Raport științific si tehnic in extenso pentru proiectul *Canal securizat între dispozitivele I/O și unitatea de procesare pentru extinderea securității software (SABOTORE)*

Etapa III – Arhitectura de referință. Etică.
L3.1 Arhitectura hardware si software a soluției
L3.2 Problemele de etică privind protecția datelor utilizatorilor și raportarea la legislația GDPR

Cuprins

1 Introducere

1.1 Obiective

Etapa curenta, etapa numărul 3 a avut doua obiective:

Obiectivul 1 (Arhitectura): “Realizarea unei arhitecturi hardware/software generice”

Obiectivul 2 (Etica): “SABOTORE va include un set de utilizatori in fiecare soluție pe care o dezvolta, pentru a valida tehnologia dezvoltata in proiect. Consorțiul este pe deplin conștient de problemele de etica, de protecțiile datelor cu caracter personal ale fiecărui utilizator. In cadrul proiectului vom colecta si prelucra datele cu caracter personal, respectând in totalitate prevederile GDPR”

1.2 Activitati

Etapa a constat in doua categorii principale de activități, activități ce corespund celor doua obiective ale etapei. Prima categorie este aceea a realizării arhitecturii hardware si software a soluției prin care am definit toate componentele software si hardware ale soluției, precum si comunicarea dintre acestea (protocoalele de comunicație). In a doua categorie de activități am făcut o analiza asupra conceptului de etica in cercetare si, cu precădere, ne-am axat pe stabilirea modului in care proiectul curent realizează cu succes protejarea datelor personale ale tuturor entităților implicate in proiect

2 Arhitectura software si hardware

În această etapă scopul principal a fost acela de a realiza o arhitectură hardware/software generică. Pentru aceasta au fost întreprinse următoarele activități.

2.1 Identificarea caracteristicilor hardware necesare pentru dispozitivul SABOTORE

In aceasta etapa au fost analizate o serie de componente hardware care vor fi necesare in realizarea proiectului SABOTORE. Pe lângă toate componentele de legătură necesare (placa pe care vor fi puse componentele, rezistente, condensatoare, circuite de alimentare etc.) au fost identificate necesitățile de procesare si de interconectare:

- Autentificarea la standarde înalte de securitate, folosind algoritmi de tip curbe eliptice;
- Autentificarea sa fie compatibilă cu standardul USB (eventual modelul type-C);
- Suport pentru criptare simetrica, minim standardul Advances Encryption Standard 128 biți (AES-128);
- Suport pentru algoritmi de hashing, minim SHA256;
- Memorie suficienta pentru stocarea unui certificat de tip X.509 (acesta memorie trebuie sa ofere protecție împotriva atacurilor de tip side-channel, sa fie greu accesibila din exterior);
- Memorie suficienta pentru stocarea codului software (de tip EEPROM sau flash sau similar);
- Compatibilitatea cu 2 porturi USB (dispozitivul va avea un port USB-tata cu care se va conecta la calculator, si un port USB-mama prin intermediul căruia se vor conecta alte dispozitive externe, precum o tastatura);
- Generator de numere aleatoare;
- Procesare la minim 128MHz (din testele efectuate in versiunea anterioara de la care a plecat acest proiect);
- Spațiul de stocare pentru un sistem de operare minimal (aprox. 128 MB).

2.2 Identificarea noilor module de hardware

In urma analizei ofertelor existente in piața, in conformitate cu specificațiile hardware detaliate anterior, pentru producerea primelor 5 unități următoarele componente, am decis ca sunt necesare următoarele componente hardware:

Nr. crt.	Denumire dispozitiv	Cantitate
1	511-STM32F415RGT6TR STM32F415RGT6TR	5

2	726-SLS32AIA020X4MA4 SLS32AIA020X4USON10XTMA4	5
3	815-ABM3-25-B2-T ABM3-25.000MHZ-B2-T	5
4	701-SP6205EM5L33/TR SP6205EM5-L-3-3/TR Low Noise 500mA	2
5	998-MIC5216-3.3YM5TR MIC5216-3.3YM5-TR	2
6	998-MIC5319-3.3YD5TR MIC5319-3.3YD5-TR	2
7	595-TLV75533PDBVR TLV75533PDBVR	2
8	595-TPD2S017DBVR TPD2S017DBVR 2Ch Ultra Low Clamp	10
9	649-87520-0110BLF 87520-0110BLF USB S/D RECEPT	5
10	538-48037-0001 48037-0001 TYPE A RA SHLDED PLG	5
11	80-C0603C104M5R C0603C104M5RACTU 50V 0.1uF 0603 X7R	20
12	963-UMK316BBJ106KL-T UMK316BBJ106KL-T 1206 50VDC 10uF 10%	10
13	581-06035A180JAT4A 06035A180JAT4A 50V 18pF C0G 0603	10
14	556-AT24CS01-SSHM-B AT24CS01-SSHM-B S/N SEEPROM 1K	5
15	855-M20-7910442R M20-7910442R 4 WAY SIL HORIZ SMT	5

16	611-PTS636SP50SMTRLF PTS636 SP50 SMTR LFS	5
17	81-BLM18SP102SN1D BLM18SP102SN1D 0603 1000ohm 25%	10
18	710-150060AS75000 150060AS75000 WL-SMCW Mono LED	10
19	530-C1F375 C1F 375 1206 SMT Fuse	5

Important de menționat ca in prima etapa vom confecționa un produs de dimensiuni ceva mai mari pentru a putea fi ușor de depanat si de programat, iar când codul sau arhitectura hardware vor fi testate ele vor fi re-asamblate într-un format de dimensiuni reduse, similare unui dispozitiv de stocare USB.

2.3 Realizarea arhitecturii hardware

A fost realizata arhitectura hardware pentru testare, urmând ca cea finala sa necesite doar o rearanjarea a componentelor. Detalierea arhitecturii hardware poate fi analizata in livrabilul 3.1, prezentam aici doar schema bloc in Figura 1.

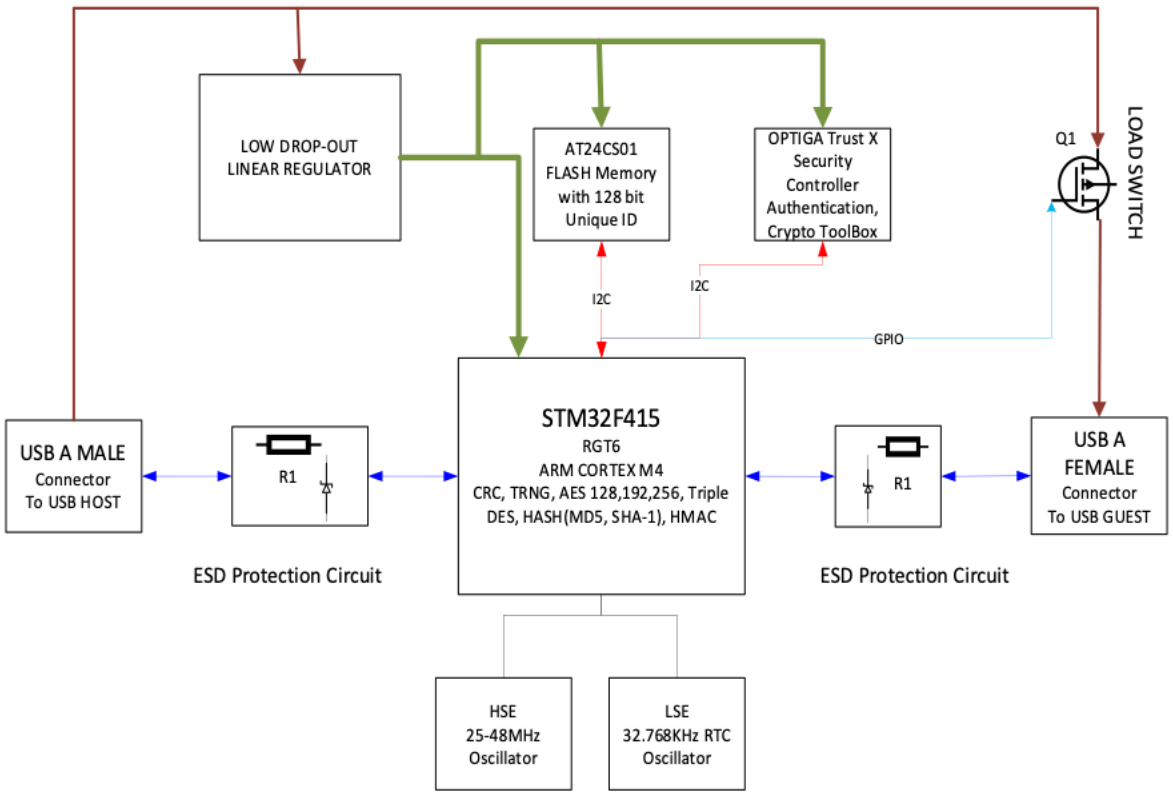

Figura 1 – Arhitectura hardware a dispozitivului SABOTORE

2.4 Realizarea arhitecturii software

In aceasta etapa a fost realizata si arhitectura software de baza, integrarea dispozitivului SABOTORE cu sistemul de operare si protocoalele de comunicare ce vor fi folosite in cele 3 scenarii identificate. Detalierea acestora este realizata in Livrabilul 3.1, mai jos realizam o introduce succinta in arhitectura software reprezentata in Figura 2.

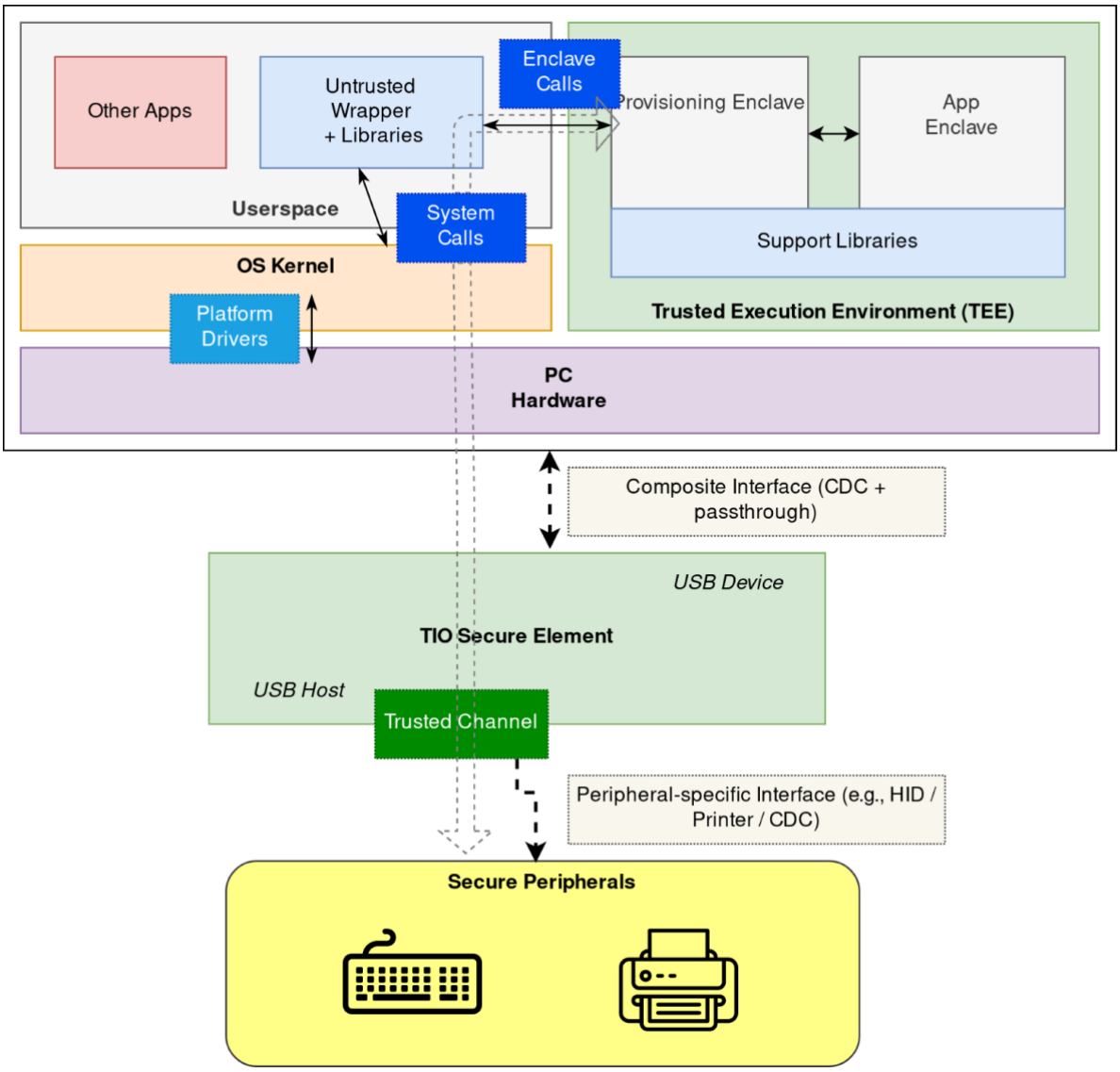

Figura 2 – Arhitectura software generică

In centrul arhitecturii software se afla componenta hardware Software Guard Extensions (SGX) oferita de către Intel in majoritatea procesoarelor moderne si componenta hardware dezvoltata in cadrul proiectului, dispozitivul SABOTORE (versiunea îmbunătățita a conceptului TIO de la care a pornit proiectul de fata).

Primul obiectiv ce trebuie realizat prin arhitectura software de fata este realizarea unui canal securizat intre cele doua componente, astfel încât prin SGX sa se poată oferi o putere de procesare mai mare in condiții de execuție securizate. Acest canal trebuie realizat o singura data, fără intervenția sistemului de operare (care este considerat maliții os in scenariile propuse). Acest pas va fi realizat prin pornirea calculatorului folosind un sistem de operare minimal, instalat pe dispozitivul SABOTORE, care va configura SGX cu o cheie publica de criptare.

Odată stabilita conexiunea sigura, aceasta poate fi folosita pentru realizarea scenariilor propuse:

- Pentru identificarea si autentificarea corecta a dispozitivului SABOTORE se va folosi aceasta cheie publica, astfel se va putea configura sistemul de operare sa accepte doar conexiuni USB prin dispozitivul nostru.
- Pentru criptarea dispozitivelor externe, cheia publică va fi folosita pentru protejarea unei chei simetrice de criptare, aceasta fiind cheia cu care se realizează criptarea/decriptarea fiecărui dispozitiv extern.
- Pentru imprimarea unor documente într-un mod securizat, se va atașa dispozitivul SABOTORE la imprimantă, documentul protejat va fi decriptat in interiorul enclavei oferite de SGX si se va trimite prin canalul securizat dintre SGX si dispozitivul nostru.

Mai multe detalii tehnice despre protocoalele folosite se regăsesc in livrabilul 3.1.

3 Alinierea la principiile de etică in cercetare si de GDPR

O prima activitate a fost aceea de analiza a cadrului legislative si a normelor in vigoare la momentul actual, atât in Romania cat si pe teritoriul Uniunii Europene: Ordonanța nr. 57 din 16 august 2002, LEGE nr. 206 din 27 mai 2004 privind buna conduită în cercetarea științifică, dezvoltarea tehnologică și inovare, Carta drepturilor Fundamentale a Uniunii Europene (2010/C 83/02), Recomandarea Comisiei Europene 2005/251/CE cu privire la Carta europeană a cercetătorului și Codul de conduită pentru recrutarea cercetătorilor, ALLEA (ALL European Academies 2017) - The European Code of Conduct for Research Integrity

3.1 Principiile fundamentale ale eticii in activitatea de cercetare si dezvoltare

In urma analizei au fost analizate cele mai importante principii de etica exprimate de acestea, precum integritatea persoanei, protecția datelor cu caracter personal, libertatea artelor și științelor exprimate in Carta drepturilor Fundamentale a Uniunii Europene

În vederea combaterii practicilor neetice, în martie 2005, Comisia Europeană adoptă Recomandarea 2005/251/CE cu privire la Carta europeană a cercetătorului și Codul de conduită pentru recrutarea cercetătorilor. Carta europeană a cercetătorului specifică rolurile, responsabilitățile și prerogativele cercetătorilor și angajatorilor. Carta și Codul conțin 40 de principii și condiții generale care sunt structurate pe patru dimensiuni: (i)aspecte etice și profesionale (ii) recrutare (iii) condiții de muncă și securitate social (iv) training.
Mergând pe aceste patru axe fundamentale, principiile etice ce au legătura cu activitatea profesionala sunt: libertatea de cercetare, responsabilitatea profesională, respectarea obligațiilor contractuale și legale, responsabilitatea, bunele practici în cercetare, distribuția și exploatarea rezultatelor, angajamentul public, relația cercetătorului cu supraveghetorii, îndatoriri de supraveghere și manageriale, dezvoltarea profesională continuă.
De asemenea, in cadrul „Codului european de etică pentru integritatea cercetării" elaborat de ALLEA, întâlnim câteva principii de etica referitoare la aspecte precum: credibilitatea, onestitatea, respectul, responsabilitatea, mediul de lucru, programele de training, supervizare și mentorat, procedurile de cercetare, elementele de securitate, managementul datelor, cercetarea în colaborare, publicarea și diseminarea rezultatelor cercetării, procesul de peer-review, evaluare și editare

Proiectul curent adera la practicile si principiile etice enunțate mai sus si le adopta, acolo unde este cazul. In livrabilul 3.2 se specifica principiile etice care se pot aplica in cadrul procesului de cercetare aplicat in proiectul curent.

3.2 Protecția datelor cu caracter personal in cadrul proiectului SABOTORE

Unul dintre cele mai importante principii care au fost analizate in detaliu in proiectul curent, in etapa numărul 3, este acela al protecției datelor cu caracter personal ale tuturor entităților implicate in acest proiect.
Astfel, după o analiza elaborata a legislației Europene, începând cu bine-cunoscutul regulament GDPR din 2016 (Regulamentul 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE) si a legislației naționale, precum Legea nr. 190 din 18 iulie 2018, Legea nr. 102/2005, deciziile ANSPDCP și Ghidul orientativ de aplicare a GDPR al ANSPDCP, dar si ghidurile și avizele Grupului de Lucru Articolul 29 privind Protecţia Datelor, in cadrul etapei am identificat datele personale care sunt prelucrate pe parcursul întregului proiect si am luat masuri astfel încât prelucrarea lor sa nu încalce drepturile persoanelor implicate in derularea proiectului de cercetare
Datele personale prelucrate, temeiul legal al prelucrării, scopul sau scopurile prelucrării lor, categoriile de persoane vizate, categoriile de date prelucrate, modul de informare a persoanei vizate precum si drepturile acesteia sunt exprimate in detaliu in Livrabilul 3.2, capitolul 4.

4 Diseminarea rezultatelor obținute

O data cu finalizarea celui mai important pas in conceperea soluției, si anume Arhitectura hardware si software, pentru diseminarea rezultatelor am completat site-ul proiectului https://sabotore.ro unde am publicat rezultatele obținute pana in prezent. Aici putem găsi, pe lângă aspectele informative ale proiectului, precum partenerii ce alcătuiesc consorțiul, sau planul de execuție a proiectului in cinci etape, si aspectele tehnice ale proiectului, precum arhitectura conceputa in etapa curentă.

Totodată, pe pagina web a certSIGN am completat secțiunea „Proiecte” (https://www.certsign.ro/ro/despre-noi/cercetare-si-inovare/proiecte/) cu câteva aspecte importante referitoare la proiectul nostru. Aceasta adăugare este importanta pentru etapa de diseminare a rezultatelor, deoarece site-ul web al partenerului coordonator este vizitat zilnic de mulți utilizatori, având, conform ultimelor statistici Google Analytics, in perioada 20 ianuarie – 16 februarie 2021, 331,449 de afișări pe pagina, din care 176,183 sunt afișări unice.

5 Concluzii

Prin identificarea modulelor hardware ce interacționează între ele într-un mod unitar, prin împărțirea soluției in componente, prin descrierea relațiilor dintre aceste componente, prin descrierea comunicației dintre ele si, mai ales, prin realizarea unui prototip hardware funcțional ce are rolul de a valida si demonstra corectitudinea arhitecturii, in aceasta etapa echipa de proiect a realizat obiectivul numărul unu al proiectului SABOTORE. In continuare, echipa va dezvolta si testa componentele software, urmând ca, in urma testelor de integrare software si hardware, sa revină, daca este cazul, si asupra arhitecturii software, pentru realizarea versiunii finale, complet funcționale si optimizate.

Prin analiza ampla asupra legislației, principiilor si bunelor practici etice in proiectele de cercetare, prin definirea conceptului de protecție a datelor cu caracter personal si prin aplicarea lor asupra datelor ce se prelucrează in cadrul proiectului, echipa a realizat îndeplinirea obiectivului numărul doi al proiectului: etica. In continuare, echipa de proiect va implementa practicile stabilite in aceasta etapa, prin directa colaborare cu departamentul de protecție a datelor, existent in certSIGN.