# Raport stiintific si tehnic in extenso pentru proiectul *Modele avansate de proiectare și evaluare a sistemelor criptografice moderne – ADECS*

*Etapa IV – Implementarea soluții de securitate și testare / evaluare*

# Cuprins

# 1 Introducere

Prin obiectivele tehnice si planurile de realizare asumate in propunerea initiala de proiect, proiectul ADECS are ca scop principal dezvoltarea unor capabilitati in domeniul cercetarii fundamentale si al algoritmilor criptografici si a tehnicilor de criptare adaptate cerintelor prezentului, tinta principala fiind realizarea unui model experimental modern in vederea implementarii unui sistem de criptare a transmisiilor de voce pentru telefoanele mobile. Solutia trebuie sa acopere principalele platforme existente – Android si Apple iOS – si va permite protectia transmisiilor de voce, in timp real, folosind sisteme de tip VOIP. In plus, printre obiectivele proiectulului se constituie si realizarea unor platforme de dezvoltare de aplicatii de securitate pentru telefoane mobile din familia celor amintite precum si a unor platforme de testare-evaluare a securitatii pentru sistemele informatice (platformă de testare-evaluare a algoritmilor criptografici si platformă de evaluare de securitate a produselor IT conform standardului FIPS 140-2).

Conform planului din cadrul proiectului, in aceasta etapa (etapa IV) s-a urmarit definitivarea specificatiilor software pentru platforma server din cadrul solutiei de criptare voce, realizarea si testarea platformelor de dezvoltare de aplicatii de securitate folosite pe smartphone –uri precum si testarea aplicatiilor incluse in platforma de testare/evaluare pentru aplicatiile de securitate (testarea conformitatii cu standardul FIPS 140-2).

Etapa a cuprins 5 activitati si livrabilele aferente:

1. Activitatea IV.1 Definitivare specificatii software pentru aplicatia server
    a. Specificatie software pentru aplicatia server
2. Activitatea IV.2 Definitivare realizare aplicatie server de criptare voce
    a. Aplicatie server de criptare voce
3. Activitatea IV.3 Realizarea platformei de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri etapa 1
    a. Platforma de dezvoltare (varianta 1) pentru aplicatii de securitate folosite pentru smartphone –uri.
4. Activitatea IV.4 Testarea kit-ului de dezvoltare software pentru aplicatii folosite pe smartphones-etapa 1
    a. Plan de testare (varianta 1) pentru kit –ul de dezvoltare software pentru aplicatii folosite pe smartphones
5. Activitatea IV.5 Testarea aplicatiilor incluse in platforma de testare/evaluare pentru aplicatiile de securitate CONFORM STANDARDULUI FIPS 140-2
    a. Plan de testare a conformitatii cu standardul FIPS 140-2 a platformei de testare/evaluare pentru aplicatiile de securitate

# 2 Activitatea IV.1 Definitivare specificatii software pentru aplicatia server

**In cadrul activitatii IV.1** a fost realizata definirea specificatiilor software pentru aplicatia de tip server.

Pentru aplicatia de tip server server au fost definite urmatoarele module:

- Modulul de semnalizare
- Modulul de rutare a comunicatiei de tip voce
- Modulul de generare al certificatelor digitale de criptare
- Modulul de licentiere utilizatori

Caracteristicile functionale ale acestor module sunt urmatoarele:

1. **Modulul de semnalizare**
    - Trebuie sa implementeze protocolul SIP (Session Initiation Protocol)
    - Trebuie sa fie accesat doar de catre utilizatorii autorizati
    - Criptarea comunicatiei trebuie sa fie realizata utilizand protocolul SSL cu dubla autentificare
    - Trebuie sa se integreze cu module terte destinate rutarii comunicatiei
    - Trebuie sa fie capabil sa ruteze mesaje de tip text transmise intre utilizatorii autorizati
    - Trebuie sa fie capabil sa detecteze atacuri de tip spoofing
    - Trebuie sa utilizeze baze de date relationale pentru stocarea diverselor elemente necesare procesului de comunicare
    - Trebuie sa implementeze metode SIP necesare pentru semnalizarea apelurilor de voce
    - Trebuie sa implementeze un mecanism de prezenta pentru utilizatori (online/offline)
    - Trebuie sa suporte scenario de tip NAT atat pentru apeluri de voce cat si pentru mesaje scrise
    - Mesajele transmise de catre utilizatori sa fie criptate punct la punct
    - Sa realizeze rutarea mesajelor SIP intre utilizatori
2. **Modulul de rutate a comunicatiei de tip voce**
    - Trebuie sa ruteze comunicatia de tip voce intre doi utilizatori care nu pot comunica in mod direct (scenarii NAT)
    - Trebuie sa prelucreze sis a gestioneze pachete de voce incapsulate conform protocolului RTP
    - Trebuie sa fie capabil sa mentina o sesiune de transfer a pachetelor de tip voce
    - Trebuie sa dispuna de o sesiune de interfatare cu terte module pentru crearea sau distrugerea sesiunilor de voce
    - Sa prelucreze mesaje conform RTCP
3. **Modulul de generare al certificatelor digitale de criptare**
    - Trebuie sa genereze certificate digitale conform standardului X509 V.3 in baza unor cereri criptografice de tip PKCS#10
    - Trebuie sa aiba implementata o interfata de tip REST pentru realizarea comunicatiei cu terte module
    - Comunicatia cu terte module sau aplicatii trebuie sa se realizeze prin protocol criptat de tip SSL/TLS

- Certificatele digitale vor fi emise doar pentru utilizatori legitimi ai sistemului
- Trebuie sa implementeze politici si proceduri de securitate in conformitate cu bunele practici in domeniul PKI

4. **Modulul de licentiere utilizatori**
    - Trebuie sa fie capabil sa genereze coduri unice pentru accesul utilizatorilor in sistem
    - Capabilitatea de gestionare a perioadei de viata ale codurilor unice
    - Sa dispuna de o interfata de administrare care poate fi accesata de utilizatorii autorizati folosind numai protocolul SSL cu dubla autentificare
    - Sa permita automatizarea procesului de transmitere a codurilor unice catre utilizatori
    - Sa permita validarea adresei de e-mail a unui utilizator
    - Sa utilizeze o baza de date relationala

# 3 Activitatea IV.2 Definitivare realizare aplicatie server de criptare voce

**In cadrul activitatii IV.2** a fost realizata implementarea aplicatiei de tip server pentru criptare voce. Aceasta activitate a fost realizata cu respectarea cerintelor definite in cadrul activitatii IV.1 .

# 4 Activitatea IV.3 Realizarea platformei de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri

**In cadrul activitatii IV.3** a fost realizata implementarea platformei de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri.

**Platforma de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri** a fost dezvoltata ca un API avand urmatoarele functionalitati majore:

- Implementarea unor rutine criptografice bazate pe: RSA, SHA-2, curbe eliptice, AES
- Pentru criptarea comunicatiilor de tip stream implementarea de rutine criptografice specifice (AES-CTR)
- Implementarea de rutine bazate pe standardul PKCS#11 pentru utilizarea de dispozitive criptografice externe de tip smartcard, dispozitive accesibile sub diverse forme: Secure SD card, smart card extern, NFC, Bluetooth
- Implementarea unor rutine criptografice pentru:
    - Criptarea mesajelor
    - Semnatura electronica
    - Functii de tip hashing

# 5 Activitatea IV.4 Testarea kit-ului de dezvoltare software pentru aplicatii folosite pe smartphones

**In cadrul activitatii IV.4** a fost realizata testarea platformei de dezvoltare software pentru aplicatii de securitate folosite pe smartphone-uri.

In cadrul testarii au fost realizate o serie de aplicatii de tip test pentru smartphne –uri bazate pe kit –ul de dezvoltare pentru smartphone. În cadrul aplicatiilor de test au fost implementate urmatoarele functionalitati (teste):

- Generarea de chei RSA folosind modulul de generare software. S-au generat 3 tipuri de chei RSA (1024/2048/4096 de biti). Aceste chei au fost exportate pe un sistem desktop si au fost apoi testate folosind un pachet software terţ (openssl).
- Generarea de chei RSA folosind modulul de generare hardware (Secure SD). S-au generat 2 tipuri de chei RSA (1024/2048 de biti). Aceste chei au fost exportate pe un sistem desktop si au fost apoi testate folosind un pachet software terţ (openssl).
- Extragerea componentelor publice din cadrul cheilor RSA (modul, exponent public).
- Criptarea/decriptarea datelor folosind RSA. S-a realizat criptarea in format PKCS#7 (CMS EnvelopedData) a unui stream de date (fisier). Criptarea simetrica s-a realizat folosind algoritmul AES (in toate cele 3 versiuni 128/192/256), iar pentru criptarea cheilor de sesiune au fost folosite cheile RSA generate anterior. A fost testata functionalitatea de decriptare. Operatiile de criptare si decriptare au fost realizate pe aceeasi platforma.
- Testarea anvelopei PKCS#7 generata anterior. Fisierul PKCS#7 generat a fost descarcat pe desktop si apoi a fost parsat folosind o aplicatii tert (ASN1Browser, openssl).
- Generarea unui anvelope PKCS#7 pe desktop folosind o cheie publica RSA si decriptarea ei pe dispozitive mobile folosind cheia privata asociata si stocata pe dispozitiv.
- Semnarea unui stream de date (fisier) folosind cheile RSA. Au fost folosite cheile RSA generate anterior, iar semnarea s-a realizat in format PKCS#1. La generarea semnaturii, pentru operatia de hashing a fost folosit algoritmul SHA-2. A fost testata functionalitatea de verificare a semnaturilor.
- Generarea de semnaturi in format PKCS#7 (CMS SignedData) folosind cheile RSA generate anterior.
- Verificarea semnaturii PKCS#7 generata anterior (realizata din aplicatia de test de pe dispozitivul mobil) folosind o aplicatie terţ de pe desktop (openssl).
- Generarea de chei specifice algoritmilor criptografici cu curbe eliptice.
- Realizarea unor operatii de semnare folosind algoritmul ECDSA si cheile generate anterior.
- Realizarea de hash –uri pe date folosind algoritmul SHA-2.
- Generarea de chei AES (128/192/256 biti) si criptarea/decriptarea de date folosind aceste chei.
- Testarea functiilor de criptare/decriptare de date folosind AES in mod CTR (AES-CTR).
- Realizarea de operatii de criptare/decriptare folosind chei hardware (SecureSD si smartcard extern) si interfata PKCS#11.
- Realizarea de operatii de semnare/verificare folosind chei hardware (SecureSD si smart-card extern) si interfata PKCS#11.
- Realizarea unei aplicatii de test pentru expedierea de mesaje SMS criptate. Criptarea mesajelor s-a realizat in format PKCS#1.

# 6 Activitatea IV.5 Testarea aplicatiilor incluse in platforma de testare/evaluare pentru aplicatiile de securitate CONFORM STANDARDULUI FIPS 140-2

**In cadrul activitatii IV.5** a fost realizata testarea platformei de testare/evaluare pentru aplicatiile de securitate. Testarea a avut in vedere functionalitatile aplicatiei in ceea ce priveste asistarea procesului de evaluare a produselor de securitate in conformitate cu standardul FIPS 140-2.

La baza elaborării specificaţiei de dezvoltare pentru produsul de bază (SDPB) au stat documentele referitoare la contractul de finanţare pentru execuţie proiecte de cercetare nr. 19/2012 în cadrul programului „Parteneriate în domenii prioritare" referitor la proiectul *„Modele avansate de proiectare şi evaluare a sistemelor criptografice moderne"*. În cadrul activităţii IV.5 *Testarea aplicaţiilor incluse în platforma de testare/evaluare pentru aplicaţiile de securitate conform FIPS 140-2* a fost realizată testarea/evaluarea aplicaţiilor incluse în platforma de testare/evaluare pentru produse de securitate IT. Testarea produsului „Platforma software de testare-evaluare pentru produse de securitate IT" a fost realizată în cadrul partenerilor certSIGN, Agenţia de Cercetare pentru Tehnică şi Tehnologii Militare (ACTTM) si Academia Tehnică Militară (ATM).

## Prezentare generală a platformei de testare/evaluare

Platforma software de testare-evaluare pentru produse de securitate IT (**ADECS-PTEPS-IT**) este destinată să asigure o platformă integrată pentru testarea şi evaluarea produselor de securitate IT. Produsul va fi utilizat ca un instrument în sprijinul activităţii de testare-evaluare, asigurând asistenţă completă echipei de testare-evaluare pe întreg parcursul procesului de testare-evaluare, de la primirea solicitării de evaluare a unui produs şi până la finalizarea raportului de testare-evaluare pentru acesta.

Platforma de testare/evaluare pentru produse de securitate IT este compusă din mai multe module software, constituind un instrument puternic pentru procesul de testare-evaluare a produselor de securitate IT, încercând să automatizeze procesul de testare-evaluare a acestora.

În realizarea platformei software s-a ţinut cont de faptul că modulele criptografice sunt evaluate conform cerinţelor de securitate din standardul FIPS PUB 140-2 iar produsele şi sistemele de securitate conform cerinţelor de asigurare din standardul Common Criteria (CC). Astfel că platforma software realizată permite evaluarea modulelor criptografice folosind criteriile de evaluare specificate în FIPS PUB 140-2 şi a produselorde securitate IT (altele decât modulele criptografice) folosind criteriile specifice CC.

## Funcţionalităţile platformei software ADECS-PTEPS-IT

Aplicaţiile software ce constituie „Platforma software de testare-evaluare pentru produse de securitate IT" au fost dezvoltate utilizând următoarele resurse:

- Mediul de dezvoltare Microsoft Visual Studio 2010;
- Limbajul de programare C#;
- Baze de date pe support XML;
- Generare de rapoarte în format Word (Pachetul Microsoft Office 2007).

Principalele funcţionalităţi implementate de „Platforma software de testare-evaluare pentru produse de securitate IT" sunt:

- Logarea la aplicaţie pe două roluri: rol de şef de laborator şi rol de evaluator;
- Acceptarea existenţei mai multor proiecte de testare - evaluare simultan;
- Rolul de şef de laborator oferă următoarele funcţionalităţi:
    - deschiderea unui proiect de testare-evaluare;
    - crearea de proiecte de testare-evaluare noi;
    - ştergerea proiectelor de testare-evaluare;
    - crearea şi ştergerea de roluri de evaluator;
    - introducerea şi ştergerea documentaţiei produsului de securitate;
    - generarea unor statistici ale evaluării;
    - vizualizarea auditului aplicaţiei;

- schimbarea parolei de acces;
- generarea rapoartelor de observare şi de testare-evaluare;
- generarea buletinelor de măsurători;
- analiza rapoartelor de observare;

- Rolul de evaluator oferă următoarele funcţionalităţi:
  - deschiderea unui proiect de evaluarea unui sistem sau produs conform standardului ales (FIPS PUB 140-2 sau CC)
  - introducerea şi ştergerea documentaţiei produsului de securitate;
  - generarea unor statistici ale evaluării;
  - vizualizarea auditului aplicaţiei
  - schimbarea parolei de acces
  - generarea rapoartelor de observare şi a buletinelor de măsurători;
  - analiza rapoartelor de observare.

Aplicaţiile software ce constituie „Platforma software de testare-evaluare pentru produse de securitate IT” au fost realizate sub formă de fişiere executabile care rulează pe sistemul de operare Windows 7. În figura 1 este prezentată interfaţa principală a aplicaţiei „SuportTestareEvaluare” din cadrul platformei software de testare-evaluare pentru produse de securitate care oferă suport pentru activitatea de testare a unui modul criptografic conform standardului FIPS 140-2.

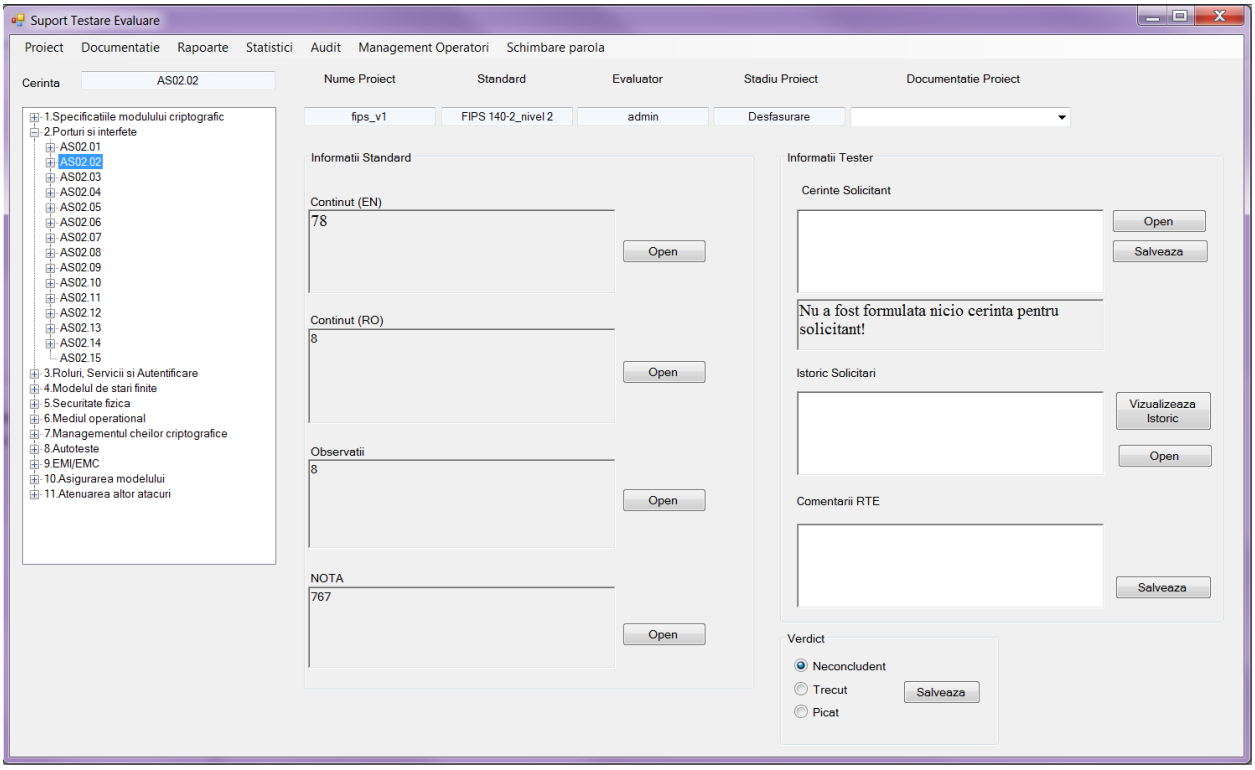


Figura 1 Interfaţa principală a aplicaţiei „SuportTestareEvaluare” din cadrul platformei software de testare-evaluare pentru produse de securitate IT

Procedura de testarea a platformei software ADECS-PTEPS-IT stabileşte metodele de verificare a produsului „Platforma software de testare-evaluare pentru produse de securitate IT” pentru următoarele verificări:

- Verificarea respectării cerinţelor pentru componentele software de uz general;
- Verificarea instalării şi dezinstalării platformei software;

- Verificarea cerinţei privind protecţia accesului la platforma software;
- Verificarea creării proiectelor de testare- evaluare a a produselor de securitate IT;
- Verificarea ştergerii proiectelor de testare –evaluare a produselor de securitate IT;
- Verificarea cerinţei privind deschiderea proiectelor de testare – evaluare a produselor de securitate IT;
- Verificarea creării rolurilor de evaluator;
- Verificarea ştergerii rolurilor de evaluator;
- Verificarea cerinţei privind introducerea în proiect a documentaţiei de evaluare a produsului ;
- Verificarea cerinţei privind ştergerea din proiect a documentaţiei de evaluare a produsului;
- Verificarea cerinţei privind generarea unei statistici a evaluării;
- Verificarea cerinţei privind vizualizarea auditului platformei software;
- Verificarea cerinţei privind schimbarea parolei de acces;
- Verificarea cerinţei privind generarea rapoartelor de observare;
- Verificarea cerinţei privind generarea rapoartelor de testare-evaluare;
- Verificarea cerinţei privind generarea buletinelor de măsurători;
- Verificarea cerinţei privind analiza rapoartelor de observare;
- Verificarea cerinţei privind acceptarea existenţei mai multor proiecte de testare - evaluare simultan.

In continuare este prezentat un rezumat al procedurii de testare a platformei software ADECS-PTEPS-IT pentru functiile de asistare a procesului de evaluare a produselor de securitate privind **conformitatea** acestora **cu standardul FIPS 140-2.** Conform FIPS PUB 140-2, obiective funcționale de securitate ale unui modul criptografic sunt următoarele:

- Să pună în aplicare și să implementeze corect funcțiile de securitate aprobate pentru protecția informațiilor
- Să protejeze un modul criptografic împotriva accesului sau utilizării neautorizate
- Să prevină descoperirea neautorizată a conținutului modului criptografic, inclusiv a cheilor criptografice și a parametrilor critici de securitate
- Să prevină modificarea neautorizată a și nedetectată a modulului criptografic și a algoritmilor criptografici (modificarea, substituirea, inserarea și ștergerea cheilor criptografice și a parametrilor critici de securitate)
- Să ofere indicații cu privire la starea de operare a modului criptografic
- Să asigure că modulul criptografic se comportă adecvat atunci când este operat corespunzător
- Să detecteze erori ce pot surveni in operarea modulului criptografic și să prevină compromiterea datelor sensibile și a parametrilor critici de securitate ce poate surveni în urma apariției unor erori.

Având la bază aceste obiective, precum și specificațiile standardului FIPS PUB 140-2, platforma de testare trebuie să permită managementul procesului de evaluare a unui produs criptografic, raportând la fiecare pas cerințele de securitate îndeplinite sau erori survenite în urma neîndeplinirii anumitor cerințe.

Procedura de testarea a platformei software ADECS-PTEPS-IT stabileşte metodele de verificare a produsului „Platforma software de testare-evaluare pentru produse de securitate IT” pentru următoarele verificări privind conformitatea cu cerintele standardului FIPS 140-2:

1. **<u>Specificaţiile modulului criptografic</u>**

Platforma de testare trebuie să permită raportarea nivelului de îndeplinire a cerinței privind:

- Numele modulului criptografic
- Funcții de securitate și moduri de operare
- Limitările unui modul criptografic din punct de vedere criptografic

## 2. Porturi și interfețe ale modulului criptografic

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să permită raportarea nivelului de îndeplinire a cerinței de restricționare a fluxului de informații în funcție de porturile fizice și interfețele logice ale produsului evaluat (distingerea datelor de intrare de cele de control, și cele de ieșire de cele de stare). Se testeaza suportul pentru asistarea procesului de evaluare conform pentru

- Nivelele de securitate 1 și 2
- Nivelele de securitate 3 și 4

## 3. Roluri, servicii si autentificare

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să permită raportarea nivelului de îndeplinire a următoarelor cerințe:

- Identificarea rolurilor
- Implementarea unei funcții de bypass
- Rularea serviciilor care nu necesită un rol autorizat
- Autentificarea unui operator și mecanismele de autentificare utilizate
- Autentificare bazată pe roluri sau Autentificare bazată pe identitate

## 4. Modelul finit de stări

Platforma de testare trebuie să ofere posibilitatea ca, în cadrul proiectului activ de evaluare a unui modul criptografic, să returneze rapoarte cu privire la modelul finit de stări. Modelul finit de stări este reprezentat în documentația modulului criptografic printr-o diagramă sau o tabelă cu tranziție a stărilor.

## 5. Securitatea la nivel fizic

**Cerințe generale de securitate la nivel fizic**

Platforma de testare trebuie să permită raportarea nivelului de îndeplinire a cerințelor de securitate la nivel fizic pe care un modul criptografic trebuie să le îndeplinească pentru a fi în conformitate cu FIPS 140-2. În primă fază sunt evaluate cerințele generale de securitate, pe care toate tipurile de implementări ar trebui să le îndeplinească, iar apoi, în funcție de caracteristicile hardware ale modului criptografic, sunt evaluate cerințele specifice de securitate fizică in raport cu nivelele 1, 2, 3 şi 4 din cadrul FIPS 140-2.

**Modulele criptografice single-chip**

Platforma de testare trebuie să permită raportarea cerințelor de securitate fizică, specifice modulelor criptografice *single-chip* in raport cu nivelele 1, 2, 3 şi 4 din cadrul FIPS 140-2.

**Module criptografice multiple-chip încorporate**

Modulele criptografice *multiple-chip* încorporate necesită respectarea unor cerințe în plus. Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic *multiple-chip* încorporat să se permită raportarea nivelului de îndeplinire a cerințelor de securitate fizică.

**Module criptografice multiple-chip autonome**

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic *multiple-chip* autonom să se permită raportarea nivelului de îndeplinire a cerințelor de securitate fizică.

## 6. Mediul de operare

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să permită raportarea nivelului de îndeplinire a cerinței privind mediul de operare către produsul evaluat. Aplicația trebuie să permită includerea în rapoartele de evaluare a faptului că produsul criptografic evaluat în cadrul unui proiect satisface următoarele cerințe:

- Mediul de operare al unui modul criptografic se referă la managementul componentelor software, firmware și/sau hardware necesare pentru funcționarea modulului. Mediul de operare poate fi nemodificabil (ex. firmware stocat în ROM, software dintr-un sistem de calcul cu dispozitive de I/O dezactivate) sau modificabil (ex. firmware stocat în RAM sau software executat de un sistem de calcul de uz general). Un sistem de operare este o componentă importantă a mediului de operare al unui modul criptografic.
- Un mediu de operare de uz general se referă la folosirea unui sistem de operare de uz general disponibil comercial (ex. manager de resurse) care să gestioneze componentele software și firmware în perimetrul criptografic și de asemenea să gestioneze sistemul și procesele/firele de execuție ale operatorilor, inclusiv aplicațiile software de uz general precum procesoarele de text.
- Un mediu de operare limitat se referă la un mediu de operare virtual static și nemodificabil (ex. mașina virtuală JAVA sau un card PC neprogramabil) cu niciun suport de sistem de operare de uz general pe care se află în mod unic mediul de operare.
- Un mediu de operare modificabil se referă la un mediu de operare care poate fi reconfigurat pentru adăugarea/ștergerea/modificarea unor funcționalități sau/și poate include capabilități ale unui sistem de operare de uz general (ex. folosirea sistemului de operare al unui calculator, sistemul de operare configurabil al unui smartcard sau firmware programabil). Sistemele de operare sunt considerate medii de operare modificabile dacă componentele software/firmware pot fi modificate de un operator și/sau un operator poate încărca sau executa software sau firmware (ex. un procesor de text) care nu era inclus ca parte a validării modulului.
- Dacă mediul de operare este un mediu de operare modificabil, se vor aplica cerințele pentru sistemul de operare din secțiunea 6.1. Dacă mediul de operare este un mediu de operare limitat, cerințele pentru sistem de operare din secțiunea 6.1 nu se aplică.

## Managementul cheilor criptografice

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să permită raportarea nivelului de îndeplinire a cerinței privind managementul cheilor criptografice către produsul evaluat. Aplicația trebuie să permită includerea în rapoartele de evaluare a faptului că produsul criptografic evaluat in cadrul unui proiect satisface următoarele cerințe:

- Cerințele de securitate pentru managementul cheilor criptografice cuprinde întreg ciclul de viață al cheilor criptografice, componentelor cheilor criptografice și parametrilor critici de

securitate folosite de modulul criptografic. Managementul cheilor include generarea numerelor aleatoare și generarea cheilor, stabilirea cheilor, distribuția cheilor, operațiile de intrare/ieșire a cheilor, stocarea cheilor și zeroizarea cheilor. Un modul criptografic poate utiliza, de asemenea, mecanismele de gestionare a cheilor ale unui alt modul criptografic. Cheile criptografice și parametrii critici de securitate criptați se referă la chei și parametri critici de securitate criptați folosind un algoritm aprobat sau o funcție de securitate aprobată. Cheile criptografice și parametrii critici de securitate criptați folosind un algoritm care nu este aprobat sau un algoritm sau metodă proprietară sunt considerați în format plaintext în domeniul de aplicare al standardului FIPS 140-2.;

- Cheile secrete, cheile private şi parametrii critici de securitate trebuie să fie protejaţi în cadrul modulului criptografic împotriva divulgării, modificării şi substituirii neautorizate;
- Cheile publice trebuie să fie protejate în cadrul modulului criptografic împotriva modificării şi substituţiei neautorizate;
- Documentaţia modulului criptografic trebuie să specifice toate cheile criptografice, componentele cheilor criptografice şi parametrii de securitate critici din cadrul modulul criptografic;

Se mai testeaza conformitatea cu urmatoarele cerinte:

- Generatoare de numere aleatoare
- Generarea cheii
- Stabilirea cheii
- Operațiile de intrare și ieșire a cheilor
- Stocarea cheii
- Zeroizarea cheilor

**Interferența electromagnetică/compatibilitate electromagnetică (EMI/EMC)**

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să permită raportarea nivelului de îndeplinire a cerinței privind **interferența și compatibilitatea electromagnetică** a produsul evaluat. Aplicația trebuie să permită includerea în rapoartele de evaluare a faptului că produsul criptografic evaluat în cadrul unui proiect satisface următoarele cerințe:

- Documentația modulului criptografic trebuie să includă dovada de conformitate cu specificațiile EMI/EMC.
- Pentru nivelurile 1 și 2 de securitate, modulul criptografic trebuie să respecte cerințele specificate în *"47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices,* ***Class A****".*
- Pentru nivelurile 3 și 4 de securitate, modulul criptografic trebuie să respecte cerințele specificate în *"47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices,* ***Class B****".*

În cazul în care respectă aceste cerințe, aplicația trebuie să genereze raportul în conformitate cu nivelul de satisfacere a cerințelor, iar rutina de testare întoarce un rezultat de succes. Dacă nu, rutina de testare trebuie sa intoarcă un cod de eroare.

**Asigurarea modelului**

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să se raporteze dacă acesta este corespunzător testat, configurat, livrat, instalat și dezvoltat și dacă este furnizată documentația de îndrumare a operatorilor. În rapoartele de evaluare, aplicația trebuie

să genereze un rezultat din care să reiasă nivelul de satisfacere al cerinței FIPS. Dacă se îndeplinește cerința, rutina de testare trebuie să întoarcă un mesaj de success, altfel, să returneze un cod de eroare.

**Diminuarea altor tipuri de atacuri**

Platforma de testare trebuie să ofere posibilitatea ca în cadrul proiectului activ de evaluare a unui modul criptografic să permită raportarea nivelului de îndeplinire a cerinței privind capabilitatea modulului de a diminua unul sau mai multe atacuri specifice. Dacă aplicația conține această facilitate, ea trebuie să genereze rapoartele de evaluare în conformitate cu nivelul de îndeplinire a cerinței FIPS iar rutina de testare întoarce un rezultat de succes, altfel, returnează un cod de eroare