Cardholder Verification

Bita Mihai-Alexandru, B3

1 Structura aplicatiei

Aplicatia este structurata pe doua programe:

1. programul terminal
2. applet-ul Java Card

Programul terminal este cel care se ocupa de pornirea cref-ului (simulatorul platformei Java Card), instalarea Smart Card-ului si comunicarea cu acesta, precum si procesarea comenzilor initiate de Cardholder (*vizualizare sold*, *creditare*, *debitare*).

Applet-ul Java Card implementeaza functionalitatea unui Smart Card. Pe langa operatiile clasice de *vizualizare sold*, *creditare*, *debitare* si *verificare PIN*, acesta prezinta atat o lista de CVMs (Cardholder Verification Methods) cat si o functie responsabila pentru transmiterea acestei structuri.

```
54    public static void main(String[] args) {
55        Terminal terminal = new Terminal();
56
57        boolean connected = false;
58        while (!connected) {
59            try {
60                // initializare simulator
61                terminal.Start();
62                terminal.Connect();
63
64                // initializare card
65                terminal.Install();
66                terminal.Create();
67                terminal.Select();
68                terminal.GetCVM();
69
70                // interactiune cu cardholder-ul
71                terminal.Input();
72
73                terminal.Close();
74
75                connected = true;
76            } catch (IOException | CadTransportException e) {
77                System.out.println(e);
78            }
79        }
80    }
```

Figure 1: Structura terminalului

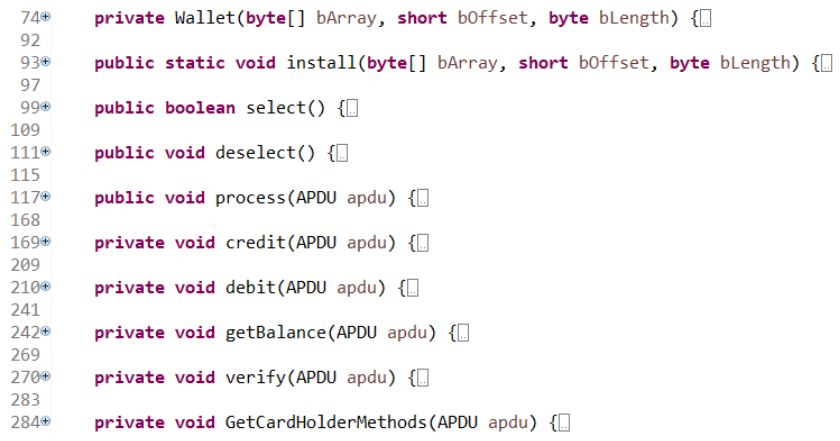

Figure 2: Structura applet-ului

2 Logica si implementarea

Lista de CVMs este implementata pe card sub forma unui tablou de bytes ce urmeaza sablonul <campul numeric V1>, <campul numeric V2>, <cod CVM_1>, <cod conditie_1>, <cod CVM_2>, <cod conditie_2>. Functia GetCardHolderMethods seteaza un buffer de 6 bytes si il umple in ordine cu fiecare element din lista de CVMs inainte de a-l trimite.

In programul terminal, functia Install parseaza linie cu linie din script-ul generat de applet si proceseaza, in ordine, fiecare comanda apdu prin intermediul functiei Process care ia ca parametru un string si construieste campurile de bytes necesare configurarii unei structuri apdu pentru a-l transmite simulatorului.

Functia GetCVM compune comanda necesara apelului GetCardHolderMethods si o transmite ca parametru functiei Process. Raspunsul primit este salvat intr-un tablou bidimensional in care fiecare element este compus dintr-o pereche (cod CVM, cod conditie), iar valorile "V1" si "V2" sunt retinute separat.

Input-ul Cardholder-ului este preluat in mod continuu prin functia Input pana la comanda "exit". Comenzile permise sunt "balance", "credit <suma>" si "debit <suma>". Fiecare comanda este procesata in functia Action. Pentru "balance" si "credit" se compune sirul de bytes comenzii respective si se transmit ca paremetru catre functia Process.

Pentru "debit" se apeleaza intai functia Verify pentru realizarea procedurii de verificare. Astfel, programul itereaza in ordine prin lista de CVMs a cardului obtinuta din pasii anteriori si efectueaza urmatorii pasi:

1. *verifica daca este acceptat codul de conditie, in caz contrar trece la iteratia urmatoare
2. verifica daca este indeplinita conditia, in caz contrar trece la iteratia urmatoare
3. *verifica daca este acceptat codul CVM, in caz contrar trece la iteratia urmatoare
4. aplica procedura CVM, in caz de esec se analizeaza bitul 7 al codului CVM: daca este setat pe 1 se trece la iteratia urmatoare, altfel daca bitul 7 este setat pe 0 sau lista de CVMs a fost epuizata atunci procedura se incheie prin esec

** verificarea presupune cautarea codurilor respective in listele terminalului: doua tablouri de bytes reprezentand codurile CVM, respectiv codurile de conditie acceptate de terminal*

Pentru CVM-ul "Plaintext PIN verification performed by SC" terminalul cere Cardholder-ului sa introduca PIN-ul. Odata preluat, se construieste si se proceseaza comanda pentru verificarea PIN-ului (in plaintext) de catre Smart Card. In cazul in care Smart Card-ul raspunde cu 0x9000, atunci PIN-ul introdus de catre Cardholder corespunde cu cel al cardului iar verificarea se incheie cu succes, in caz contrar verificarea esueaza.

Daca procedura a esuat, operatiunea de "debit" nu este efectuata.

3 Testarea aplicatiei

In cele ce urmeaza sunt prezentate o serie de cazuri de test in care soldul actual este 100 (0x64):

1. atat codurile CVM cat si codurile de conditie prezente pe card sunt acceptate de terminal

   (a) valoarea tranzactiei < 50

```
> debit 30
<trimis> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 1e, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 1e, Le: 00, SW1: 90, SW2: 00
Operatiunea de debitare a fost efectuata cu succes!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 46, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 70
```

Figure 3: Rezultatul testului 1(a)

   (b) valoarea tranzactiei ≥ 50

```
> debit 60
PIN: 12345
<trimis> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 01, 02, 03, 04, 05, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 01, 02, 03, 04, 05, Le: 00, SW1: 90, SW2: 00
Operatiunea de verificare PIN a fost efectuata cu succes!
<trimis> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 3c, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 3c, Le: 00, SW1: 90, SW2: 00
Operatiunea de debitare a fost efectuata cu succes!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 28, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 40
```

Figure 4: Rezultatul testului 1(b), PIN corect

```
> debit 60
PIN: 54321
<trimis> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 05, 04, 03, 02, 01, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 05, 04, 03, 02, 01, Le: 00, SW1: 63, SW2: 00
Operatiunea de verificare PIN a esuat.
PIN incorect!
PIN: exit
Nu s-a putut efectua operatiunea de debit. Verificarea identitatii a esuat!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 64, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 100
```

Figure 5: Rezultatul testului 1(b), PIN gresit

2. codul No CVM required prezent pe card nu este acceptat de terminal **SAU** codul 06 (valoarea tranzactiei < V1) prezent pe card nu este acceptat de terminal

   (a) valoarea tranzactiei < 50

```
> debit 30
Nu s-a putut efectua operatiunea de debit. Verificarea identitatii a esuat!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 64, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 100
```

Figure 6: Rezultatul testului 2(a)

   (b) valoarea tranzactiei ≥ 50

```
> debit 60
PIN: 12345
<trimis> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 01, 02, 03, 04, 05, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 01, 02, 03, 04, 05, Le: 00, SW1: 90, SW2: 00
Operatiunea de verificare PIN a fost efectuata cu succes!
<trimis> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 3c, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 3c, Le: 00, SW1: 90, SW2: 00
Operatiunea de debitare a fost efectuata cu succes!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 28, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 40
```

Figure 7: Rezultatul testului 2(b), PIN corect

```
> debit 60
PIN: 54321
<trimis> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 05, 04, 03, 02, 01, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 20, P1: 00, P2: 00, Lc: 05, 05, 04, 03, 02, 01, Le: 00, SW1: 63, SW2: 00
Operatiunea de verificare PIN a esuat.
PIN incorect!
PIN: exit
Nu s-a putut efectua operatiunea de debit. Verificarea identitatii a esuat!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 64, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 100
```

Figure 8: Rezultatul testului 2(b), PIN gresit

3. codul Plaintext PIN verification performed by SC prezent pe card nu este acceptat de terminal **SAU** codul 09 (valoarea tranzactiei > V2) prezent pe card nu este acceptat de terminal

   (a) valoarea tranzactiei < 50

```
> debit 30
<trimis> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 1e, Le: 7f, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 40, P1: 00, P2: 00, Lc: 01, 1e, Le: 00, SW1: 90, SW2: 00
Operatiunea de debitare a fost efectuata cu succes!
> balance
<trimis> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, SW1: 00, SW2: 00
<primit> CLA: 80, INS: 50, P1: 00, P2: 00, Lc: 00, Le: 02, 00, 46, SW1: 90, SW2: 00
Operatiunea de verificare sold a fost efectuata cu succes! Sold curent: 70
```

Figure 9: Rezultatul testului 3(a)

   (b) valoarea tranzactiei ≥ 50

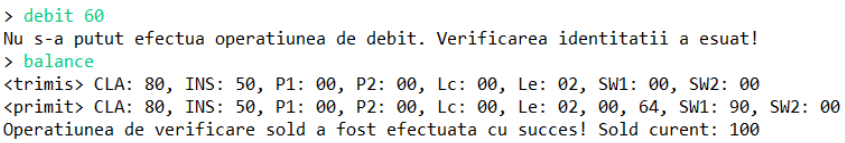

Figure 10: Rezultatul testului 3(b)

4. niciunul din cele doua coduri CVM prezente pe card nu este acceptat de terminal **SAU** niciunul din cele doua coduri de conditie prezente pe card nu este acceptat de terminal

   (a) valoarea tranzactiei < 50

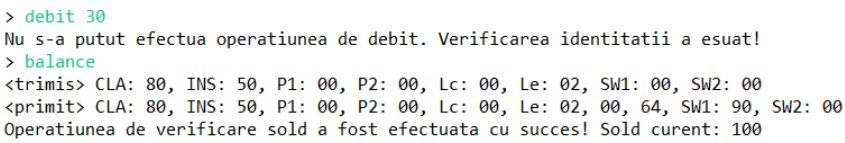

Figure 11: Rezultatul testului 4(a)

   (b) valoarea tranzactiei ≥ 50

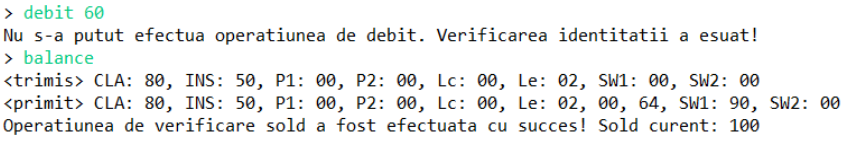

Figure 12: Rezultatul testului 4(b)