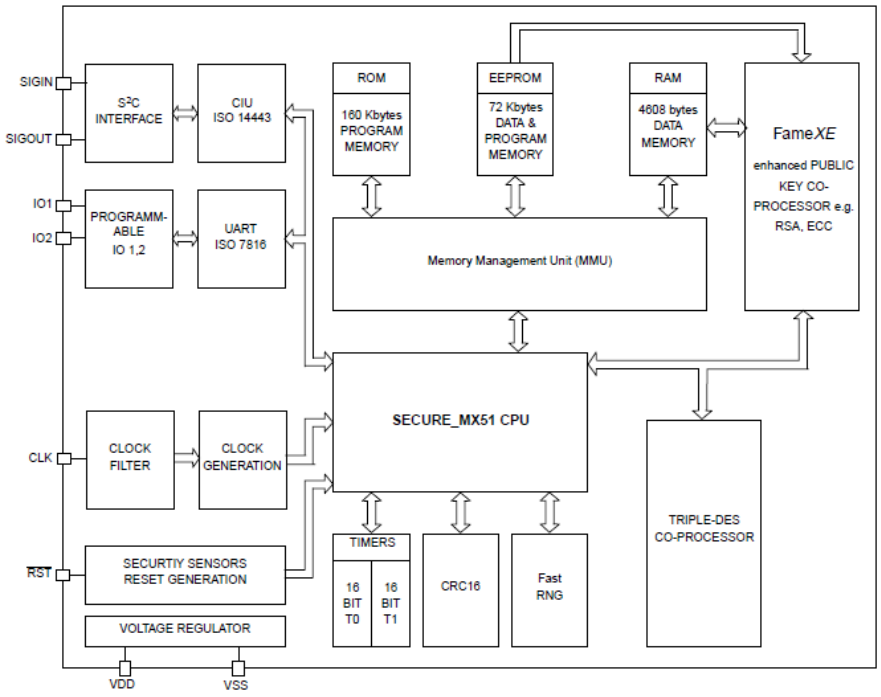


Figura 16: Diagrama bloc a P5CN072

Este conectată la unitatea internă de interfațare contactless (CIU) tip ISO 14443, care se ocupă cu modularea și demodularea semnalelor S^2C. Alimentarea P5CN072 cu energie electrică se realizează prin pinii V_{DD} și V_{SS}. În această configurație, elementul securizat este compatibil cu infrastructura existentă de cititoare tip MIFARE și poate să emuleze MIFARE 1K și 4K pentru integrare rapidă și compatibilitate cu MIFARE standard și carduri ProX.

Comunicația bidirecțională cu interfața de contact se realizează prin două porturi I/O seriale, al căror control se află la discreția aplicației software, care poate să stabilească politicile condiționale de acces a memoriei.

Partea hardware de pe cip este controlată prin Regiștrii cu Funcție Specială, care reflectă activitățile desfășurate de CPU, întreruperi, dispozitivele I/O, EEPROM etc.

P5CN072 oferă două moduri activabile software de economisire a energiei când activitatea este scăzută în intensitate: IDLE și SLEEP sau CLOCKSTOP.

Dispozitivul operează cu un voltaj singular de alimentare de 1,8V, 3V sau 5V), la o frecvență de tact externă de 10 MHz (intern, 30 MHz) ce este furnizată prin suprafața de contact.

6.4 PN65 (NXP)

PN65 reprezintă sistemul pe cip NFC + eSE utilizat în telefoanele Google Nexus S.

Modulul microcontroler este format dintr-un nucleu 80C51 core, 32 kbytes de ROM și 1 kbyte de RAM, ce rulează un firmware corespunzător modulului PN512 de transmisie de date contactless prin NFC (frecvența 13 MHz). Combinația dintre cele două module poartă termenul PN531.

Elementul securizat utilizat pe acest dispozitiv este P5CN072, prezentat în secțiunea anterioară. Există o interfață adițională și o stivă software specială pentru a putea utiliza și cardul SIM ca element securizat, ceea ce face necesar suportul protocolului SWP. Posibilitatea de a utiliza două elemente securizate impune ca software-ul ce rulează pe gazdă să aibă accesul de a trimite comenzi la NFC prin HCI, pentru a selecta elementul securizat dorit.

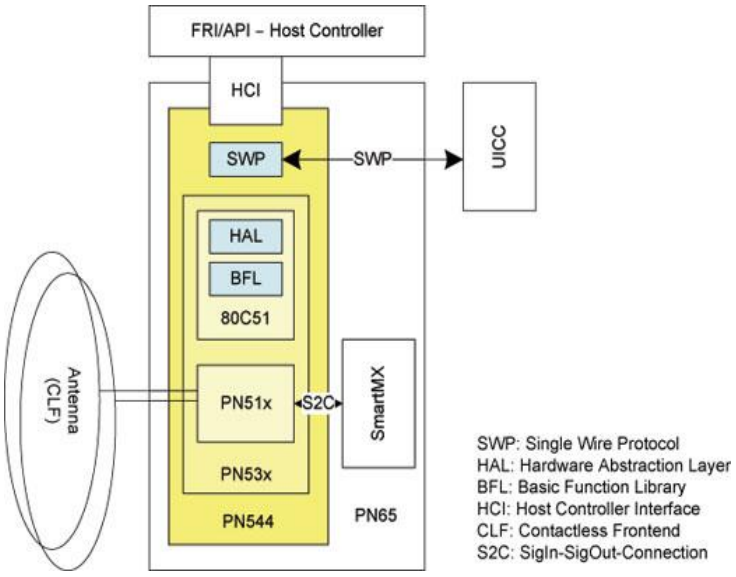


Figura 17: Diagrama bloc a sistemului PN65

7. Concluzii

Plata electronică, fidelizarea clienților și autentificarea securizată reprezintă o serie de aplicații digitale de actualitate care pot da un impuls semnificativ economiei de consum. Prezența acestora pe agenda publică este datorată unor progrese tehnologice recente în domeniul tehnologiei informației și telecomunicațiilor, și s-a materializat de curând în realitate cu ajutorul telefoanelor mobile, mai precis a capabilității de transmitere a datelor NFC și a sistemelor de calcul integrate de tip element securizat.

Elementul securizat este o componentă cheie în orice dispozitiv electronic destinat să vehiculeze informații confidențiale, precum date personale și conturi bancare. Această componentă a fost proiectată special pentru a servi drept un mediu complet securizat de stocare și transmitere a informațiilor confidențiale, precum și execuția de aplicații ce realizează operațiuni critice. Elementul securizat este dotat atât cu mecanisme de protecție software, la nivel de sistem de operare, ce asigură domenii de securitate separate și izolate pentru fiecare furnizor de servicii, dar și mecanisme de protecție hardware extreme, precum imposibilitatea de a detașa fizic memoria de stocare pentru citirea frauduloasă a conținutului său. Performanțele proclamate de producătorii de elemente securizate au fost confirmate de cei mai mari jucători de pe piața plăților, precum Mastercard, VISA, Google, Apple etc.

Furnizorii de servicii de plăți independenți au la dispoziție o multitudine de variante tehnice pentru a implementa propriile lor soluții pe un dispozitiv mobil cu combinația NFC-SE. Există mai mulți factori de formă ai elementului securizat și mai multe tipuri de magistrale ce pot asigura comunicarea cu dispozitivul gazdă pe de o parte, și cu frontendul de NFC pe de altă parte. În funcție de factorul de formă, apar provocări în legătura cu certificarea și autorizările ce trebuie obținute de la celelalte entități implicate, precum producătorul terminalului sau operatorul rețelei mobile. Una din probleme stringente ce trebuie adresate astăzi o reprezintă înlesnirea dezvoltării de soluții proprii fără implicarea părților terțe menționate anterior.

Integrarea elementelor securizate în aplicații are de suferit și din cauza lipsei de transparență asupra tehnologiilor implicate. Acest lucru este însă de înțeles, având în vedere ca multe din tehnicile de criptare și autentificare sunt proprietare și private, iar deschiderea lor ar crea tocmai vulnerabilitățile sistemice de securitate pe care încercăm să le ținem sub control. Cu toate acestea, adopția pe scară largă a elementelor securizate ar putea avea de câștigat de pe urma dezvoltării unui cadru de testare universal și abstractizat, ce ar putea fi folosit pentru prototipare rapidă a diferitelor aplicații.

Se constată faptul că elementele securizate sunt indispensabile aplicațiilor ce prezintă pentru utilizator riscul de a-i fi furată identitatea. Mulți producători de sisteme pe circuite integrate oferă deja spre comercializare astfel de soluții dedicate, iar producătorii de dispozitive mobile și operatorii telecom distribuie elemente securizate în produsele lor, dar își rezervă dreptul exclusiv de a-l folosi. În aceste condiții, furnizorii particulari de servicii pot întâmpina dificultăți în a-și construi propriile aplicații securizate, fără a încheia parteneriate cu deținătorii elementelor securizate sau fără a supune consumatorul la o oarecare scădere de confort în experiența de utilizare a propriului dispozitiv mobil.

8. Bibliografie

[1] NFC Secure Element Stepping Stones, version 1.0

[2] Reveilhac, M.; Pasquet, Marc, "Promising Secure Element Alternatives for NFC Technology," Near Field Communication, 2009. NFC '09. First International Workshop on , vol., no., pp.75,80, 24-24 Feb. 2009

[3] Roland, M.; Langer, J.; Scharinger, J., "Practical Attack Scenarios on Secure Element-Enabled Mobile Devices," Near Field Communication (NFC), 2012 4th International Workshop on , vol., no., pp.19,24, 13-13 March 2012

[4] Alimi, V.; Pasquet, Marc, "Post-Distribution Provisioning and Personalization of a Payment Application on a UICC-Based Secure Element," Availability, Reliability and Security, 2009. ARES '09. International Conference on , vol., no., pp.701,705, 16-19 March 2009

[5] Roland, Michael, Josef Langer, and Josef Scharinger. "Relay Attacks on Secure Element-Enabled Mobile Devices." Information Security and Privacy Research. Springer Berlin Heidelberg, 2012. 1-12.

[6] Jara, Antonio J., Miguel A. Zamora, and Antonio FG Skarmeta. "Secure use of NFC in medical environments." RFID Systems and Technologies (RFID SysTech), 2009 5th European Workshop on. VDE, 2009.

[7] Monteiro, David M., Joel JPC Rodrigues, and Jaime Lloret. "A secure NFC application for credit transfer among mobile phones." Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on. IEEE, 2012.

[8] Vanderhoof, Randy. "Applying the NFC Secure Element in Mobile Identity Apps." RSA2012.