

Cardholder verification

raport

Structura

Proiectul contine componentele:

1. Java Card Applet - Sample Wallet modificat astfel incat sa accepte o noua metoda - getCardHolderMethods() ce returneaza o lista de Card Verification Methods suportate de applet.
2. Terminal - Aplicatie scrisa in Java ce comunica cu applet-ul prin intermediul pachetului com.sun.javacard.apduio. Aplicatia deschide simulatorul (cref_t0.exe) unde instaleaza Applet-ul pentru a putea face tranzactiile si verificarile ulterioare.

Logica

Applet-ul Java Card este un proiect default Java Card modificat corespunzator cerintelor proiectului. Acesta are definit un INS additional pentru a suporta metoda ceruta.

```
final static byte GET_CARDHOLDER_METHODS = (byte) 0x70;
switch (buffer[ISO7816.OFFSET_INS]) {
case GET_BALANCE:
    getBalance(apdu);
    return;
case DEBIT:
    debit(apdu);
    return;
case CREDIT:
    credit(apdu);
    return;
case VERIFY:
    verify(apdu);
    return;
case GET_CARDHOLDER_METHODS:
    getCardHolderMethods(apdu);
    return;
default:
    ISOException.throwIt(ISO7816.SW_INS_NOT_SUPPORTED);
}
```

Aceasta functie are forma:

```
private void getCaldHolderMethods(APDU apdu) {
    byte[] buffer = apdu.getBuffer();
    short le = apdu.setOutgoing();
    apdu.setOutgoingLength((short) cvm_list.length);
    for(byte i=0;i < cvm_list.length; i++) {
        buffer[i] = cvm_list[i];
    }
    apdu.sendBytes((short)0, (short)cvm_list.length);
}
```

Primește drept argument APDU și prin intermediul buffer-ului trimite către Terminal cvm_list.

Lista de Card Verification Methods este:

```
final byte[] cvm_list = {0x32, 0x00, 0x01, 0x07, 0x1F, 0x00};
```

Primul byte reprezintă X-ul (valoarea tranzacției), al doilea reprezintă Y-ul (al doilea byte din valoarea tranzacției în cazul în care este necesar).

Următorii bytes sunt perechi de forma (B1,B2) unde b1 este un CVM Code iar b2 este un CVM Condition Code.

În cazul nostru avem X=50, Y=0, B1=0x01 (00000001 - Fail if CVM not successful & Require Plaintext PIN), B2=0x07 (07 - If transaction > X), B1= 0x1F(no cvm required), B2=0x00(always).

Aceste CVM codes sunt înregistrate pe card și trebuie respectate de aplicația Terminal.

Terminalul este inițializat cu următoarele funcții:

```
public static void main(String[] args) {
    openCref();
    createConnection();
    startTerminal();
    setupWallet();
    getBankCVM();
    getBalance();
    startTransactions();
    getBalance();
    stopTerminal();
}
```

- openCref() - deschide simulatorul unde trebuie instalat Applet-ul.
- createConnection() - deschide un Socket la portul 9025 pentru a se conecta cu simulatorul.

- `startTerminal()` - porneste simulatorul prin intermediul metodei `powerUp()`
- `setupWallet()` - parcurge o un array ce contine liste de bytes preluati din cad-wallet.scr ce au ca scop instalarea Applet-ului pe simulator
- `getBankCVM()` - realizeaza un request catre Applet cu INS-ul 0x70 si primeste lista CVM.
- `getBalance()` - realizeaza un call pentru a verifica balanta cardului (initial este initializat cu 200 RON)

Daca toti pasii au fost indepliniti cu succes pana in acest moment se trece la partea de tranzactii. Metoda `startTransactions()` intra intr-un loop in care citeste de la tastatura valoarea tranzactiei.

Valoarea tranzactiei este apoi analizata in functie de lista de CVM primita iar in cazul in care valoarea acesteia depaseste 49 RON, este cerut PIN-ul.

Verificarea PIN-ului se face convertind string-ul de numere in numere separate. Apoi aceste numere sunt convertite in bytes si in functie de cate numere sunt se trimite comanda de verificare a PIN-ului catre Applet. Daca raspunsul primit este diferit de SW1: 0x90 SW2: 0x00, inseamna ca PIN-ul a fost introdus incorect si se cere reintroducerea acestuia pana la 3 ori. Daca PIN-ul a fost introdus gresit de 3 ori tranzactia nu mai are loc.

Dupa finalizarea cu succes a tranzactiei se face `getBalance()` din nou pentru a se verifica tranzactia efectuata si apoi se opreste simulatorul.

Cazuri de testare

Testarea se face din consola introducand valoarea debitata urmatoare, daca este necesar, de introducerea pin-ului. Acestea sunt testele realizate:

```
<terminated> Terminal [Java Application] C:\Program Files\Java\jdk-11.0.6\bin\javaw.exe (May 13, 2020, 1:09:01 PM – 1:09:08 PM)
cref_t0.exe a fost deschis.
Conexiune realizata cu succes la applet.
Terminalul a fost pornit cu succes.
Setup wallet complet.
Get Cardholder CVM apelat cu succes.
Balanta curenta a contului 200
Introdu valoarea tranzactiei:
50
Te rog introdu PIN-ul:
123
Pin incorect.
Te rog introdu PIN-ul:
1234
Pin incorect.
Te rog introdu PIN-ul:
1
Pin-ul a fost introdus de mai mult de 3 ori incorect. Tranzactia se anuleaza.
Pin incorect.
Balanta curenta a contului 200
Terminalul a fost oprit cu succes.
```

Fig 1.0 - Eroare la tranzactie in valoare de 50 RON datorita introducerii PIN-ului incorect.

```
<terminated> Terminal [Java Application] C:\Program Files\Java\jdk-11.0.6\bin\javaw.exe (May 13, 2020, 1:09:15 PM – 1:09:20 PM)
cref_t0.exe a fost deschis.
Conexiune realizata cu succes la applet.
Terminalul a fost pornit cu succes.
Setup wallet complet.
Get Cardholder CVM apelat cu succes.
Balanta curenta a contului 200
Introdu valoarea tranzactiei:
49
Debitarea s-a realizat cu succes
Balanta curenta a contului 151
Terminalul a fost oprit cu succes.
```

Fig 1.1 - Tranzactie ce nu necesita introducere PIN-ului.

```
<terminated> Terminal [Java Application] C:\Program Files\Java\jdk-11.0.6\bin\javaw.exe (May 13, 2020, 1:09:26 PM – 1:09:32 PM)
cref_t0.exe a fost deschis.
Conexiune realizata cu succes la applet.
Terminalul a fost pornit cu succes.
Setup wallet complet.
Get Cardholder CVM apelat cu succes.
Balanta curenta a contului 200
Introdu valoarea tranzactiei:
50
Te rog introdu PIN-ul:
123
Pin incorect.
Te rog introdu PIN-ul:
12345
Pin confirmat cu succes.
Debitarea s-a realizat cu succes
Balanta curenta a contului 150
Terminalul a fost oprit cu succes.
```

Fig 1.2 - Tranzactie ce necesita introducere PIN-ului.

```
Terminal [Java Application] C:\Program Files\Java\jdk-11.0.6\bin\javaw.exe (May 13, 2020, 1:14:06 PM)
cref_t0.exe a fost deschis.
Conexiune realizata cu succes la applet.
Eroare la deschiderea terminalului.
Eroare la instalarea applet-ului.
Eroare la preluarea CVM-ului bancii
Eroare la preluarea balantei.
```

Fig 1.3 - Eroare la deschiderea terminalului;