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

Etapa II –Elaborarea solutiilor pentru securitatea datelor si implementarea de componente pentru 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 s-a urmarit elaborarea solutiilor pentru securitatea datelor si implementarea unora din componentele de securitate şi testare/evaluare propuse. Etapa a cuprins 6 activitati si livrabilele aferente:

1. Activitatea II.1 Efectuarea specificatiilor software pentru aplicatia client de criptare-voce pe canal de date, cu livrabilul:
    a. Specificatii software pentru aplicatia client de criptare-voce pe canal de date
2. Activitatea II.2 Efectuarea specificatii software pentru componente aplicatie server, cu livrabilul:
    a. Specificatii software pentru componentele aplicatie server
3. Activitatea II.3 Efectuarea specificatii componente privind crearea unei platforme comune pentru aplicatiile de securitate:
    a. Specificatii componente privind crearea unei platforme comune pentru aplicatiile de securitate
4. Activitatea II.4 Realizarea aplicatiei client de criptare voce pe canal de date:
    a. Aplicatie client de criptare voce pe canal de date
5. Activitatea II.5 Realizare componente ale platformei de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri:
    a. Platforma de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri
6. Activitatea II.6 Realizarea platformei de testare/evaluare pentru produse de securitate, cu livrabilul:
    a. Realizarea platformei de testare/evaluare pentru produse de securitate

2 Activitatea II.1 Efectuarea specificatiilor software pentru aplicatia client de criptare-voce pe canal de date

In cadrul activitatii II.1 a fost realizat un document ce cuprinde specificatiile software pentru aplicatia client de criptare-voce pe canal de date. Documentul prezintă descrierea conceptuală privind componentele sistemului de criptare a vocii propus a fi realizat in cadrul proiectului si denumit in continuare CryptoVoIP.

In continuarea acestei sectiuni din prezentul raport stiintific sunt descrise intr-o forma sintetica cateva din elementele tehnice realizate in cadrul acestei activitati, pentru proiectarea sistemului de securizare a vocii prin criptare.

Astfel, sistemul de criptare voce isi propuse sa asigure operatiuni de criptare/decriptare in timp real a convorbirilor facute peste protocolul IP folosind telefoane mobile avand preinstalate urmatoarele sisteme de operare:

- iOS v. 4.0 sau superior (inclusiv v. 5.0)
- Android v.2.2 sau superior (inclusiv v. 4.0.4)

In acest sens, aplicatiile componente din cadrul sistemului trebuie sa poata fi instalate pe orice tip de telefon care ruleaza unul din sistemele de operare mai sus mentionate. Aceaste aplicatii permit initierea si derularea de conexiuni criptate pe retele de date de tip; 3G, 4G si respectiv WIFI.

Pentru a putea realiza criptarea fluxurilor de voce vehiculate, sistemul va trebui configurat astfel incat:

- sa utilizeze o pereche de chei publica/privata si un certificat digital propriu pentru fiecare utilizator mobil in parte;
- certificatul aplicatiei server;
- date de conectare la aplicatia de tip server (adresa IP, DNS etc).
- lista de participanti (agenda) – aceasta lista va fi de tip tabel ce contine ID-ul interlocutorului si numele acestuia.

Designul aplicatiei va permite schimbarea facila a algoritmului RSA cu algoritmi de criptare bazati pe curbe eliptice. In plus, aplicatia va trebui sa aiba capabilitatea de a introduce si utiliza algoritmi de criptare proprietari beneficiarului.

In procesul de criptare a datelor aplicatia trebuie sa permita doua variante:

1. Criptare de Nivel 1 folosind urmatoarele elemente criptografice:
   a. Perechea de chei publica/privata si certificatul digital propriu aplicatiei
   b. Cheie de sesiune generata la momentul initierii conexiunii folosind un generator de numere pseudoaleatoare propriu telefonului mobil. Cheia de sesiune trebuie sa aiba dimensiune de 256 de biti iar pentru criptare se va utiliza algoritmul AES.

2. Criptare de Nivel 2 folosind urmatoarele elemente criptografice:
   a. Perechea de chei publica/privata si certificatul digital propriu aplicatiei
   b. Chei de sesiune generate anterior de catre aplicatia CryptoVoIPk folosind un generator aleator. Cheile vor fi generate pentru fiecare conexiune de tip 1-1 si vor fi criptate cu cheia publica a utilizatorului. Acestea vor fi stocate in prealabil, pe un dispozitiv de tip SD card inserat in dispozitivul mobil.

Pentru un nivel de inalta securitate elementele criptografice principale (perechea de chei RSA si certificatul corespunzator) vor fi stocate astfel:

1. In cazul iOS – dispozitive de tip smart card externe
2. In cazul Android – dispozitive de tip secure SD card.

Au fost definite elementele de protocol criptografic in cazul celor doua tipuri de criptari.

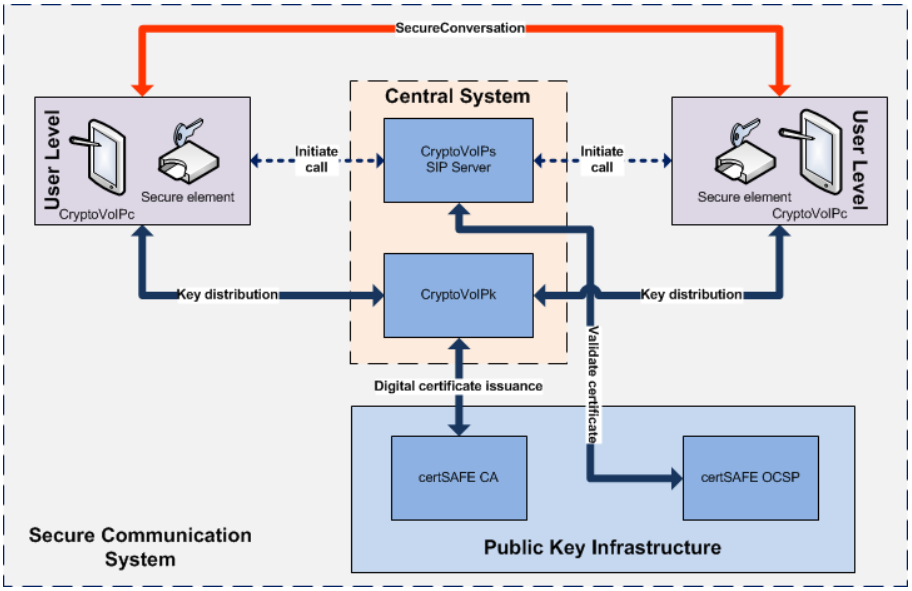
Din punct de vedere al interfetei au fost definite urmatoarele elemente:

1. Un ecran principal continand o lista de adrese ale utilizatorilor cu care poate initia conexiuni securizate. Lista va fi incarcata dinamic sau in prealabil. Aceasta lista se va actualiza la fiecare 20 secunde si va contine starea (online/offline) pentru fiecare contact existent. Lista va contine:
    - Numele persoanei care se doreste a fi contactata
    - Id-ul acesteia
2. Un ecran continand mesajele de tip sms. Mesajele transmise si receptionate vor fi criptate in permanenta in telefon
3. Un ecran cu ultimele apeluri efectuate
4. Un ecran de setari care va contine:
    - Elemente de profil:
        - Nume utilizator
        - Invitatii
    - Elemente de securitate:
        - Criptare activa sau nu
        - Tip de criptare:
            - Soft folosind certificate digitale in format PKCS#12
            - Hard folosind certificate digitale stocate pe dispozitive de tip smartcard
        - Locatia containerului PKCS#12 in cazul criptarii soft
        - Pastrarea istoricului apelurilor efectuate
        - Securizare prin PIN a mesajelor transmise si receptionate
        - Perioada de viata a mesajelor
    - Elemente de notificare:
        - Notificare in caz de apel
        - Notificare in caz de sms
    - Elemente de conectivitate
        - Adresa server-ului

In momentul selectarii unui contact utilizatorul trebuie sa aiba posibilitatea de a initia:

- Apel de voce securizat
- Chat de tip securizat

O schema de proiectare a sistemului de securizare voce este data mai jos:



3 Activitatea II.2 Efectuarea specificatii software pentru componentele aplicatiei server

In cadrul activitatii II.2 au fost realizate specificatiile software pentru implementarea aplicatiei de tip server, componenta a sistemului de securizare a vocii.

Aplicatia va fi implementata sub forma un server de tip proxy, scopul principal fiind acela de stabilire a conexiunilor VOIP securizate intre utilizatori si apoi de rutare a pachetelor de tip VOIP schimbate de acestia.

Aplicatia va avea urmatoarele doua componente:

1. Componenta operationala – realizeaza stabilirea si operarea conexiunilor VOIP securizate intre utilizatori. Functionalitatile acestei componente vor fi:
   - Interfatarea cu aplicatiile client in vederea stabilirii/intreruperii si gestiunii conexiunilor VOIP intre utilizatori
   - Rutarea pachetelor de mesaje criptate in cadrul conexiunilor VOIP
   - Autentificarea aplicatiilor client pe baza de certificate
   - Implementarea functiilor de stabilire a parametrilor criptografici necesari in protocoalele descrise mai sus
   - Validarea certificatelor utilizate la autentificarea aplicatiilor client la server si la stabilirea de conexiuni VOIP intre utilizatori

2. Componenta de management – este o componenta WEB based ce asigura functionalitatile de administrare/configurare pentru componenta operationala:
   - Update topologie retea si managementul listei participanti
   - Gestiunea elementelor criptografice cerute in cadrul protocoalelor descrise (cheia privata si certificatul serverului, certificatele utilizatorilor,
   - Gestiunea politicilor de securitate definite la nivelul topologiei de retea

Aplicatia de management trebuie sa permita update-ul topologiei de retea astfel:

1. Automat – in cazul criptarii de nivel 1, utilizatorii pot initia ei insisi legaturi catre alti utilizatori
2. Manual – in cazul criptarii de nivel 2, administratorul poate acorda drepturile de comunicare in raport cu elementele criptografice generate si politica de securitate a retelei.

Aplicatia trebuie sa permita functionarea in mod complet manual astfel incat utilizatorii sa nu aiba dreptul de a stabili legaturi cu alti utilizatori.

Aplicatia va implementa protocolul public de tip SIP. Pentru utilizatorii provenind din retele diferite se va implementa o componenta de tip proxy.

Aplicatia de management a cheilor este o solutie complexa de administrare, generare si distributie chei de criptare precum si de management a utilizatorilor ce opereaza in cadrul retelei de securitate. Prin retea de securitate definim elementele de infrastructura, personalul necesar operarii cat si ansamblul de reguli, masuri si elemente de securitate necesare pentru protectia informatiilor critice transmise pe canalele de date.

Aplicatia va permite realizarea urmatoarelor operatiuni:

- Definirea de retele de securitate; Acestea sunt definite de catre administratorul/administratorii de securitate luindu-se in consideratie urmatoarele elemente:
    - Operatorii pentru generarea materialului criptografic (chei de criptare) – acele persoane definite in cadrul organizatiei care pot genera chei de criptare pentru o anumita retea;
    - Nume – numele retelei;
    - Algoritmi de criptare – reprezinta algoritmii criptografici care pot fi utilizati in cadrul unei retele. In prezent sistemul permite alegerea metodelor de criptare dintre urmatorii algoritmi:
    - AES – algoritm simetric de tip bloc cu criptare in mod CTR utilizand cheie de 256 de biti;
    - UEA – algoritm de criptare simetric proprietar UTI, de tip stream cu criptare utilizand chei de lungimi 256 si 512 biti.
    - Numarul maxim de utilizatori ce pot fi definiti intr-o retea;
    - Durata de viata a cheilor de criptare – pentru asigurarea unui inalt nivel de securitate se pot defini perioada maxima de valabilitate a cheilor criptografice. Dupa expirarea termenului de valabilitate, cheile criptografice nu mai pot fi utilizate;
    - Cheia de retea – cheie utilizata in criptarea anumitor informatii de retea (repere chei, identificatori utilizatori) ce sunt transmise odata cu documentele criptate;
    - Timp si conditii pentru efectuare de copii de siguranta a informatiilor generate.
- Parametrii de utilizator; utilizatorii sunt acele persoane sau entitati care executa operatiuni criptografice (criptare/decriptare) in cadrul unei retele si care pot fi definiti prin urmatorii parametri:
    - Nume si ID – sunt elementele de baza in identificarea utilizatorilor – din ratiuni de securitate acestea sunt definite de obicei pe baza de coduri;
    - Nivelul de securitate;
    - Numarul serial al dispozitivului de criptare utilizat;
    - Cheie de criptare – cheie utilizata in protectia materialului criptografic de baza.
- Parametrii de legatura; sunt acele elemente care identifica in mod clar legatura intre doi utilizatori. Acestia sunt:

    - Numele si ID-ul utilizatorilor de legatura – aceste date identifica in mod unic utilizatorii cu care se poate lua legatura in cadrul unei retele de securitate;
    - Dimensiunea cheilor asociate unei legaturi;
    - Chei de urgenta – acele chei care vor fi utilizate in cazul in care materialul criptografic de baza este compromis pentru criptarea unor mesaje de avertizare;
- Tipul de legatura – acesta poate fi:
    - Punct la punct – comunicatia se realizeaza intre doi utilizatori ai sistemului;
    - Circulara – comunicatia se realizeaza circular in sensul ca un document electronic criptat poate fi transmis catre toti utilizatorii definiti in fisierul de legatura.
- Aplicatia de management clickSIGN K va genera pentru fiecare utilizator al sistemului urmatoarele:
    - Chei criptografice pentru algoritmii definiti in etapa de configurare a sistemului;

Aplicatia de management va utiliza un generator hardware de numere aleatoare RNG. Cheile generate vor fi verificate de un numar de 16 teste statistice care au scopul de a verifica aleatorismul unor secvenţe binare (de lungime arbitrară) produse în scopuri criptografice de generatoare de numere aleatoare. Aceste teste se concentrează pe o varietate de tipuri diferite de determinism (nonaleatorism) existente într-o secvenţă. Cele 16 teste sunt :

1. Test frecvenţă (monobit) – Frequency (Monobit) Test
2. Test frecvenţă în cadrul unui bloc - Frequency Test within a Block
3. Test privind numărul total de secvenţe neîntrerupte de biţi identici – Runs Test
4. Test privind determinarea celei mai mari secvenţe neîntrerupte de biţi cu valoarea 1 dintr-un bloc – Test for the Longest-Run-of-Ones in a Block
5. Testarea rangului matricelor binare – Binary Matrix Rank Test
6. Testarea transformărilor Fourier discrete – Discrete Fourier Transform (Spectral) Test
7. Test pentru detectarea generatorilor care determină apariţia unei secvenţe neperiodice prestabilite de prea multe ori, fără suprapunerea secvenţelor de eşantion de test – Non-overlapping Template Matching Test
8. Test pentru detectarea generatorilor care determină apariţia unei secvenţe neperiodice prestabilite de prea multe ori, cu suprapunerea secvenţelor de eşantion de test – Overlapping Template Matching Test
9. Testul Maurer privind stabilirea posibilităţii de compresie a unei secvenţe fără pierderea informaţiilor – Maurer's „Universal Statistic" Test
10. Test de compresie Lempel-Ziv - Lempel-Ziv Compression Test
11. Test de complexitate liniară pentru a stabili dacă o secvenţă este suficient de complexă pentru a fi considerată aleatoare – Linear Complexity Test
12. Test serial – Serial Test
13. Test de entropie – Approximate Entropy Test
14. Test de sume cumulative – Cumulative Sums (Cusums) Test
15. Test pentru a determina dacă numărul de treceri la o anumită stare din cadrul unui ciclu diferă de rezultatul aşteptat pentru o secvenţă aleatoare – Random Excursions Test
16. Test pentru a determina devierile de la numărul aşteptat de treceri la diferite stări în cadrul unui proces aleator – Random Excursions Variant Test

4 Activitatea II.3 Efectuarea specificatii componente privind crearea unei platforme comune pentru aplicatiile de securitate

In cadrul activitatii II.3 au fost realizate specificatiile unei platforme de dezvoltare comune pentru aplicatiile de securitate.

Specificatiile au la baza realizarea unui API comun de lucru cu functiile criptografice astfel incat sa existe o baza comuna a elementelor de securitate.

In vederea asigurarii unui nivel inalt de abstractizare precum si de securitate, dezvoltarea acestei platforme va fi realizata in C/C++ urmand a fi realizate wrapere ulterior pentru diverse platforme de calcul fixe sau mobile (C++, Java Android, ObjectiveC pentru iOS)

Arhitectura va fi realizata pe baza nucleului criptografic reprezentat de modulul openSSL. Platforma dezvoltata va implementa functiile criptografice necesare in procesele de securizare semnare/criptare/decriptare pe dispozitive mobile:

- criptare/decriptare de date pe baza standardului PKCS#7
- semnatura digitala pe baza standardului PKCS#7
- folosirea cheilor private stocate in anvelope PKCS#12
- folosirea cheilor stocate pe dispozitive hardware tip smart-card, pe baza standardului PKCS#11
- interogare servere LDAP
- codificare/decodificare de mesaje S/MIME
- functii de validare a certificatelor si de comunicatie cu servere OCSP

Avand in vedere dezvoltarea specifica pe platforme mobile se va dezvolta un modul special de asigurare a comunicatiei cu dispozitive de tip smartcard.

Dispozitivele de tip smart card utilizate in procesele de semnatura digitala si criptare vor trebuie sa fie acreditate FIPS 140-2 Level 2.

Pentru crearea de semnaturi digitale se vor implementa functii pentru realizarea structurii SignedData. Prin intermediul modulului PKCS #11 al bibliotecii, se va accesa cheia privata corespunzatoare certificatului de semnare aflat pe smart card si se va creea o structura de tip signerInfo. Cheia privata nu va parasi niciodata smart card-ul; operatiunile asupra datelor care vor fi protejate se vor efectua in pasi succesivi, prin trimiterea de date in smart card, unde sunt prelucrate de procesorul criptografic aflat pe acesta.

Pentru criptarea de voce precum si a mesajelor pentru sistemul de mesagerie, se va implementa o structura de tipul EnvelopedData. Mecanimul de criptare folosit va fi urmatorul:

- se genereaza o cheie unica de sesiune, specifica algoritmului simetric folosit; aceasta cheie se genereaza in interiorul smart card-ului;
- cheia este criptata pentru destinatr si apoi se transmite acestuia
- In baza cheii private, destinatarul decripteaza cheia de sesiune
- Cheia de sesiune este utilizata ulterior in procesul de criptare/decriptare

Cheile de sesiune sunt generate pentru fiecare apel respectiv mesaj in parte.

5 Activitatea II. 4 Realizarea aplicatiei client de criptare voce pe canal de date

In cadrul activitatii II.4 a fost realizata in baza specificatiilor tehnice de la activitatea II.1 aplicatia client pentru criptarea vocii pe canal de date. Functionalitatile implementate respecta integral cerintele activitatii II.1 conform celor prezentate mai jos.

In procesul de criptare a datelor aplicatia permite doua variante de criptare:

1. Criptare de Nivel 1 folosind urmatoarele elemente criptografice:
   a. Perechea de chei publica/privata si certificatul digital propriu aplicatiei
   b. Cheie de sesiune generata la momentul initierii conexiunii folosind un generator de numere pseudoaleatoare propriu telefonului mobil. Cheia de sesiune are o dimensiune de 256 de biti iar pentru criptare se utilizeaza algoritmul AES.
2. Criptare de Nivel 2 foloseste urmatoarele elemente criptografice:
   a. Perechea de chei publica/privata si certificatul digital propriu aplicatiei
   b. Chei de sesiune generate anterior de catre aplicatia CryptoVoIPk folosind un generator aleator. Cheile sunt generate pentru fiecare conexiune de tip 1-1 si sunt criptate cu cheia publica a utilizatorului. Acestea sunt stocate in prealabil, pe un dispozitiv de tip SD card inserat in dispozitivul mobil.

Pentru un nivel de inalta securitate elementele criptografice principale (perechea de chei RSA si certificatul corespunzator) sunt stocate pe:

3. In cazul iOS – dispozitive de tip smart card externe
4. In cazul Android – dispozitive de tip secure SD card.

Au fost realizate elementele de protocol criptografic in cazul celor doua tipuri de criptari.

Din punct de vedere al interfetei au fost realizate urmatoarele elemente:

5. Un ecran principal continand o lista de adrese ale utilizatorilor cu care poate initia conexiuni securizate. Lista este incarcata dinamic sau in prealabil. Aceasta lista se actualizeaza continuu si contine starea (online/offline) pentru fiecare contact existent. Lista contine:
   - Numele persoanei care se doreste a fi contactata
   - Id-ul acesteia
6. Un ecran continand mesajele de tip sms. Mesajele transmise si receptionate sunt criptate in permanenta in telefon
7. Un ecran cu ultimele apeluri efectuate
8. Un ecran de setari care contine:
   - Elemente de profil:
     - Nume utilizator
     - Invitatii
   - Elemente de securitate:
     - Criptare activa sau nu
     - Tip de criptare:
       - Soft folosind certificate digitale in format PKCS#12
       - Hard folosind certificate digitale stocate pe dispozitive de tip smartcard

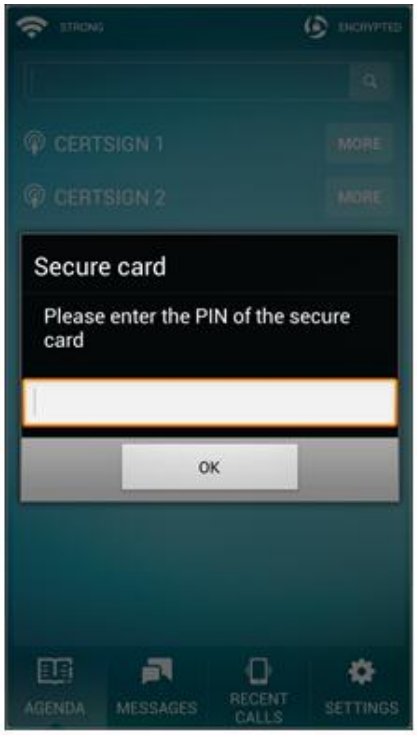
- Locatia containerului PKCS#12 in cazul criptarii soft
- Pastrarea istoricului apelurilor efectuate
- Securizare prin PIN a mesajelor transmise si receptionate
- Perioada de viata a mesajelor

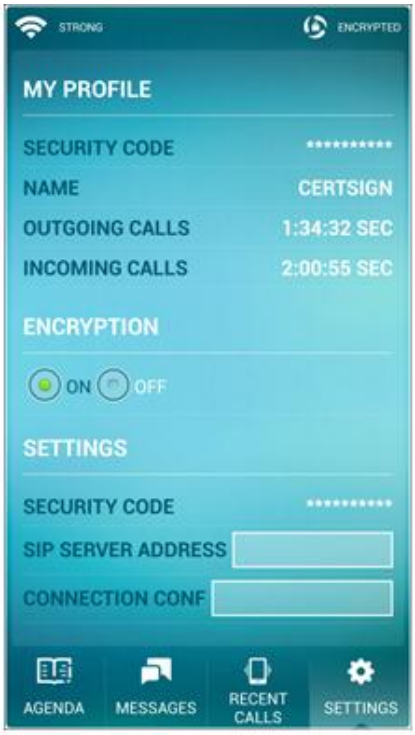
- Elemente de notificare:
  - Notificare in caz de apel
  - Notificare in caz de sms
- Elemente de conectivitate
  - Adresa server-ului

In momentul selectarii unui contact utilizatorul are posibilitatea de a initia:

- Apel de voce securizat
- Chat de tip securizat

Mai jos sunt prezentate cateva capturi de ecran cu functionalitatile aplicatiei.





6 Activitatea II. 5 Realizare componente ale platformei de dezvoltare pentru aplicatiile de securitate folosite pe smartphone-uri

In cadrul activitatii II.5 au fost realizata componenta principala a plaformei de dezvoltare pentru dispozitive mobile avand in vedere specificatiile elaborate la activitatea II.3.

In cadrul acestei actiivitati au fost dezvoltate mai multe componente software ce vor fi parte integranta a platformei de dezvoltare de aplicatii de securitate pentru smartphone-uri:

- Un SDK cu functionalitati si primitive criptografice de baza necesare.
- SDK –uri specifice pentru platformele mobile urmarite in cadrul proiectului (iOS si Android) obtinute prin extinderea SDK –ului de baza pe aceste platforme.
- Module software de nivel aplicatie pentru securizarea informatiei la nivel de dispozitive mobile.

In acest fost dezvoltat un API de baza (CRYUBase-SDK) implementat in C/C++ pentru realizarea de pe dispozitivele mobile a urmatoarelor operatiuni criptografice:

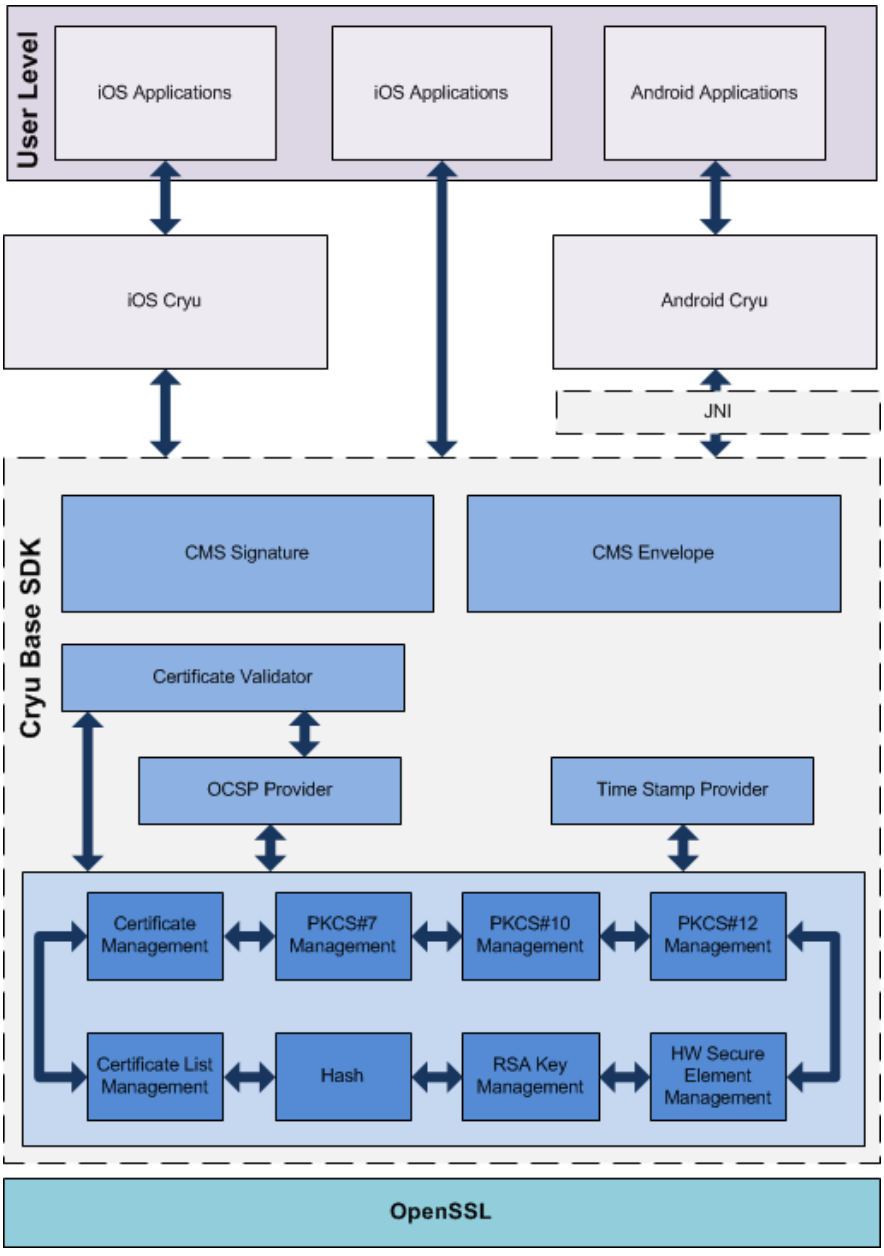
- generarea si managementul de chei criptografice pe dispoziitive mobile si elemente de tip secure-element
- crearea si gestiunea de cereri de certificate pentru cheile criptografice publice in vederea obtinerii de certificate de la servicii de tip PKI specializate;
- gestiunea de certificate in vederea importului si utilizarii lor in aplicatii dezvoltate pe smartphone-uri.
- utilizarea de chei criptografice pentru realizarea de semnaturi compatibile CMS/PKCS#7
- criptare/decriptare de date pe baza standardului CMS/PKCS#7
- gestiunea si utilizarea cheilor private stocate in anvelope PKCS#12
- folosirea cheilor stocate pe dispozitive hardware tip smart-card, pe baza standardului PKCS#11
- folosirea cheilor stocate pe dispozitive hardware de tip smartcard, folosind comunicatii de niel sczut (bazat pe protocoale de tip APDU) si implementarea unor drivere generice in acest sens pentru a putea fi apoi foarte usor adaptate pentru orice producator de dispozitive criptografice hardware.
- interogare servere LDAP
- codificare/decodificare de mesaje S/MIME
- functii de validare a certificatelor si de comunicatie cu servere OCSP

Aceasta platforma de dezvoltare comuna va expune interfete catre diverse limbaje de programare facand astfel posibila integrarea acesteia pe diverse platforme de dispozitive mobile.

Peste aceasta componenta au fost dezvoltate componente criptografice de tip API, specifice pentru platformele targetate: iOS-Cryu si Android-Cryu. O schema descriptiva pentru arhitectura componentelor realizate este data mai jos. In afara componentei OpenSSL, toate componentele din schema au fost dezvoltate in cadrul proiectului, in aceasta etapa.

Pe baza acestor componente au fost dezvoltate si testate si cateva componente de aplicatii pentru platformele Android si iOS care exploateze functionalitatile criptografice ale SDK –urilor prezentate mai sus: aplicatii de semnatura electronica si criptare de date, utilizand chei software sau de pe dispozitive hardware de tip secure element; aplicatii de integrare cu sisteme PKI existente in vederea realizaraii

operatiilor de enrollment si obtinere de certificate pentru utlizator. Practic s-a urmarit inchiderea unui flux complet de lucru specific acestui tip de aplicatii.



O parte importanta de cercetare a fost investitat in studiul comportamentului dispozitivelor specializate de tip secure element si a cititoarelor necesare pe cele doua platforme mobile precum si a posibilitatilor oferite nativ de sistemele amintite pe zona de aplicatii de securitate si PKI. In urma activitatii de cercetare si dezvoltare realizată au fost trase concluzii importante si au deschise practic piste de urmat pe mai departe in dezvoltarea de aplicatii de securitate pe dispozitive mobile.

7 Activitatea II. 6 Realizarea platformei de testare/evaluare pentru produse de securitate

Platforma de testare/evaluare pentru produse de securitate IT (denumită în continuare PTEPS-IT) a fost proiectată şi realizată sub forma unui pachet de programe software care va constitui un instrument foarte util şi eficient, în sprijinul activităţii, în primul rând, a celor trei laboratoare de testare-evaluare certificate la nivel naţional (din cadrul MApN, SIE şi SRI). După maturizarea produsului şi în funcţie de feedback-ul obţinut de la entităţile evaluatoare, vor fi întreprinse demersuri pentru diseminarea produsului către structurile specializate ale UE.

Un prim impact pozitiv a fost obţinut în urma **diseminării informaţiilor** referitoare la produs în cadrul conferinţei internaţionale Romanian CryptologyDays, RCD-2013, eveniment organizat în 16-17 septembrie 2013 de SIE în parteneriat cu Academia Română.Reprezantantul UE la eveniment a manifestat un interes deosebit axat pe importanţa şi utilitatea produsului prezentat de ACTTM, la nivelul structurilor competente din UE.

Pachetul software realizat constituie o implementare a procesului de testare-evaluare care rezolvă probleme complexe legate de automatizarea cât mai multor etape şi elemente ale acestui proces. Este realizată astfel asistenţa completă a echipei de testare-evaluare pe întreg parcursul procesului, de la primirea solicitării de evaluare a unui produs şi până la finalizarea raportului de testare-evaluare pentru acesta. Sunt astfel curpinse toate cele 3 faze ale procesului de evaluare:

a) Faza I Pregătirea evalării;
b) Faza II Desfăşurarea evaluării;
c) Faza III Concluzia evaluării.

Principalele funcţionalităţi implementate in platforma de testare/evaluare pentru produse de securitate sunt:

- posibilitatea de logare 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:
    - crearea de roluri de evaluator;
    - crearea de proiecte de testare evaluare noi;
    - introducerea datelor referitoare la documentaţia sistemului (tipul, numele, număr de înregistrare şi versiunea documentului);
    - generarea unor statistici ale evaluării;
    - generarea diferitelor tipuri de rapoarte;
- rolul de evaluator oferă următoarele funcţionalităţi:
    - evaluarea unui sistem sau produs conform standardului ales (FIPS PUB 140-2 sau CC);
    - hotărăşte ce decizie (trecut/picat) trebuie luată pentru fiecare test efectuat;
    - generarea fişelor de măsurători după terminarea testelor unui domeniu din FIPS sau a unei clase de asigurări din Common Criteria, etapă de testare pentru algoritmi.

Platforma permite existenţa mai multor proiecte de testare - evaluare simultan, fiecare din aceste proiecte fiind identificat de un set de date de identificare. Acesta este format din următoarele date:

- Nume produs evaluat;
- Versiune produs evaluat;
- Tip produs evaluat: modul criptografic, produs criptografic, sistem criptografic, profil de protecşie, algoritm criptografic;
- Standard utilizat pentru testare - evaluare : FIPS PUB 140-2, CC sau alte standarde;
- Nivel de securitate/încredere solicitat;
- Date despre solicitantul evaluării: nume, adresă, telefon/fax;
- Date despre dezvoltatorul produsului: nume, adresă, telefon/fax.

Platforma generează statistici referitoare la rezultatele testelor efectuate sau a unor statistici care indică procentul de acoperire al unei evaluări.

Platforma permite de asemenea generarea de tipuri diferite de rapoarte pe parcursul efectuării unei evaluări: raport de observaţii şi raport de testare - evaluare final. Rapoartele de observaţii conţin informaţii despre rezultatele parţiale ale evaluării şi sunt create ori de câte ori apare o problemă pe parcursul unei evaluări sau trebuie analizat stadiul în care se află evaluarea respectivă. Acestea pot preciza printre altele stadiul în care se află o evaluare, care din testele efectuate nu au trecut, din ce motive şi ce măsuri trebuie luate pentru continuarea evaluării. Aceste rapoarte se trimit solicitantului care pe baza lui trebuie să decidă ce trebuie să facă (să modifice produsul, să completeze documentaţia etc) pentru a se putea continua procesul evaluare.

Avantajele obţinute prin automatizarea procesului de testare-evaluare folosind platforma dezvoltata in aceasta etapa a proiectului:

- Managementul coerent al procesului de testare-evaluare: conducătorul echipei de evaluare are la dispoziţie un instrument prin care poate planifica, controla şi optimiza activitatea echipei şi de asemenea are controlul asupra unor elemente esenţiale cum ar fi timpul necesar, resursele implicate şi modul în care acestea sunt utilizate în mod curent;
- Reducereasubstanţială a duratei procesului de testare-evaluare:estimăm o reducere cu 25-30% a timpului necesar, ceea ce se poate traduce uşor în economii de resurse financiare şi umane;
- Detectarea din faza incipientă a erorilor:având la dispoziţie instrumentul automatizat ce permite compararea facilă a modului în care un produs răspunde la cerinţele standardului conform căruia este evaluat, evaluatorul va putea evidenţia rapid erorile în proiectarea sau implementarea produsului evaluat;
- Concentrarea efortuluievaluatorului către identificarea vulnerabilităţilor:evaluatorul este degrevat de activitatea laborioasă de urmărire a elementelor cuprinse în standard şi identificare a aplicării acestora în produsul evaluat, putând astel să se concentreze preponderent pe identificarea acelor teste şi elemente care conduc către eventuale vulnerabilităţi ale produsului evaluat;
- Menţinerea actualizată a tuturor rezultatelor şi probelor obţinute pe parcursul procesului de evaluare: tot procesul poate fi urmărit şi înregistrat astfel încât să se respecte principiile reproductibilităţii şi repetabilităţii acestuia;
- Reducerea intervenţiei evaluatorului pe parcursul procesului: elementele ce ţin de standardul de evaluare, documentaţiile şi celelalte informaţii necesare derulării procesului, odată introduse în aplicaţie, vor putea fi utilizate pe tot parcursul procesului şi nu vornecesita intervenţii suplimentare din partea evaluatorului;

- Sincronizarea rezultatelor obţinute de mai mulţi evaluatori: aplicaţiile pot fi utilizate concomitent de mai mulţi membri ai echipei de evaluare, conform indicaţiilor conducătorului echipei de evaluare, urmând ca acesta din urmă să poată integra toate informaţiile la finalizarea activităţii;
- Controlul stadiului procesului de evaluare: în orice moment conducătorul echipei de evaluare va putea cunoaşte procentual care este stadiul procesului şi va putea identifica eventualele deficienţe în derulare aacestuia;
- Generarea facilă a documentaţiilor şi rapoartelor necesare în cadrul procesului de evaluare: pot fi obţinute automat în proporţie de 70-90% documente esenţiale precum raportul tehnic de evaluare, buletinele de masurători sau rapoartele conţinând observaţii sau solicitări de clarificare care sunt destinate solicitantului evaluării.

In livrabilul aferent acestei activitati, pe langa pachetele software dezvoltate, a fost realizata si o descriere detaliata a platformei de testare si evaluare de produse de securitate. Documentatia cuprinde elementele de proiectare si dezvoltare ale platformei si descrierea in detaliu ale aplicatiilor componenete ale platformei.