Secure Protocol in Identity Management Systems using Smart Cards

Prep. Cristian Valeriu TOMA
Catedra de Informatică Economică, A.S.E. Bucureşti
cristian.toma@ie.ase.ro

Almost everyone has multiple identification cards (IDs), issued by multiple public and private organizations. Such IDs include driver's licenses, membership cards, credit cards, and corporate identification papers/cards. Organizations that need to verify identities find very important the concern regarding privacy and the protection of personal information. So, identity management ant contact-less communication feature is an important tool in any kind of information system, including e-business, e-payment, military systems and energetic sector. In order to fulfill those security requirements of such complex systems, the public and private institutions reshape and rethink identity management systems.
Keywords: *identity management systems, digital signature, smart cards.*

1 Introducere

Necesitatea controlului accesului uman în sistemele informatice a condus la adoptarea pe scară din ce în ce mai largă a tehnologiilor de tip card. Cardurile existente se clasifică în carduri cu bandă magnetică şi cele smart, inteligente. La rândul lor cardurile inteligente se clasifică în funcţie de mai multe criterii. De exemplu, după modul în care interacţionează cu cititorul de carduri – card reader, sunt carduri: conatctless – comunică cu cititorul de carduri prin unde radio, contact – are contact fizic cu cititorul de carduri sau hibride.

Conform standardului ISO/IEC 7816 elaborat de Joint Technical Committee 1 (JTC1) al International Standards Organization (ISO) şi de International Electronic Committee (IEC) în 1987 şi actualizat în 2003, un smart card – card inteligent este o cartelă de plastic ce conţine un circuit integrat.

În funcţie de tipul circuitul integrat folosit apare o nouă clasificare a cardurilor inteligente, astfel există:

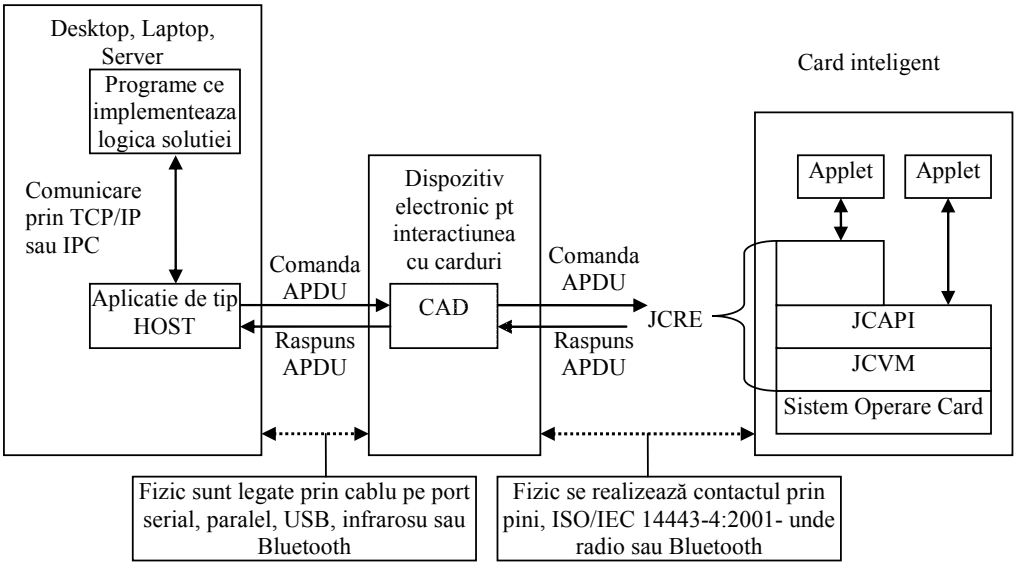
- *Carduri cu circuit integrat microprocesor*, sau pe scurt chip cards, conţine un microprocesor care îi permite să efectueze operaţii complicate computaţional. Un astfel de card conţine pe lângă microprocesorul de 8, 16 sau chiar 32 de biţi şi unul sau mai multe chipuri de memorie, care în mod uzual asigură 16 sau 32 KB memorie de tip read-only, şi 1MB memorie cu acces aleator – RAM. Aceste caracteristici oferă unui astfel de card puterea echivalentă cu un computer original IBM-XT. Chip card-urile sunt folosite în diverse sisteme informatice, începând de la carduri de credit bancar, card-uri pentru controlul accesul la resursele unei reţele de echipamente electronice şi terminând cu SIM-uri pentru telefoane mobile şi carduri pentru accesul la pachet de programe TV digitale.
- *Carduri cu circuit integrat memorie*, ce pot deţine diferite informaţii dar nu pot prelucra informaţiile stocate local pentru că nu are un microprocesor. Din această cauză ele sunt dependente de cititorul de carduri. Ele reprezintă alternativa puţin costisitoare pentru carduri cu bandă magnetică. O altă alternativă dar mai costisitoare o reprezintă cardurile optice. Momentan acestea nu conţin un microprocesor şi nu folosesc un protocol standard pentru comunicarea cu cititorul de card-uri.

În comunitatea ştiinţifică se conturează ideea că un card inteligent, este doar acel card care poate executa calcule computaţionale. Cu alte cuvinte sunt considerate carduri inteligente doar acele carduri care conţin un microprocesor. În acest sens, diferenţa între un card şi un card inteligent este că acesta din urmă conţine un microprocesor care îi permite să efectueze operaţii complicate computaţional, pe când cel cu bandă magnetică poate fi folosit

doar pentru stocare informații. Un card inteligent conține pe lângă microprocesorul de 8, 16 sau chiar 32 de biți și unul sau mai multe chipuri de memorie, prin care se pot oferi 16KB de memorie de tip read-only și 4MB de memorie cu acces aleator.

2. Aplicații complete pentru tehnologia Java Smart Card

O aplicație Java card se referă la un applet care rulează pe cardul inteligent. Dar acest applet de cele mai multe ori are nevoie să interacționeze cu diverse sisteme și aplicații. Astfel, în literatura de specialitate s-a consacrat termenul de aplicație Java card completă pentru o suită de programe care cooperează împreună cu appletul de pe card pentru a oferi un serviciu către utilizatorul final. În figura 1 este prezentată o aplicație Java card completă:



Legenda:

JCVM=Java Card Virtual Machine
JCAPI=Java Card Advanced Programming Interface
JCRE =Java Card Runtime Environment
CAD=Card Acceptance Device
IPC=Inter-Process Communication
APDU=Application Protocol Data Unit

Fig. 1. Aplicație Java card completă.

De exemplu într-un sistem informatic ce folosește carduri inteligente o aplicație Java card completă se consideră:

- Aplicațiile de tip Back-end – cele care au legătură cu serverele de baze de date, cele care în mare măsură implementează logica serviciului;
- Aplicațiile de tip host sau off-card – cele care comunică cu cititorul de carduri, adică sunt interfața între aplicațiile Back-end și cititorul de carduri. Aceste aplicații pot rula pe desktopul la care este conectat cititorul de carduri, pot rula pe un terminal specializat cum ar fi ATM-Automatic Teller Machine sau pot rula pe un telefon mobil în cazul în care acesta joacă rol de cititor de carduri inteligente;
- Aplicațiile Card Reader – cele care rezidă în cititorul de carduri și sunt responsabile de coordonarea și realizarea interacțiunii cu aplicațiile de pe card. În literatura de specialitate, echipamentul fizic, cititorul de carduri, plus aplicațiile ce rulează pe el, tot acest ansamblu este denumit CAD – Card Acceptance Device. CAD-ul este responsabil de cum realizează conexiunea fizică cu cardul, prin unde radio sau prin contact electric, și totodată CAD-ul este responsabil și de alimentarea cardului cu energie. De asemenea, CAD-ul preia comenzile – APDU-Application Protocol Data Unit, înșiruiri standard de octeți – de la aplicațiile de tip host și le translatează către cardurile fizice;
- Aplicațiile de pe cardul inteligent – în

platforma java card pot coexista mai multe aplicații, appleturi. Appleturile sunt rulate în JCRE – Java Card Runtime Environment.
Există trei modele prin care se comunică între aplicația host şi appletul Java. Primul model este destul de simplu şi presupune trasmiterea şi receptarea de mesaje tipice de un anume format – *Message-Passing Model*. Al doilea model este *Java Card Remote Method Invocation – JCRMI*, care este un set de clase şi proceduri asemănătoare cu cele din modelul J2SE – Java 2 Standard Edition RMI, iar la bază foloseşte primul model. Un al treilea model prin care se poate realiza comunicația între aplicația host şi aplicația de pe card, din punct de vedere al dezvoltatorilor de aplicații pentru smart card-uri, este SATSA – Security and Trust Services API. SATSA este definit în JSR 177, permite dezvoltatorilor la bază să folosească oricare din cele două modele – Message-Passing Model sau JCRMI, dar este un API mult mai abstract bazat pe GFC – Generic Connection Framework API.

3. Obiective şi avantaje ale sistemelor pentru managementul identității

În viziunea specialiştilor managementul, identității – Identity Management –reprezintă un sistem de tehnologii, practici, politici si legi care îndeplinesc următoarele deziderate:

- Asigură identificarea unică la nivel de tranzacție în sistemele publice, guvernamentale şi private;
- Reduce costurile accesului şi/sau îmbunătățeşte calitatea serviciilor guvernamentale;
- Asigură securitatea publicului;
- Păstrează sau îmbunătățeşte dreptul la libertățile în ce priveşte intimitatea si securitatea informațiilor despre identitate.

În acest moment fiecare companie privată sau instituție publică are propriul sistem de management al identității indiferent că este vorba de o un sistem informatic simplu ori complex, sau este vorba de asigurarea unui flux informațional securizat.
Ca şi avantaje ale utilizării sistemelor de management al identității în sectorul privat se enumera:

- Eficiența organizațională – activează tranzacțiile şi comunicările inter-umane;
- Avantaj Competitiv – se capturează noi disponibilități de piață, îmbunătățind poziția companiei față de competitori;
- Securitate – controlează accesul autorizat şi previne accesul neautorizat la informații şi servicii;
- Viteză de reacții la schimbare – nu trebuie regândit un alt mod de autentificare când au loc modificări structurale şi de resurse umane;
- Prevenirea fraudelor – este greu de cuantificat această caracteristică dar în timp se pot observa absențele fraudelor şi anomaliilor;
- Consistent Treatment of the Individual. "End-to-end" management of employees, "single view of the customer," "joined-up government.";
- Asigură infrastructura de informații integrata.

În practică, cele mai cunoscute sisteme de management al identității sunt:
Microsoft Passport .NET şi Liberty Alliance.

4. Protocol pentru realizarea schimbului de mesaje securizat

În această secțiune se propune un protocol pentru realizarea schimbului de mesaje în afara unui sistem de management al identității. Desigur, protocolul se foloseşte şi în interiorul unui sistem de management al identității dar cu diferite grade de aplicare.
Înainte de a fi explicat, se recomandă însuşirea sistemelor criptografice cu chei simetrice şi cu chei asimetrice [BRUC96], [IVAN02]. Asupra datelor care urmează să fie folosite într-un sistem criptografic, se pot aplica diverse operații. Una din ele, care asigură un grad satisfăcător de securitate, şi este folosită atât la criptare cât şi la semnare digitală este PCBC – Propagation Cipher Block Chaining – figura 2.

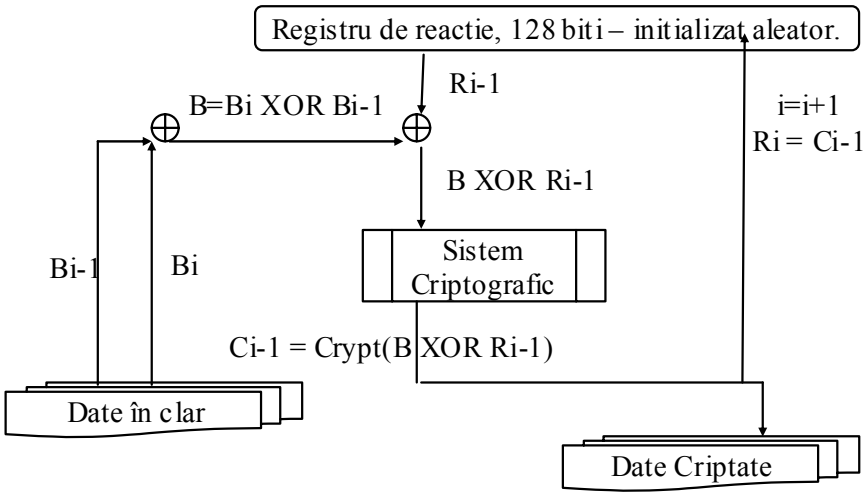


Fig. 2. PCBC.

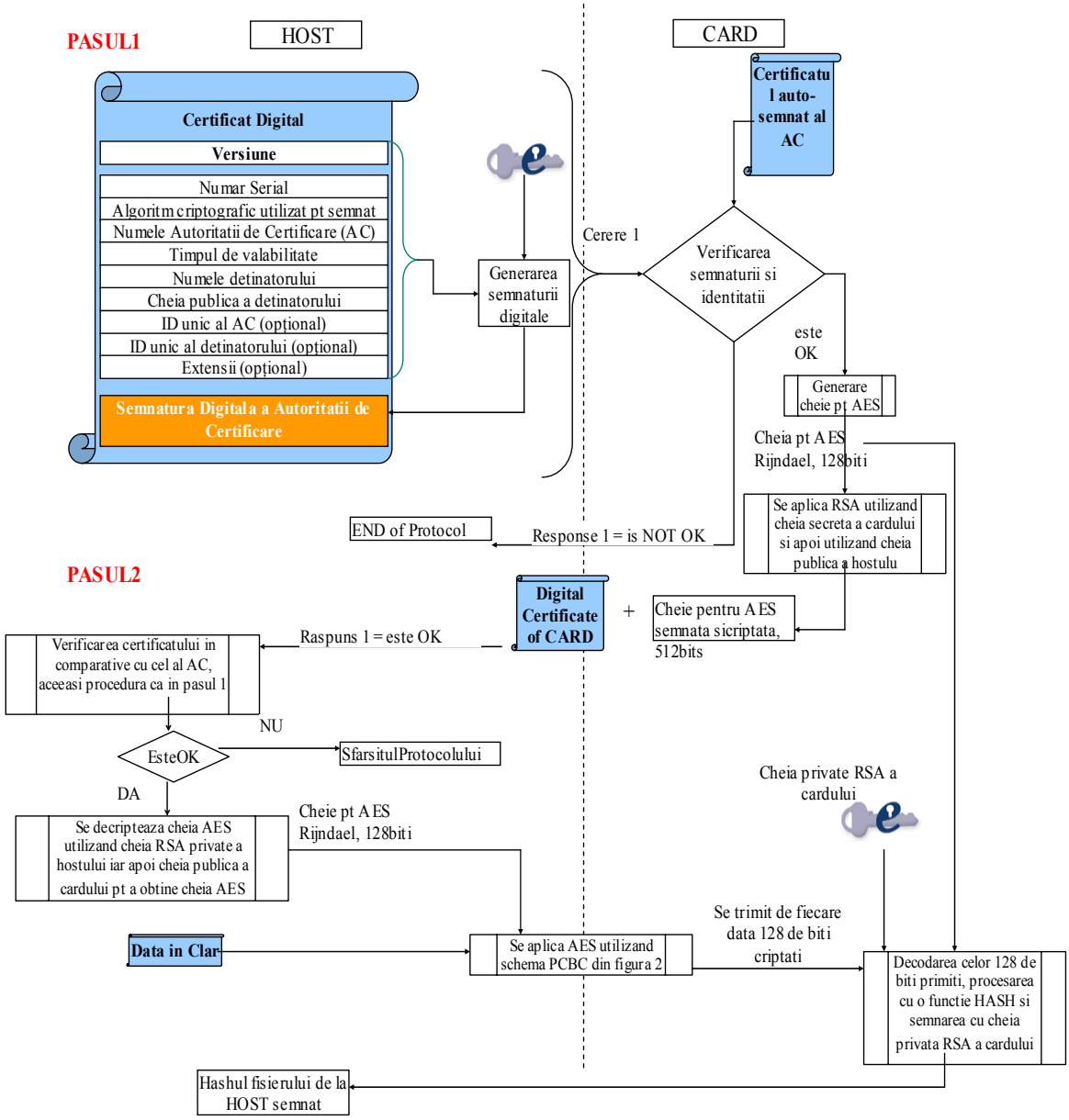


Fig. 3. CSCCP descriere generală.

Pentru schema PCBC din figura 2 sunt câteva implementări. Una din implementări presupune ca şi registrul de iniţializare şi algoritmul criptografic să rezide pe smart card. Altă implementare forţează ca pe card să existe doar algoritmul criptografic iar celelalte elemente să se ruleze la host. Indiferent de tipul implementării, schema presupune parcurgerea unor paşi simpli. Sunt luate 2 blocuri de 128 de biţi fiecare – 16 octeţi – din datele în clar şi asupra lor se aplică operaţia de XOR pe biţi. Rezultatul este combinat cu XOR pe 128 de biţi cu un registru de reacţie ce conţine o valoare aleatoare, apoi ce se obţine devine intrare pentru sistemul criptografic ales. Biţi obţinuţi din aplicarea sistemului criptografic, sunt biţi criptaţi şi totodată ei devin nouă valoare pentru registrul de reacţie. Parcurgerea inversă a schemei din figura 2 asigura descifrarea corectă a datelor criptate.
În figura 3 se propune un protocol criptografic – Crypto Smart Card Communication Protocol – CSCCP folosit pentru a implementa semnătura digitală asupra oricăror tipuri de date în orice fel de sistem informatic – cu sau fără sistem de management al identităţii. Protocolul din figura 3 este autodescriptiv, iar mai multe detalii se obţin de la autori. Desigur, protocolul are aplicabilitate în sisteme informatice bancare, financiare, militare si energetice.

Concluzii

Dorinţa de a utiliza sisteme deschise, sigure şi fără o multitudine de proceduri de autentificare „single sign-on", forţează adoptarea unor sisteme securizate pentru managementul identităţii. Integrarea tehnologiilor smart card în astfel de abordări, asigură creşterea gradului de securitate şi fiabilitate în sistemele pentru managementul identităţii.
Impactul sistemelor de management al identităţii la nivelul companiilor din sectorul privat şi instituţiilor publice a sistemului de management al identităţii este clar: „Se reuşeşte o securizare a identităţii astfel încât persoanele autorizate vor accesa resursele şi informaţiile din domeniul de competenţă in maniera cea mai eficient posibilă".

Bibliografie

[BRUC96], Bruce Schneier, „Applied cryptography", John Weily & Sons Publishing House, USA, 1996.
[CHEN00], Zhiqun Chen, „Java Card Technology for Smart Cards: Architecture and Programmer's Guid", Editura Addison Wesley, USA, iunie 2000.
[ENRI03], C. Enrique Ortiz, Septembrie 2003, articol on-line: http://developers.sun.com/techtopics/mobility/javacard/articles/javacard2/
[IVAN02], Ion Ivan, Paul Pocatilu, Marius Popa, Cristian Toma, "The Digital Signature and Data Security in e-commerce", Revista Informatică Economică Nr. 3/2002, Bucharest 2002.
[JCDT04a], Sun Java Card Development Toolkit 2.2.1: http://java.sun.com/products/javacard/dev_kit.html
[MANU03], Manualul Programatorului, Octombrie 2003, Application Progaming Notes 2.2.1 incorporat in [JCDT04a]
[MANU03a], Manualul utilizatorului, Octombrie 2003, Development Kit User Guide 2.2.1 incorporat in [JCDT04a]
[SCTI98], Scott Guthery, Tim Jurgensen, „Smart Card Developer's Kit", Editura Macmillan Computer Publishing, ISBN: 1578700272, USA 1998: http://unix.be.eu.org/docs/smart-card-developer-kit/ewtoc.html