

## **ETAPA DE EXECUȚIE NR. 1**

### **CU TITLUL „Fundamentarea soluției pentru platforma informatica PLATSEC”**

#### **Obiectivele Etapei de Executie**

Etapa I a proiectului își propune îndeplinirea următoarelor obiective generale:

- I.** Elaborarea unui studiu de soluție pentru managementul securizat al datelor personale ale cetățenilor pe baza cartii de identitate electronice, prin definirea cadrului general de proiectare și operare a sistemelor integrate ce folosesc cardul de identitate electronic.
- II.** Elaborarea unui studiu tehnic pentru soluția de management securizat al datelor personale ale cetățenilor pe baza cartii electronice de identitate, prin definirea arhitecturii generale a sistemului și definirea unor clase de aplicații specifice.

Îndeplinirea acestor obiective este realizată în cadrul celor două activități ale etapei, care se finalizează în:

- I.** Raportul de cercetare privind sistemele informatice existente la nivel internațional și a standardelor actuale în domeniu
- II.** Studiul tehnic pentru soluția de management securizat al datelor personale ale cetățenilor pe baza cartii electronice de identitate.

## Rezumatul Fazei

În cadrul acestei faze a proiectului sunt prezentate principalele concepte ale sistemelor bazate pe utilizarea cardurilor electronice de identitate și este fundamentată o arhitectura generală a sistemului propus prin definirea principalelor clase de aplicații ce vor fi implementate în cadrul proiectului.

Obiectivele etapei au fost realizate prin baleierea literaturii de specialitate din domeniu la care s-au adăugat eforturile proprii de cercetare. Autorii speră că și-au adus contribuția la conturarea unei metodologii generale de abordare a unui sistem integrat de tranzacții electronice având la baza tehnologii avansate ce folosesc smart card-uri, care să armonizeze tendințele actuale manifestate la nivel național și European, studiile referindu-se la:

- analiza infrastructurii necesare pentru emiterea și gestionarea cardurilor electronice de identitate;
- identificarea cerințelor aplicațiilor potențiale la nivel guvernamental, administrativ, medical și bancar;
- analiza cerințelor specifice ale aplicațiilor și sistemelor integrate ce urmează să utilizeze cardul de identitate;
- interoperabilitatea cu sisteme integrate de servicii similare, implementate la nivel european.

Pornind de la cerințele comune ale aplicațiilor din domeniile menționate anterior în materie de infrastructură și servicii, s-a conturat un cadru general de folosire a smart-card-urilor și a infrastructurilor PKI în sfera sectoarelor publice. Acest cadru general cuprinde definirea principalilor actori în procesele de emitere, manipulare și revocare a smart-cardurilor și a certificatelor digitale. Fiecare actor are asociate diferite roluri, sarcini și drepturi.

Pentru a asigura securitatea datelor înscrise pe card, s-au definit două categorii de actori: cei abilitați să citească datele de pe card și cei care au dreptul de scriere/actualizare a informațiilor. Astfel, în cadrul fiecărei aplicații de pe card, corespunzător fiecăruia din cele două roluri, vor exista autorități de certificare separate. Actualizarea datelor se va putea realiza numai în prezenta acelor carduri care au certificate emise de autoritatea de certificare pentru scriere.

Pornind de la rezultatele raportului de cercetare corespunzător primei activități a etapei s-a realizat un studiu tehnic în care sunt propuse o arhitectura a sistemului ce va utiliza cartea electronică de identitate și s-au definit următoarele clase de aplicații:

- carte electronica de identitate pentru cetateni (autentificare si semnatura digitala calificata);
- stocare sigura informatii confidentiale (dosar medical, reteta medicala);
- servicii administrative (completarea automata a formularelor, rambursarea automata a serviciilor medicale)
- aplicatii de verificare a identitatii folosind mecanisme biometrice (verificare de tip „match-on-card”).

Ulterior acestei etape, se vor realiza specificatii pentru alte aplicatii precum: control acces la diferite informatii, servicii sau spații fizice, vot electronic, licente auto, portofel electronic, transport public. De asemenea, se va studia migrarea acestora către dispozitive mobile, cum sunt cele folosite in telefonie celulara (acestea contin, in structura lor, un smart card).

Soluția propusa foloseste smart-card-uri multiaplicație bazate pe tehnologie JavaCard sau Multos. Aceste tehnologii permit coexistenta mai multor aplicații într-un mod securizat pe același smartcard, fiind folosită de industria de specialitate din întreaga lume în diverse aplicații financiare, guvernamentale și de telecomunicație. Atuurile principale sunt: securitate ridicata, interoperabilitate, capacitatea multiaplicație și aderența la standarde deschise. Principalele informatii stocate pe card vor fi:

- a) datele personale si fotografia posesorului
- b) un identificator unic al cardului
- c) amprenta digitala
- d) două certificate digitale (autentificare și semnătură electronică) in format X.509
- e) cheile private asociate
- f) lantul de certificate ale Autorităților Emitente.

Pe langa funcția principală de carte electronică de identitate si instrument de semnatura digitala, cardului i se pot asocia funcționalități auxiliare (ex. control acces).