НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2019 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Цифрова реалізація ідентифікаційних документів на мобільних пристроях з гарантуванням автентичності

Виконав (-ла): студент (-ка) ____ курсу, групи _____
(шифр групи)

Блинков Володимир Геннадійович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Стьопочкіна Ірина Валеріївна_____ _____
(підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи, технології та математичні методи кібербезпеки»)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2019 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Блинков Володимир Геннадійович
(прізвище, ім'я, по батькові)

1. Тема дисертації Цифрова реалізація ідентифікаційних документів на мобільних пристроях з гарантуванням автентичності

науковий керівник дисертації к.т.н., доц. Стьопочкіна Ірина Валеріївна _____ ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «___» _____ 2019 р. № _____

2. Термін подання студентом дисертації 10.12.2019 р.

3. Об'єкт дослідження _____
_____

4. Вихідні дані _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____

_____
_____

7. Орієнтовний перелік публікацій _____
_____
_____

8. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Дана робота місить 90 сторінок, 14 ілюстрацій, 22 таблиці, 43 джерел за переліком посилань.

Актуальність роботи

Останнім часом в Україні велика увага приділяється питанням електронного урядування, і відповідно, забезпечення цифрової взаємодії зі своїми громадянами, що підвищило попит на надійні рішення електронної ідентифікації.

Існуючі рішення базуються на технологіях які потенційно вразливі до низки атак зловмисників. На жаль, розвиток як пристроїв, так і послуг обумовлено ринковим попитом, з акцентом на нові функції і частіше зневагою безпекою. Тому розробка більш захищеного рішення цифрової реалізації ідентифікаційних документів є необхідністю.

Мета і завдання дослідження

Метою роботи є дослідження існуючих рішень електронної ідентифікації, виявлення потенційних вразливостей та на основі аналізу представлення удосконалення технологій та рішень що можуть підвищити рівень безпеки ідентифікаційних документів що представлені на мобільних пристроях.

Завданням роботи є аналіз існуючих рішень електронної ідентифікація та визначення потенційних вразливостей, розробка архітектури більш захищеного рішення електронної ідентифікації на основі аналізу існуючих рішень, яке не буде вразливим до визначених атак, розробка програмного модуля що реалізує цифровий ідентифікаційний документ на мобільному пристрої за визначеною архітектурою, проведення NFC Relay Attack для перевірки захищеності та яка засвідчить працездатність запропонованого рішення.

Об’єкт дослідження – цифрові, електронні та мобільні ідентифікаційні документи.

Предмет дослідження – системи та технології реалізації цифрових ідентифікаційних документів.

Наукова новизна одержаних результатів

В роботі представлено нову архітектуру реалізації цифрових ідентифікаційних документів, отриману в результаті порівняльного аналізу існуючих рішень на ринку та використанню новітніх технологій по підвищенню рівня захищеності конфіденційних даних на мобільних пристроях. Розроблено модель розгортання системи мобільних ідентифікаційних документів, для можливості впровадження системи в реальних умовах. Запропоновано програмну реалізацію більш захищеного рішення мобільної ідентифікації, реалізовано модуль що реалізує цифровий ідентифікаційний документ на мобільному пристрої для ОС Android.

Практичне значення одержаних результатів

Практична цінність результатів роботи полягає у можливості використання даного рішення для представлення звичайних, фізичних документів на мобільних пристроях з гарантуванням автентичності, наприклад використовувати мобільний телефон як паспорт або водійське посвідчення. Та можливості використання рішення для систем контролю фізичного доступу до ресурсів або об’єктів. Також представлена модель розгортання даної системи що може допомогти в розгортанні систем цифрових ідентифікаційних посвідчень.

Ідентифікаційні документи, мобільний пристрій, конфіденційні дані, embedded Secure Element, Trusted Execution Environment, аплет, траслет, посвідчення особистості, рівень захищеності, ідентифікація

ABSTRACT

This work contains 90 pages, 14 figures, 22 tables, 43 sources of references.

Research motivation

Recently, in Ukraine, much attention has been paid to e-governance issues and, consequently, ensuring digital engagement with its citizens, which has increased the demand for robust electronic identification solutions.

Existing solutions are based on technologies that are potentially vulnerable to a number of attackers. Unfortunately, the development both devices and services is driven by market demand, with a focus on new features and more frequent with neglect of security. Therefore, developing a more secure digital ID solution is a necessity task.

Goals and Objectives of research

The purpose of the study is to investigate existing electronic identification solutions, identify potential vulnerabilities and to analyze the performance of technology enhancements and solutions that can enhance the security of identification documents presented on mobile devices.

The objective of the work is the analysis of existing solutions for electronic identification and identification of potential vulnerabilities, the development of a more secure solution for electronic identification based on the analysis of existing solutions that will not be vulnerable to certain attacks, the development of a software module that implements a digital identification document on a mobile device by a specified architecture, provide NFC Relay Attack for security testing and validation of the proposed solution.

Object of research – digital, electronic and mobile identification documents.

Subject of research – systems and technologies of implementation of digital identification documents.

Scientific novelty of the results

The paper presents a new architecture for the implementation of digital identification documents, obtained as a result of a comparative analysis of existing solutions in the market and the use of the latest technologies to improve the security of

sensitive data on mobile devices. The model of deployment of the system of mobile identification documents has been developed for the possibility of implementation of the system in real conditions. A software implementation of a more secure mobile identification solution is proposed, and a module that implements a digital ID document on a mobile device for Android OS is implemented.

Practical significance of the results

The practical value of the work results is the ability to use this solution to present ordinary, physical documents on mobile devices with authentication guaratee, such as using a mobile phone as a passport or a driver's license. And the ability to use solutions to provide physical access control to resources or objects. A deployment model for this system is also provided that can assist in the deployment of digital identification systems.

Identity Documents, mobile device, confidential data, Embedded Secure Element, Trusted Execution Environment, applet, trustlet, identity card, assurance level, identification

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів 10

Вступ 11

1 Мобільні ідентифікаційні документи 14

1.1 Поняття ідентифікаційних документів 15

1.2 Варіанти використання 16

1.3 Існуючі рішення на ринку 18

1.4 Електронна ідентифікація 19

1.5 Переваги електронних документів 20

1.6 Недоліки електронних документів 21

1.7 Технології реалізацій мобільних ідентифікаційних документів 22

Висновки до розділу 1 28

2 Технології реалізацій мобільних ідентифікаційних документів 30

2.1 Аналіз та порівняння існуючих рішень 30

2.2 Атаки на SIM карту 33

2.3 Атаки на смарт картки 37

2.4 Розробка архітектури системи цифрових ідентифікаційних документів на мобільних пристроях 40

Висновки до розділу 2 44

3 Реалізаця мобільних ідентифікаційних документів та нова модель розгортування системи 46

3.1 Програмна реалізація 46

3.2 Розробка моделі розгортання системи 53

3.3 Перевірка захищеності рішення шляхом відтворення NFC Relay Attack 54

Висновки до розділу 3 56
4 Розробка стартап проекту 58
4.1 Опис ідеї проекту 58
4.2 Технологічний аудит ідеї проекту 60
4.3 Аналіз ринкових можливостей запуску стартап-проекту 62
4.5 Розроблення маркетингової програми стартап проекту 78
Висновки до розділу 4 82
Висновки 84
Перелік джерел посилань 86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

eSE – embedded Secure Element

TEE – Trusted Execution Environment

REE – Rich Execution Environment

APDU – Application Protocol Data Unit

TUI – Trusted User Interface

CBOR – Concise Binary Object Representation

JC – JavaCard

ID – Identity, identification

SIM – Subscriber Identification Module

API – Application Programming Interface

ОС – Операційна Система

JCOP – Java Card OpenPlatform

JCVM – Java Card Virtual Machine

ICAO – International Civil Aviation Organization

SD – Security Domain

EAL – Evaluation Assurance Level

ARM – Advanced RISC Machine

NFC – Near Field Communication

ВСТУП

На сьогоднішній день мобільні телефони стали невід’ємною частиною життя. Сучасні мобільні пристрої дозволяють виконувати безліч різноманітних операцій, від звичайних дзвінків до складних банківських операцій. Ці пристрої стали звичайним явищем за останні кілька років, об'єднуючи кілька технологій бездротових мереж для підтримки додаткових функцій і послуг.

По мірі того, як все більше і більше урядів вступають на шлях електронного уряду, забезпечення цифрового взаємодії зі своїми громадянами підвищило попит на надійні рішення для електронної ідентифікації, які можуть забезпечити однозначну відповідність між електронною та фізичною особистістю. Поряд з цією тенденцією, доступність і поширення мобільних пристроїв перетворилися в сильний поштовх для урядів щодо диверсифікації каналів електронної ідентифікації шляхом розробки цифрової ідентифікації на мобільних пристроях, також відомої як мобільна електронна ідентифікація. Мобільна електронна ідентифікація пропонує громадянам однозначну ідентифікацію, автентифікацію і кваліфіковані електронні підписи, і вона вже була успішно впроваджена в деяких країнах в масштабі всієї країни.

У сучасних дослідженнях мобільна електронна ідентифікація вивчається з не технічної точки зору, з фокусом на потенційних моделях розгортання, проте мало що відомо про проблеми, з якими стикається країна при впровадженні мобільних ідентифікаційних документів з ширшим числом громадян тобто користувачів. Та які технічні аспекти безпеки повинні враховуватись при впровадженні даної системи, також які можливі проблеми безпеки можуть бути на шляху впровадження мобільних ідентифікаційних документів. Вирішуючи цю проблему, в даній роботі проводиться тематичне дослідження по загальнонаціональним рішенням для мобільної та електронної ідентифікації, щоб дослідити які бар'єри для мобільного електронної ідентифікації з точки зору

безпеки можуть виникати. Та яким чином можна вдосконалити безпечність системи на мобільних пристроях.

Відповідно з зростанням попиту мобільних пристроїв та електронної ідентифікації особистості, актуальним залишається питання безпеки таких систем.

Метою роботи є пошук існуючих способів електронної та мобільної ідентифікації особистості, порівняння технологій які використовуються в даних методах та аналіз рівня безпеки конфіденційних даних користувачів таких рішень. Пошук та аналіз можливих рішень представлених на мобільних пристроях. Дослідження нових технологій що можуть підвищити рівень безпеки конфіденційних даних на мобільних пристроях.

Завданнями даної роботи є:

1. Пошук та аналіз існуючих способів електронної та мобільної ідентифікації.

2. Аналіз технологій що забезпечують безпеку даних в існуючих рішеннях електронної ідентифікації.

3. Виявлення вразливостей та можливих атак які можна застосувати до існуючих рішень електронної ідентифікації.

4. Визначення нових технологій підвищення рівня безпеки конфіденційних даних на мобільних пристроях.

5. Розробка більш захищеного рішення мобільної ідентифікації на основі аналізу існуючих рішень та впровадження нових технологій підвищення рівня безпеки конфіденційних даних на мобільних пристроях.

6. Розробка програмної частини цифрових ідентифікаційних документів на мобільних пристроях.

7. Проведення NFC Relay Attack для демонстрації захищеності представленого рішення.

8. Розробка моделі розгортання системи цифрових ідентифікаційних посвідчень на мобільних пристроях.

Об’єктом дослідження даної роботи є цифрові, електронні та мобільні ідентифікаційні документи.

Предметом дослідження даної роботи є системи що реалізують цифрові ідентифікаційні документи та рівень безпеки конфіденційних даних який вони надають.

Практична значення роботи полягає у можливості використання даного рішення для представлення звичайних, фізичних документів на мобільних пристроях з гарантування автентичності, наприклад використовувати мобільний телефон як паспорт або водійське посвідчення. Також представлена модель розгортання даної системи може допомогти в розгортанні систем цифрових ідентифікаційних посвідчень.

.

1 МОБІЛЬНІ ІДЕНТИФІКАЦІЙНІ ДОКУМЕНТИ

Особистість людини унікальна. Вона складається з набору характеристик і ознак, якими ніхто інший не володіє і які визначають цю людину і роблять її впізнаваною для інших. Вони постійні і не змінюються з часом. Як суспільство, ми повинні мати інструменти для перевірки того, що людина є тим, ким, за її словами, вона є, перш ніж надавати доступ до обмеженої або захищеної інформації або до надання яких небудь послуг [1].

З широким використанням Інтернету і онлайн-сервісів; з'явилася концепція цифрової особистості, яка відноситься до будь-яких даних, які можуть бути використані для унікального опису людини, і містить інформацію, що стосується відносин між цією людиною та його її онлайн або цифровий активністю.

Люди мають набір різних цифрових ідентифікаційних даних, такі як облікові записи електронної пошти, профілі в соціальних мережах або облікові записи онлайн-банкінгу [1]. Існують дві основні проблеми, пов'язані з цифровими ідентифікаційними даними, перша з яких полягає в правильному управлінні паролями, оскільки користувачі зазвичай недостатньо дисципліновані в цьому питанні або не знають, як важливо зберігати свою особистість в безпеці, а друга - уникати крадіжки особистих даних, що може призвести до фінансових, емоційних, тощо негативних наслідків для жертв.

У цьому контексті можна розглядати мобільний телефон як постійно підключений, персональний багатофункціональний пристрій, який завжди в межах досяжності людей. Мобільні пристрої стали безпечним і досить зручними, так як містять ідентифікаційні дані свого власника та надійно інтегрують атрибути, які безпомилково ідентифікують власника як у фізичному, так і в цифровому світі та являють собою ключовий елемент в об'єднанні фізичної та цифрової особистості. З огляду на можливості, мобільні пристрої можуть виступати як фізичний доказ або смарт-карти (оскільки смарт-карти містять інформацію, яка тісно пов'язана з відповідними ідентифікаційними даними

окремих осіб у вигляді чіпа, яка надійно зберігається всередині мобільного пристрою в незмінних умовах), в якості пристрою автентифікації (наприклад, при відправці одноразових паролів в рамках процедур онлайн-банкінгу) або в якості надійного власника особистості (наприклад, для документів, що вимагають цифровий підпис).

1.1 Поняття ідентифікаційних документів

Ідентифікаційний документ – це будь-який документ, який може вживатися для підтвердження та засвідчення особи. У більшості країн це може бути паспорт, водійське посвідчення тощо. [1]

Ідентифікаційні документи, використовується для зв'язку людини з інформацією про цю людину, зазвичай яка знаходиться в базі даних. Фотографія використовуються для зв'язку людини з документом. Зв'язок між документом, що засвідчує особу, та інформаційною базою даних базується на особистій інформації, що міститься в документі [1], такій як повне ім'я власника, вік, дата народження, адреса, номер карти, стать, громадянство, ідентифікаційний номер і багато іншого.

Електронний ідентифікаційний документ – це захищений документ, який гарантує захист фізичного і цифрового посвідчення його власника з використанням найсучасніших стандартів безпеки і захисту від підробок. Персональні дані власника документа, включаючи біометричні дані, належним чином зібрані й записані в електронний чіп. [2] Ці дані підписані довіреною стороною в цифровій формі і не можуть бути змінені. Це гарантує швидку і ефективну ідентифікацію власника документа і перевірку документа після цього.

Загальні проблеми, які пов'язані з електронними документами це:

- Для можливості використання повинні бути наявні електронні пристрої, захищені від зловживань і некоректного використання, які однозначно підтверджують, особистість в електронних транзакцій. [3]

- Відповідні дані повинні бути достовірними і вважатись автентичними. [3]
- Робота з такою системою електронної ідентифікації потребує адекватних правових положень з точки зору захисту даних і персонального контролю особистих даних. [3]

Цифрове посвідчення особи – це фізичний токен, який містить особисту інформацію, використовувану для доказу того, що власником є конкретна особа, громадянин даної країни. [3]

Біометрія також розглядається, як ряд методів, щоб довести, що людина являє собою того, ким вона є за її словами, використовує свої фізичні особливості (такі як фотографія, відбитки пальців, сканування рук, малюнки очей, малюнки вух) або поведінку (наприклад, розпізнавання голосу , підпису). Кілька країн в даний час запроваджують паспорта і електронні посвідчення особи, включаючи біометричну інформацію, для підтвердження того, що їх власником є конкретна особа.

1.2 Варіанти використання

Найбільш очевидне і поширене використання мобільного посвідчення особи відбувається в формі державної ідентифікації громадян. Мобільний ідентифікатор не тільки надає державним органам більш безпечний спосіб ідентифікації громадян, але і оптимізує інфраструктуру і знижує витрати на розгортання, забезпечуючи широкий спектр електронних послуг [4]. З огляду на те, що більшість громадян вже мають мобільні пристрої, які можна використовувати для розміщення мобільних ідентифікаторів, розгортання мобільного ідентифікатора може привести до дематеріалізації будь-яких загальнодоступних послуг, пов'язаних з автентифікацією і ідентифікацією громадян таких як:

- Цифрове голосування
- Збір податків

- Доступ до програми соціального забезпечення:
- Реєстратор переписів і населення
- поліцейські служби

Крім спрощення взаємодії між громадянами, мобільний ідентифікатор може бути корисним для взаємодії між урядами [4]. Такі взаємодії включають, наприклад, міжвідомчу автентифікацію в якості співробітника або підрядника і визначення заснованого на політиці доступу до ресурсів стороннього агентства. В цілому, програми цифрової ідентифікації можуть сприяти міжвідомчої обміну інформацією про громадян шляхом створення децентралізованої системи унікальних ідентифікаторів для громадян, яка дозволяє агентствам пов'язувати дані в своїх відповідних базах даних

Також видана урядом цифрова ідентифікація може бути корисна для підприємств, наприклад, при встановленні права на роботу, підприємства також можуть отримати вигоду з використання мобільної ідентифікації [5] в якості заміни або доповнення до своїх існуючих корпоративних систем пропуску та авторизації. Це включає надання співробітникам і підрядникам доступу як до фізичних засобів, так і до онлайн-систем з використанням централізованої, безпечної системи ідентифікації. [6]

Система мобільної ідентифікації для охорони здоров'я може бути дуже схожа на систему для підприємств – наприклад, підтримуючи облікові записи і автентифікацію для постачальників медичних послуг [7] – важливість охорони здоров'я означає, що цифрова ідентифікація може забезпечити додаткові переваги:

- Відстеження записів пацієнтів
- Обмін інформацією про пацієнтів
- Реєстрація пацієнтів
- Відстеження та контроль виписаних рецептів на ліки
- Медичне страхування

Фінансові установи можуть не тільки підвищити безпеку і скоротити витрати на шахрайство за допомогою цифрової ідентифікації, а також мобільна

ідентифікація може надати зручну форму цифрового підпису, що дозволяє створювати нові безпечні фінансові та банківські програми. Як приклад PostFinance [8] в Швейцарії пропонує своїм клієнтам послуги мобільного ідентіфікації17. У Туреччині клієнти банків в декількох банках можуть використовувати мобільний ідентифікатор для онлайн-банкінга. [9]

Ідентифікація в даний час використовується різними способами в комерційних застосунках, починаючи від перевірки віку для транзакцій з обмеженим доступом (наприклад, алкоголь, тютюн, вогнепальна зброя), до перевірки законного права на послуги (наприклад, перевірка водійських прав на послуги прокату автомобілів) і ідентифікації для бронювання (наприклад, авіакомпанія і готель). Хоча мобільна ідентифікація може служити більш зручним способом включення цих послуг, інновації за допомогою мобільних застосунків можуть забезпечити нові способи надання цих послуг.

1.3 Існуючі рішення на ринку

На європейському ринку є п'ять країн які пропонують послуги мобільної ідентифікації:

Естонія, носій глобального стандарту завдяки широкому спектру кінцевих послуг, які використовують мобільну ідентифікацію, а також співпраці між провайдерами, операторами і органами державного управління [10]. Естонія визнана однією з найрозвиненіших країн світу. У чіпі карти зберігається пара ключів, що дозволяє користувачам криптографічно підписувати цифрові документи на основі принципів криптографії з відкритим ключем з використанням DigiDoc [11]. Згідно естонського законодавства, з 15 грудня 2000 року криптографічний підпис юридично еквівалентний для особистого підпису. Естонське електронне ідентифікаційне посвідчення особи також використовується для автентифікації в амбітній інтернет-програмі голосування. [12]

Фінляндія є яскравим прикладом взаємодії з її домовленостями між національними операторами мобільного зв'язку про взаємодію зі службою для автентифікації користувачів при доступі до сторонніх послуг [13]. Фінляндія має один з найвищих показників в світі з точки зору впровадження мобільного телефонного зв'язку.

Норвегія, лідер в банківській сфері, де користувачі можуть отримати доступ до послуг мобільного банкінгу і виконувати фінансові операції завдяки розвиненій системі мобільної ідентифікації. [14]

Туреччина, прапороносець для мобільних підписів [9], оскільки відповідно до чинної правової бази підписи часто потрібні для виконання ряду операцій, коли для виконання цих операцій підпис не потрібен в інших країнах.

Швейцарія, з її пріоритетом зробити користувальницький досвід ключовим елементом в масовому впровадженні кінцевих послуг. [15]

І, нарешті Сполучене Королівство та його пілотне дослідження, присвячене вивченню приватного життя [16], який був просунутий урядом за участю всієї галузі, запрошеної взяти участь, гарантуючи повну прозорість для громадськості на основі згоди.

1.4 Електронна ідентифікація

Цифрова ідентифікація – це будь-які дані, які однозначно описують людину і містять інформацію про їхні стосунки як частини їх онлайн або цифровий активності. [17]

Мобільна ідентифікація - це безпечна інтеграція атрибутів, які безпомилково ідентифікують людину в фізичному і онлайн-світах всередині мобільного телефону. [17]

Мобільна ідентифікація – це розвиток онлайн-автентифікації і цифрових підписів, коли SIM-карта мобільного телефону служить інструментом ідентифікації. Мобільна ідентифікація забезпечує юридично обов'язкову

автентифікацію і підписання транзакцій для онлайн-банкінгу, підтвердження платежів, корпоративних послуг і споживання онлайн-контенту [17]. Сертифікати користувача зберігаються на SIM-карті оператора зв'язку, і для їх використання користувач повинен ввести особистий секретний PIN-код. При використанні мобільної ідентифікації окремий пристрій для читання карт не потрібен, оскільки сам телефон вже виконує обидві функції.

Загалом, «електронна ідентифікація» – це засіб, за допомогою якого люди можуть в електронному вигляді довести, що вони є тими, ким себе називають, і таким чином отримати доступ до послуг. Ідентифікація дозволяє відрізнити суб'єкт (громадянин, бізнес, адміністрацію) від будь-якого іншого суб'єкта. [3]

Рисунок 1.1 – Мобільний пристрій є ключовим елементом фізичної і цифрової конвергенції особистості.

1.5 Переваги електронних документів

Автентичність документів. Максимально можливий рівень захисту документів, завдяки чому документ практично неможливо підробити або фальсифікувати. Вбудовані рішення для управління життєвим циклом документів «захищають» особисті дані у всіх ситуаціях використання документів: персоналізація і видача документів, перевірка документів при переміщенні і перетині кордонів, перевірка віку, доступ до державних послуг тощо. [4]

Підтримка електронних (онлайн) послуг. Сумісна електронна ідентифікація є ідеальним інструментом доступу до всіх видів електронних послуг будь-якого уряду. Це надає можливість для індивідуального надання послуг як в публічній, так і в приватній сфері. Прикладами є виділений доступ до державних баз даних, персоналізований доступ до веб-сайтів. Без електронної ідентифікації електронний уряд не зможе вийти за рамки надання доступу до загальної інформації.

Обмеження можливостей для шахрайства, крадіжки особистих даних і фішингу. Шахрайство з ідентифікаційними даними - це зростаюча проблема з передбачуваним впливом в кілька мільярдів євро на рік. [3] Крадіжка особистих даних, фішинг і шахрайство – це серйозні загрози, з якими уряди повинні боротися, щоб підтримувати довіру громадськості до своїх електронних послуг. Необхідний достатній базовий рівень безпеки, який може бути отриманий за допомогою електронного посвідчення особи.

1.6 Недоліки електронних документів

Витрати. Електронна ідентифікаційна інфраструктура потребує великої кількості фінансів. Більш того, враховуються не тільки витрати на компоненти системи, а й організаційні витрати, такі як випуск карти і реєстрація власника карти. Відповідне економічне обґрунтування має включати вигоди, одержувані в результаті численних проектів, як для уряду, так і для приватного сектора. [19]

Сумісність. Кілька схем ідентифікації розгортаються на основі сектора / країни. На даному етапі не гарантується сумісність [19]: існує безліч стандартів і відсутній загальноприйнятий стандарт, відображення інформації про ідентичність в транскордонних транзакціях не є прямим, а фізичні контейнери, які використовуються для зберігання електронних посвідчень, розрізняються (смарт-карта, банківська карта, SIM / мобільний телефон ...).

Юридичні труднощі. Нинішні правові рамки не є однозначно визначеними і потребують прийняття необхідних норм та законів для регулювання електронної ідентифікації на рівні держави.

Конфіденційність. Конфіденційність є великою проблемою для кінцевих користувачів. Людина втрачає контроль, коли стикається з такими діями, як профілювання, поведінковий аналіз, соціальне сортування, динамічне ціноутворення, чорні списки, постійний нагляд. Використання унікального ідентифікатора, може призвести до погіршення ситуації. Однак при налаштуванні архітектури на основі ідентифікаторів є можливість надати користувачам контроль над інформацією, якою вони діляться зі службами. Крім того, засоби підвищення конфіденційності можуть бути вбудовані в структуру інфраструктури електронних документів для чіткого поділу різних секторів, в яких користувач активний.

1.7 Технології реалізацій мобільних ідентифікаційних документів

1.7.1 JavaCard

Технологія Java Card є підмножиною мови програмування Java в поєднанні із середовищем виконання, яка оптимізована для крихітних вбудованих пристроїв з дуже обмеженими обчислювальними ресурсами таких як смарт-карти [20] та

елементи безпеки. Середовище виконання складається з віртуальної машини Java Card [21], API-інтерфейсу, специфічного для Java-карти, і функцій безпеки, специфічних для Java-карти. Основне призначення продукту – застосування в смарт картках. У зв'язку з цим основний акцент був зроблений на підтримку стандартних криптоалгоритмів. Java Card дає можливість безпечним чином встановлювати і виконувати невеликі Java- застосунка (аплети) на смарт-картах та інших пристроях з вельми обмеженим обсягом пам'яті які мають в собі віртуальну машину Java Card та Java Card ОС. Ця платформа дозволяє програмувати пристрої і робити їх адаптованими під конкретне застосування. Java Card широко використовується в SIM-картах, банківських картках, електронних ідентифікаційних картках та інших видів смарт. [22]

Основні принципи які враховувались при розробці технології Java Card – це: переносимось та безпека.

Java Card описує стандартну середу виконання на смарт-картах з метою дати можливість одному і тому ж застосунку працювати на різних пристроях. Досягається це тим самим підходом як і в стандартній Java, аплет який було написано один раз може бути встановлений на будь-яку смарт-картку яка містить віртуальну машину Java Card та Java Card ОС [22] необхідної версії і стандартизовані бібліотеки класів, що дозволяє аплету значно абстрагуватися від особливостей конкретних моделей смарт-карт. Також є Java Card OpenPlatform (JCOP) комплекс заходів для розробки єдиного стандарту операційної системи з віртуальною машиною Java Card [21] для систем сильної ідентифікації особистості і платіжних систем. Розроблений IBM з широкою інтеграцією з організаціями GlobalPlatform, ICAO. На сьогодні є практично синонімом JCVM.

Безпека забезпечується різними властивостями платформи:

- Приховування даних. Програми запускаються в ізольованому середовищі (віртуальна машина Java Card) [21] і можуть отримувати доступ до операційної системи і апаратного забезпечення тільки через спеціалізовані інтерфейси;

- Екран (екранування) аплетів. Кілька аплетів можуть бути активними одночасно, проте вони ізольовані за моделлю «пісочниці» [21]: для застосунка виділяється контекст, до даних якого воно має доступ. Дані інших застосунків огороджені екраном. Для забезпечення спільної роботи декількох застосунків є механізм перемикання контекстів, який виконується через процес, контрольований віртуальною машиною [21];
- Криптографія. Підтримуються популярні алгоритми шифрування, такі, як DES, 3DES, AES, RSA [22]. Також підтримуються інші криптографічні сервіси: цифрові підписи, генерування електронних ключів, обмін цими ключами иа криптографія на еліптичних кривих;
- Механізм аплетів. Аплет Java Card – це, по своїй суті, скінчений автомат, який приймає дані, обробляє вхідні команди і відповідає, повертаючи дані або інформацію про статус;

Аплети Java Card не слід плутати з апплетами Java через ідентичні назви – аплет. Аплет JavaCard – це Java-програма, яка дотримується ряду угод, що дозволяють запускати її в середовищі виконання JavaCard. Аплет Java Card не призначений для роботи в середовищі браузера [21]. Причина за якою назва аплет була обрана для застосунків Java Card, полягає в тому що аплети Java Card можуть бути завантажені в середу виконання Java Card після того, як карта була виготовлена. Тобто, на відміну від застосунків в багатьох вбудованих системах, аплети не потрібно записувати в ПЗП під час виробництва, вони можуть бути динамічно завантажені на карту пізніше [22].

1.7.2 Embedded Secure Element

В контексті мобільних пристроїв треба враховувати, що Flash-пам'яті не можна довіряти. Несанкціонований доступ або маніпулювання даними

сторонніми застосунками є серйозною загрозою безпеки для критично важливих систем [23]. Одна зі спроб вирішити цю проблему – використовувати безпечне обладнання для безпечного зберігання критично важливих застосункі і даних. Embedded secure element (eSE) забезпечує таке середовище, де апаратна реалізація забезпечує захист від несанкціонованого доступу.

eSE являє собою окремий процесор зі своєю власною операційною системою, постійною та оперативною пам’яттю відокремлений від звичайної операційної системи мобільного телефона. eSE є надійною та захищеною від несанкціонованого доступу середою виконання. Він заснований на технологіях смарт-карт [23]. Java і MultOS – дві популярні операційні системи для цього середовища виконання. Global Platdorm опублікувала докладні специфікації для смарт-карт і реалізації eSE [24]. Середовище виконання eSE складається з різних типів віртуальних машин. Ці віртуальні машини є по суті виконуваними модулями, що містять програми та дані. Віртуальна машина кожної програми eSE пов'язана з виконуваною віртуальною машиною, званої Security Domain (SD), яка містить брандмауер. Цей зв'язок і ізоляція гарантується середовищем виконання карти. SD відповідає за безпечне зберігання ключів і за криптографічні операції. Після ініціалізації eSE першою встановленою віртуальною машиною є диспетчер карт (Card Manager) [24], а першим створеним доменом безпеки є домен безпеки емітента. Також створюється середовище виконання Global Platform (OPEN). OPEN відповідає за безпечну архітектуру eSE і реалізує ізоляцію застосунків і API-функції між застосунками eSE і Card Manager. Диспетчер карт відправляє і отримує APDU для застосунків eSE, використовуючи OPEN API, і навпаки. Card Manager має глобальний доступ до eSE і всіх інших застосунків eSE і доменів безпеки. Card Manager діє як інтерфейс між встановленими застосунками eSE і зовнішнім світом. Він також діє як проксі для інших застосунків eSE і перенаправляє всі APDU відповідними програмами у eSE, якщо тільки APDU не спрямовані до самого себе. Диспетчер карт також надає послуги з перевірки власника карти, по суті, послуги перевірки PIN-коду.

Іншими словами eSE - це смарт-карта, вбудована в мобільний пристрій виробником пристрою. eSE має обмеження контролю доступу, встановлені виробником пристрою. Отже, застосунки та необхідні дані можуть бути надані або встановлені лише виробником пристрою.

eSE які встановлюють в смартфони сертифікуються за рівнем Evaluation Assurance Level (EAL)5+ [25] що дозволяє розробнику отримати максимальну гарантію від проектування безпеки, заснованого на строгих комерційних методах розробки, підтримуваних помірним застосуванням спеціалізованих методів проектування безпеки, інакше кажучи надійність даних які зберігаються на eSE гарантується навіть при фізичному доступі зловмисника до пристрою.

1.7.3 Trusted Execution Environment

Trusted Execution Environment (TEE) – це захищена область в головному процесорі мобільного телефону, яка забезпечує безпечне виконання довірених застосунків. Він також надає механізми для безпечного зберігання конфіденційних даних, таких як дані платіжних карт [26]. TEE використовує власну операційну систему, яка відокремлює апаратні і програмні ресурси від основної мобільної операційної системи. TEE забезпечує контроль доступу для захисту доступу до конфіденційних даних і виконання довірених застосунків. Одна з популярних реалізацій TEE знаходиться в мобільних процесорах ARM яка називається TrustZone [27]. У цій структурі процесорні ядра розділені на два віртуальних ядра, які представляють нормальний світ і безпечний світ відповідно. За замовчуванням безпечний світ може отримати доступ до всіх станів нормального світу, але не навпаки. Це створює ще один рівень привілеїв виконання на додаток до традиційного розрізнення режимів користувача і ядра. Перемикання між двома світами ретельно контролюється режимом монітора. Цей режим є режимом з більш високими привілеями, який може управляти режимом,

який повинен бути активним [26]. Крім того, кожен віртуальний процесор має доступ до свого власного блоку управління віртуальною пам'яттю. Кеш-пам'ять має додаткові біти тегів, щоб визначити, чи вміст кешований в безпечному або звичайному світі.

Незважаючи на свої переваги, TEE схильний до атак клонування, атакам по побічним каналам та атак які змінюють поведінку TEE (наприклад, використання атак з переповненням буфера), щоб отримати доступ до конфіденційних даних або змусити TEE виконувати несанкціоновані сервіси [27].

Також TEE містить в собі Trusted User Interface (TUI). TUI – це особливий режим, в якому мобільний пристрій контролюється TEE – захищеною областю, яка знаходиться в головному процесорі смартфона. Довірений користувацький інтерфейс перевіряє, що інформація, яка відображається на екрані мобільного пристрою, надходить із затвердженої довіреної програми та ізолюється від звичайного світу, звичайної операційної системи, яка вразлива для атак шкідливих програм [28]. Таким чином TUI являє собою користувацький інтерфейс на якому відображаються конфіденційні дані, які не можуть бути скопійовані або підроблені.

Довірена програма виконується в контексті TEE і захищений програмним забезпеченням і криптографічного ізоляцією. Такий застосунок зазвичай являє собою невеликий набір двійкового коду, який реалізує API-інтерфейси TEE [29]. Вони криптографически підписані, надійно завантажені і відповідають за транзакції, чутливі до безпеки. Довірена програма також відома як траслет. Будь-який траслет зв'язується з іншими застосунками, такими як застосунки в ОС Android, через клієнтський API TEE, який забезпечує інтерфейс зв'язку між безпечним ядром і звичайною операційною системою пристрою. Крім того, траслети також мають доступ до безпечного сховища в TEE. TA полегшує створення безпечного каналу з іншими довіреними об'єктами, такими як eSE, з метою обміну чутливими даними безпеки. Він грає ключову роль в надійному

зборі облікових даних користувача і виконанні операцій, чутливих до безпеки [29].

1.7.4 Near Field Communication

NFC якщо дослівно перевести – це комунікація ближнього поля; технологія бездротової передачі даних на не великі відстані, яка дає можливість обміну даними між пристроями, що підтримують дану технологію та протокол та що знаходяться на відстані не більше 10 сантиметрів [30], але зазвичай ця відстань не перевищує декількох сантиметрів. Багато експертів стверджують, що NFC дійсно дуже безпечна технологія завдяки своїй надзвичайно малої відстані дії. Щоб зловити сигнал NFC, зловмисник повинен знаходитись дуже близько до пристрою. Незручно близько. Іншими словами, зловмиснику необхідно буде доторкнуться пристроєм зчитування для можливості зловити сигнал.

Висновки до розділу 1

В межах даного розділу було розглянуто поняття ідентифікаційних документів загалом, на основі цього визначено що таке електроні та мобільні ідентифікаційні документи, їхні складові, та варіанти представлення. Також було розглянуто рішення які вже існують на ринку та визначено можливі варіанти та сценарії використання електронних ідентифікаційних документів. Було дано поняття електронної ідентифікації що включає в себе електронну, цифрову та

мобільну ідентифікацію. Наступним кроком було визначено сильні та слабкі сторони цифрових ідентифікаційних документів, їх переваги та недоліки на фоні фізичних документів. Останнім було досліджено та описано нові технології підвищення рівня безпеки конфіденційних даних на мобільних пристроях які можуть бути використані для реалізації системи цифрових ідентифікаційних документів на мобільних пристроях.

2 ТЕХНОЛОГІЇ РЕАЛІЗАЦІЙ МОБІЛЬНИХ ІДЕНТИФІКАЦІЙНИХ ДОКУМЕНТІВ

2.1 Аналіз та порівняння існуючих рішень

Естонія запустила програму електронних посвідчень особи в 2000 році і встановила національні керівні принципи для створення обов'язкового національного посвідчення особи. Ідентифікаційна карта була створена для використання в якості фізичного і електронного ідентифікатора. Закон говорить, що національне посвідчення особи буде містити цифрові дані, що дозволяють громадянам здійснювати електронні транзакції, зокрема, сертифікат, що дозволяє здійснювати цифрову ідентифікацію та цифрову підпис [10]. На лицевій стороні картки національного посвідчення особи Естонії вказано: ім'я, фотографія, підпис, персональний ідентифікаційний номер, дата народження, стать, статус громадянства, номер карти і термін дії карти. На зворотному боці карти вказана наступна інформація: місце народження, дата видачі карти і інформація про вид на проживання, якщо така є. Карта також містить неграфічні інформацію (тобто дані, що не включають фотографію або підпис)у форматі зрозумілому лише для машин. Чіп на ідентифікаційній картці містить два сертифікати, один для електронної автентифікації і один для електронних підписів. Естонія є однією з небагатьох європейських країн, де функціональність електронного підпису є обов’язковою. [10] Сертифікати містять ім'я власника карти і персональний ідентифікаційний номер, а сертифікат автентифікації також містить офіційну адресу електронної пошти, унікальний для кожного власника карти. Карта є обов'язковою для громадян у віці 15 років і старше.

Естонія також запустила «Mobiil-ID» електронний ідентифікатор для мобільних телефонів [31]. Як і електронна ідентифікаційна карта, Mobiil-ID містить сертифікати, які дозволяють окремим особам ідентифікувати себе і

підписувати документи в цифровій формі. Сертифікати Mobiil-ID зберігаються на SIM карті [31], яка використовується в мобільних телефонах. Багато цифрових сервісів дозволяють людям використовувати Mobiil-ID замість ID-карти.

В Норвегії уряд надає MinID («MyID»), добровільну систему електронних ідентифікаторів, яку можна використовувати для доступу до різних онлайн-сервісів уряду [32]. Він доступний для громадян старше тринадцяти років. Фізичні особи реєструються на MinID онлайн, використовуючи свій національний ідентифікаційний номер [32]. Податковий орган потім відправляє набір одноразових паролів поштою на адресу, вказану в національному реєстрі. Люди можуть використовувати ці коди для автентифікації в онлайн-сервісах. Крім того, люди можуть зареєструвати мобільний телефон і отримати одноразові паролі за допомогою SMS. MinID надає користувачам можливість єдиної реєстрації приблизно в п'ятдесяти державних службах.

На даний момент в Норвегії працюють над розробкою нової системи яка буде використовувати мобільні телефони для ідентифікації особистості [14], мобільний пристрій буде виступати носієм конфіденційної інформації користувача і система зможе працювати в офлайн режимі.

Туреччина пропонує нову реалізація смарт-карт які замінить нинішню паперову ідентифікаційну карту. Лицьова сторона карти буде містити фотографію, ім'я, стать, дату народження, громадянство, номер картки і дату закінчення терміну дії особистості, а також ідентифікаційний номер Турецької Республіки, унікальний персональний ідентифікаційний номер, який використовується усіма державними органами і часто транзакції приватного сектора (як це надруковано на національній ідентифікаційної картці). На зворотному боці карти будуть вказані імена батьків власника карти, прізвище при народженні, місце народження, орган видачі, група крові, сімейний стан і релігія [9]. Чіп додатково містить біометричні дані (відбиток пальця і групу крові) і цифровий сертифікати. Біометрична інформація громадянина зберігається тільки на електронній ідентифікаційної карти.

Шведська система електронних посвідчень особи представляє цікавий контраст з багатьма європейськими країнами. Замість того, щоб створювати єдину державну електронну ідентифікаційну карту, Швеція створила систему електронних ідентифікаційних даних в партнерстві з приватним сектором [15]. У Швеції як уряд, так і приватний сектор видають електронні ідентифікатори, і, в залежності від обраного електронного ідентифікатора, шведські користувачі можуть отримати електронний ідентифікатор на картці, мобільному пристрої або в файлі який завантажений на персональний комп’ютер. Всі електронні ідентифікатори включають два сертифікати: один для автентифікації і один для підпису. Вони також містять ім'я і особистий ідентифікатор людини [15]. Електронні ідентифікатори доступні фізичним особам для особистого і професійного використання. Професійні електронні ідентифікатори пов'язані з ідентифікаційним номером конкретної організації, а не з індивідуальним ідентифікаційним номером.

Фінське посвідчення особи не дуже відрізняється від наведених вище рішень. Фінське посвідчення особи є одним з двох офіційних документів, що засвідчують особу у Фінляндії, іншим є фінський паспорт. Будь-який громадянин, мешканець може отримати посвідчення особи. [13] Громадяни Фінляндії отримають вказівку громадянства на картці. Також фінське посвідчення особи доступне у вигляді електронної ідентифікаційної карти, який дозволяє отримати доступ до певних державних служб в Інтернеті, на локальних комп'ютерах або додавати цифрові підписи до документів або створювати контейнери в форматі DigiDoc [11], які також дозволяють шифрувати дані під час шифрування. передача контенту. Посвідчення особи застосовується в поліцейській дільниці і видається поліцією.

Таким чином проаналізував стан електронних ідентифікаційних документів в світі та провівши рішення які представлені різними державами можна виділити сході риси та зробити висновок що є дві основні технології реалізації електронних ідентифікаційних документів: на основі SIM карт та на основі смарт карт з вбудованим елементом безпеки. Також в деяких країнах пропонують електронну

ідентифікацію на мобільних пристроях але такий тип ідентифікації полягає в зберіганні сертифікатів у пам’яті мобільного пристрою що не є цілком безпечним.

2.2 Атаки на SIM карту

2.2.1 Simjacker

У деяких випадках SIM-карта може становити більшу загрозу безпеці, ніж програмне забезпечення телефону. Дослідники AdaptiveMobile Security кажуть, що виявили нову вразливість яку назвали Simjacker [34], яка використовується для отримання інформації яка знаходиться на SIM карті та для спостереження за пристроями людей неназваною компанією-спостерігачем. Цей метод відправляє SMS-повідомлення, що містять інструкції для застосунків SIM Toolkit (STK) и S@T Browser, які підтримуються на SIM-картах деяких операторів. S@T спочатку призначався для запуску браузерів, відтворення звуків або запуску деяких дій на телефонах, Simjacker [34] використовує його для отримання інформації що знаходиться на SIM-карті наприклад інформація про місцезнаходження і номерів IMEI, які згодом відправляються на «пристрій зловмисника» (знову за допомогою SMS), яке містить в собі дані з SIM-карти. Схематично атака зображена на рисунку 2.1.

Важливо відзначити, що даний підхід прихований від користувача. Хоча він використовує SMS, користувач не будете отримувати повідомлення і бачити що SMS повідомлення відправляються з пристрою [34]. Експлойт також не залежить від пристроїв і може бути використано проти iPhone, численних брендів телефонів на Android і деяких пристроїв Інтернету речей, оснащених SIM-картами.

Рисунок 2.1 – Схематичне зображення атаки Simjacker

2.2.2 SIM hijacking

SIM hijacking – це зміна SIM-карти, по суті, процес активації хакерами вашого номера на SIM-карту, якою вони володіють. Цей процес допомагає їм захопити ваш номер телефону, тому наступного разу, коли хтось спробує отримати доступ до вашого профілю онлайн-банкінгу чи іншої системи де потребується автентифікація за номером телефона зловмисники отримають код підтвердження жертви. Зазвичай це найпростіший та ефективніший шлях для того щоб отримати пароль жертви або пройти двоетапний процес перевірки. Існує безліч способів провести атаку такого типу, які в більшості своїй використовують соціальну інженерії. Найбільш поширений тип реалізації такої атаки коли зловмисники обманим шляхом зазвичай використовуючи соціальну інженерії змушують жертву дзвонити на певні номери, а потім звертаються до операторів мобільного зв’язку з проханням відновити втрачену сім карту, зазвичай операторам достатньо назвати три номери на які найчастіше були зроблені дзвінки за останній місяць і таким чином довести належність сім карти. Після чого оператор видає нову сім карту з номером жертви зловмисникам.

2.2.3 WIBattack

Ginno Security Lab докладно описала ще один експлойт, WIBattack, який компрометує застосунок WIB (бездротовий інтернет-браузер) який використовується на деяких SIM-картах для управління ключовими функціями телефону. Так само як і Simjacker, WIBattack заражає телефон за допомогою ретельно відформатованого тексту SMS, який виконує інструкції на картах, у яких не включені ключові функції безпеки [33]. Відправляючи шкідливе SMS-повідомлення на номер телефону жертви, зловмисник може використовувати уразливості в сім-браузері WIB, щоб віддалено отримати контроль над мобільним телефоном жертви і в разі успіху зловмисники можуть виконувати такі шкідливі дії, як: відправка смс, виконання телефонного дзвінка, визначення місця розташування жертви, запуск інших браузерів [33]. (Наприклад, WAP-браузер), отримати IMEI жертви та іншої конфіденційної інформації жертви. Іншими словами дозволяє отримати доступ майже до всіх ресурсів телефона. Кілька команд WIB, які можуть віддалено виконуватись на скомпрометованому пристрої через OTA SMS на сім-карту жертви зображено на рисунку 2.2.

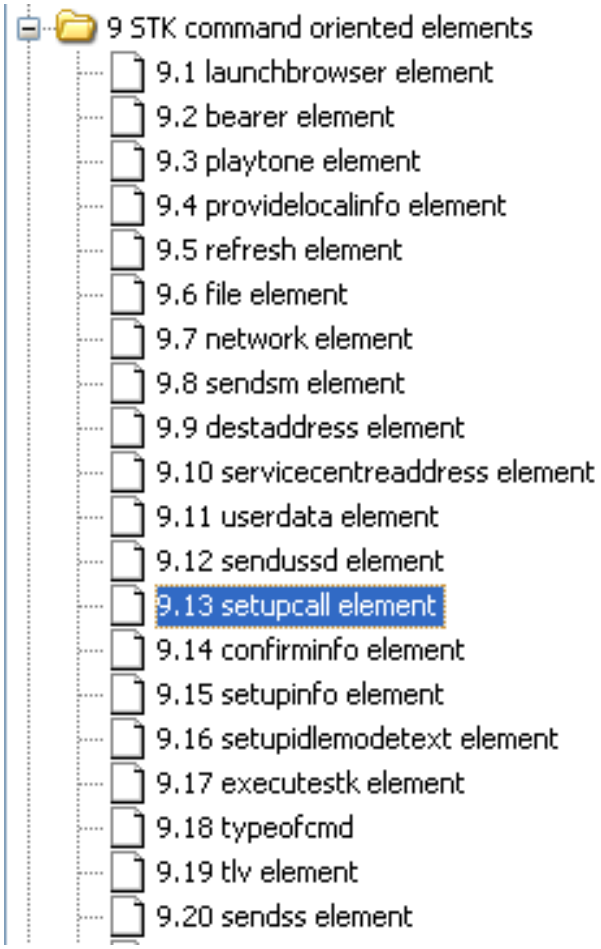

Рисунок 2.2 – перелік команд WIB, які можуть віддалено виконуватись на скомпрометованому пристрої

2.2.4 SS7 exploit

Протокол SS7, також відомий як сигналізаційних система № 7 (Signaling System 7), відноситься до мережі передачі даних і до ряду технічних протоколів або правил, які регулюють обмін даними по ним [35]. Він був розроблений для відстеження та підключення викликів в різних мережах операторів зв'язку, але тепер він зазвичай використовується для розрахунку білінгу стільникового зв'язку і відправки текстових повідомлень на додаток до маршрутизації мобільних і стаціонарних викликів між операторами і регіональними комутаційними центрами.

Атака проводиться наступним чином. Зловмисник підключається до сигнальної мережі SS7 і відправляє службову команду Send Routing Info в мережевий канал, вказуючи номер телефону що атакується в якості параметра. Домашня абонентська мережа відправляє у відповідь таку технічну інформацію: IMSI (International Mobile Subscriber Identity) і адреса MSC, за яким в даний час надає послуги підписнику. Після цього зловмисник змінює адресу білінгової системи в профілі підписника на адресу своєї власної псевдобіллінговой системи. Далі атакуючий вводить оновлений профіль в базу даних через спеціальне повідомлення «Insert Subscriber Data» (ISD). Коли абонент здійснює вихідний дзвінок, його комутатор звертається до системи зловмисника замість фактичної білінгової системи. Система зловмисника відправляє комутатора команду, що дозволяє перенаправити виклик третій стороні, контрольованої зловмисником і таким чином отримати доступ до прослуховування розмов та перехвату смс повідомлень. [35]

2.3 Атаки на смарт картки

Смарт картки є на порядок безпечнішими пристроями, адже вони не мають постійного доступу до мережі, і можуть бути скомпрометовані лише при фізичному доступі, чи під час проведення транзакції, що значно зменшує вразливість конфіденційної інформації до зловмисників, але це не означає що дане рішення є самим надійним та захищеним і не схильним до атак зловмисників.

2.3.1 Атака зчитування ПЗП

Хоча постійний запам'ятовувальний пристрій зазвичай не містить ніякого матеріалу криптографічного ключа, часто містить досить даних введення-виведення, контролю доступу та криптографічних процедур для використання при розробці не інвазійних атак [36]. Методи оптичної реконструкції можуть бути використані для читання ПЗУ безпосередньо. Бітова послідовність ПЗУ зберігається в дифузійному шарі, який практично не залишає оптичної індикації даних на поверхні чіпа [36]. Деякі технології ПЗУ зберігають біти не в формі активної області, а змінюючи порогові напруги транзистора. В цьому випадку необхідно застосовувати додаткові методи селективного фарбування, щоб зробити біти видимими [36].

2.3.2 Читання вмісту пам'яті за допомогою шини

За винятком ПЗП, зазвичай непрактично зчитувати інформацію, що зберігається на процесорі безпеки, безпосередньо з кожної окремої комірки пам'яті. Доступ до збережених даних повинен здійснюватися через шину пам'яті, де всі дані доступні в одному місці. Мікрозондування використовується для спостереження всієї шини і запису значень в пам'ять по мірі їх доступності [36]. Простого відтворення транзакцій може бути недостатньо, щоб процесор отримав доступ до всіх критичних елементів пам'яті. Іноді зловмисникам які стежать за шиною везе, і вони стикаються з картою, на якій програміст вважав, що, обчислюючи і перевіряючи деяку контрольну суму пам'яті після кожного скидання, можна якось збільшити опір несанкціонованого доступу. Це, звичайно, дає зловмиснику негайний та легкий доступ до всіх елементів пам'яті на шині і значно спрощує виконання операції зчитування [37].

2.3.3 Пошук ключів за допомогою перезапису ПЗП

Окремі біти в ПЗП можуть бути перезаписані за допомогою лазерного мікроскопа, і ця можливість іноді дозволяє зловмисникові внести зміни в код, які приведуть до розкриття ключа. Хороший приклад з DES. Там, де реалізація DES добре відома, зловмисник може знайти один біт (або невелику кількість бітів) з властивістю, при якій, змінюючи біти це дозволить легко витягти ключ [38]. Деталі будуть залежати від точної реалізації DES, але зловмисник може, наприклад, зробити команду переходу безумовної і, таким чином, скоротити кількість раундів до одного або двох. Зловмисник також може поступово видаляти такі інструкції, як «виключне або» з ключового матеріалу, щоб спростити вилучення ключа [39].

2.3.4 Пошук ключів за допомогою знищення входу

Принаймні, в DES ключі можуть бути вилучені, якщо зловмисник має можливість пошкодити шлюз в регістрі, тому він зациклюється на постійному значенні протягом всього процесу криптографії [40]. DES зазвичай реалізується з апаратним забезпеченням для одного раунду, плюс регістр, який містить вихідні дані раунду k і відправляє їх назад в якості вхідних даних для раунду k + 1. Біхам і Шамір вказали, що, якщо молодший значущий біт цього регістра застряг, то ефект полягає в тому, що молодший значущий біт виведення функції округлення встановлюється в нуль. Порівнюючи молодші шість бітів лівої і правої половин, можна відновити кілька бітів ключа; беручи до уваги близько десяти шифротекстів від чіпа, який був пошкоджений таким чином, інформація про ключі попередніх раундів може бути отримана з використанням методів

диференціального криптоаналізу, і достатню кількість інформації ключа можна відновити, щоб спростити подальший пошук ключів [41].

2.3.5 Пошук ключів за допомогою пробних бітів

Локально спостерігаючи значення декількох бітів оперативної пам’яті або адресної шини (можливо, одного) під час виконання криптографічного алгоритму, зазвичай за допомогою зондуючої стрілки, зловмисник може легко відновити інформацію про використання секретного ключа [42]. Атаки, застосовуються до криптосистемам з відкритим ключем, таким як RSA, а також до схем шифрування з секретним ключем, включаючи DES і RC5. Це новий тип пасивної атаки ж більш ефективним, ніж попередні. У більшості випадків статистичний аналіз не потрібен. Передбачається, що зловмисник просто має доступ до зондуючої станції, яка на короткий час є свого роду стрілкою, що дозволяє відстежувати значення одного біта під час виконання будь-якого криптографічного алгоритму [43]. Цікава особливість цих атак полягає в тому, що вони не обов'язково є руйнівними, як більшість раніше запропонованих атаки, тобто не наносять шкоди самій карті. По суті, зондування не завжди вимагає обрізки проводів або впровадження несправностей або навіть додаткового втручання до пристрою, щоб воно працювало ненормально. Для цієї атаки атакуючий просто стежить за одним бітом під час виконання операцій або транзакцій.

2.4 Розробка архітектури системи цифрових ідентифікаційних документів на мобільних пристроях

Проаналізувавши існуючі рішення електронної ідентифікації було знайдено ряд недоліків що робить ці рішення потенційно вразливими до атак зловмисників. Враховуючи знайдені недоліки та аналіз механізмів підвищення рівня безпеки конфіденційних даних на мобільних пристроях, пропонується розробити нову архітектуру яка не буде вразлива до визначених атак.

Запропонована система складається з двох модулів: перший – це сторона користувача, який в свою чергу складається з Android застосунку, застосунку – аплету для eSE та інтерфейсу в TEE. Другий модуль – це сторона зчитувача, який також складається з Android застосунку та застосунку – траслету в TEE.

2.4.1 Архітектура модуля користувача

Так як на даний момент eSE являє собою максимально захищене рішення для зберігання та обробки конфіденційної інформації, пропонується використовувати eSE як основний компонент системи, в якому будуть зберігатися конфіденційні дані користувача, та виконуватись необхідні криптографічні операції. Для цього потрібно розробити аплет в якому буде сховище для надійного зберігання даних користувача та приватних ключів. Також аплет повинен містити криптографічні функції які будуть забезпечувати безпечний обмін ключами, генерування спільного секрету, цифровий підпис та перевірку підпису, шифрування даних. Аплет на вхід повинен приймати строго задекларовану команду, проводи необхідні обчислення та видавати на вихід результат або інформацію про статус.

Наступним рівнем треба буде розробити інтерфейс у TEE який буде виконувати роль посередника між eSE та операційною системою для можливості відправки команд з операційної системи пристрою до eSE. Інтерфейс також буде

працювати в зворотному напрямку для можливості отримання результату операції або інформації про статус від eSE.

Останнім кроком буде розробка Android застосунку який буде мати користувацький інтерфейс, реалізовувати протокол передачі інформації NFC та посилати необхідні команди до eSE за рахунок зв'язку з TEE.

Рисунок 2.3 – Схема модуля користувача

2.4.2 Архітектура модуля зчитувача

Так як зчитувач не буде зберігати конфіденційні дані користувача, необхідність використовувати eSE зникає, тому архітектура модуля зчитувача дещо відрізняється від архітектури модуля користувача.

Необхідно розробити траслет для TEE який буде виконувати обробку даних від користувача в безпечному середовищі для забезпечення конфіденційності даних користувача. Траслет так як і аплет повинен містити криптографічні функції які будуть забезпечувати безпечний обмін ключами, генерування спільного секрету, цифровий підпис та перевірку підпису, шифрування та дешифрування даних. Також необхідно реалізувати TUI, для безпечного відображення даних на зчитувачі. Траслет на вхід приймає дані, проводить необхідні обчислення та відображає результат в TUI або відсилає результат до Android застосунку.

Для зчитувача також необхідний Android застосунок, який буде реалізовувати схожий функціонал з застосунком користувача. Також має користувацький інтерфейс, реалізовує протокол передачі інформації NFC та має можливість зв’язку с TEE.

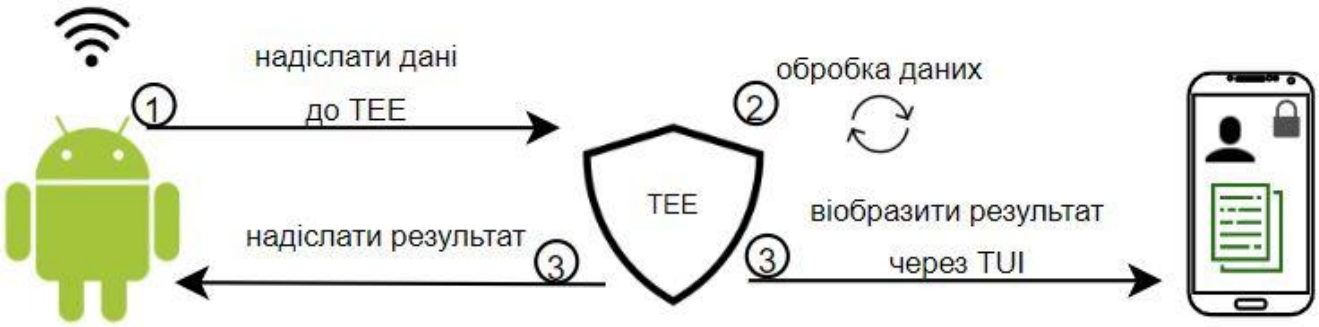

Рисунок 2.4 – Схема модуля зчитувача

2.4.3 Процес взаємодії модулів між собою

Першим кроком необхідно встановити всі необхідні компоненти системи. Далі дані користувача ретельно збираються та формується структура які містить всі необхідні ідентифікаційні дані, ці данні підписуються закритим ключем органу що видає документи та встановлюються на eSE також додається приватний ключ для можливості використання електронного цифрового підпису та сертифікат яким можна перевірити підпис зчитувача.

На TEE зчитувача додається сертифікат яким можна перевірити підпис даних які надходять від користувача та приватний ключ яким можна підписати дані для передачі до користувача.

Далі при взаємодії користувача та зчитувача виконуються наступні кроки:

1. Встановлюється незахищене з’єднання користувача та зчитувача через NFC.

2. Користувач та зчитувач генерують пари ключів (закритий та відкритий).

3. Користувач підписує відкритий ключ приватним ключем який був встановлений разом із даними та відправляє відкритий ключ до зчитувача.

4. Зчитувач перевіряє підпис відкритого ключа користувача та генерує спільний секрет за алгоритмом Діффі-Хеллмана.

5. Зчитувач підписує свій відкритий ключ приватним ключем який був встановлений органом що видає документи та відправляє відкритий ключ до користувача.

6. Користувач перевіряє підпис відкритого ключа зчитувача та генерує спільний секрет за алгоритмом Діффі-Хеллмана.

7. Далі користувач та зчитувач використовують функцію формування ключа на основі спільного секрету та отримують на виході ключ який буде використовуватися для шифрування повідомлень симетричної криптографією шифром AES.

8. Користувач шифрує структуру з даними алгоритмом AES256, підписує та відправляє на зчитувач.

9. Зчитувач перевіряє підпис, розшифровує структуру та виводить ідентифікаційні дані на екрані зчитувача за допомогою TUI.

Висновки до розділу 2

В даному розділі були визначені країни в яких вже існують системи електронної ідентифікації. Рішення які пропонують різні країни були проаналізовані, також були описані основні риси та характеристики які властиві даним підходам до електронної ідентифікації. На основі аналізу було знайдено спільні риси. Існуючі рішення базуються на таких технологіях: на основі SIM карт та на основі смарт карт з вбудованим елементом безпеки. Також в деяких країнах пропонують електронну ідентифікацію на мобільних пристроях, але ці рішення

мають недоліки, пов’язані із слабкою захищеністю документів у пам’яті мобільного пристрою.

В наступному підрозділі було знайдено та описано найпоширеніші атаки на SIM карти та смарт карти, для розуміння недоліків існуючих рішень які можна покращити шляхом пропонування нової системи з використанням нових технологій підвищення рівня безпеки конфіденційних даних на мобільних пристроях.

В останньому підрозділі було запропоновано нову архітектуру системи цифрових ідентифікаційних документів на мобільних пристроях, яка на основі аналізу існуючих рішень враховує недоліки, та використовує нові механізми підвищення рівня безпеки конфіденційних даних на мобільних пристроях для забезпечення максимального рівня захищеності даних. Також було розроблено та детально описано архітектури кожного окремого модуля та архітектуру взаємодії цих модулів між собою. Запропонована архітектура допоможе в подальшій розробці системи.

3 РЕАЛІЗАЦЯ МОБІЛЬНИХ ІДЕНТИФІКАЦІЙНИХ ДОКУМЕНТІВ ТА НОВА МОДЕЛЬ РОЗГОРТУВАННЯ СИСТЕМИ

За запропонованою архітектурою було розроблено систему цифрових ідентифікаційних документів на мобільних пристроях використовуючи дві основні мови програмування: Java та C також було використано мову JavaCard яка є по суті Java з обмеженими можливостями. Основні технології які були використані це embedded Secure Element, Trusted Execution Environment, Trusted User Interface та криптографія на еліптичних кривих. Система містить простий та зрозумілий користувацький інтерфейс та забезпечує високий рівень захищеності конфіденційних даних, що досягається використанням зазначених технологій. Результатом роботи системи є однозначна можливість ідентифікації особистості за допомогою мобільних пристроїв. В даному розділі описується програмна реалізація, механізми безпеки, модель розгортання даної системи та проводиться NFC Relay Attack яка засвідчує працездатність запропонованого рішення.

3.1 Програмна реалізація

На основі запропонованої архітектури системи цифрових ідентифікаційних документів на мобільних пристроях було розроблено програмну реалізацію системи.

Першим кроком стала розробка програмного модуля користувача який включає в себе три компоненти: аплет для eSE, інтерфейс у TEE та Android застосунок.

Спочатку треба було розробити аппет для eSE який би зберігав конфіденційні дані користувача та приватний ключ. Для цього було написано

застосунок на мові JavaCard з використанням бібліотек javacard.framework та org.globalplatform які дозволяють керувати аплетом та виконувати необхідні операції. Наступним кроком стала реалізація криптографічних методів захисту інформації. Було обрано криптографію на еліптичних кривих. Для цього було обрано еліптичну криву secp256r1 та реалізовано клас генерації пари ключів на основі цієї еліптичної кривої.

```
import javacard.security.ECPrivateKey;
import javacard.security.ECPublicKey;
import javacard.security.KeyPair;


class Secp256r1
{
    public static KeyPair new_key_pair()
    {
        KeyPair key = new KeyPair(KeyPair.ALG_EC_FP, (short) 256);

        ECPrivateKey priv_key = (ECPrivateKey) key.getPrivate();
        ECPublicKey pub_key = (ECPublicKey) key.getPublic();

        priv_key.setFieldFP(p, (short) 0, (short) p.length);
        priv_key.setA(a, (short) 0, (short) a.length);
        priv_key.setB(b, (short) 0, (short) b.length);
        priv_key.setG(G, (short) 0, (short) G.length);
        priv_key.setR(r, (short) 0, (short) r.length);

        pub_key.setFieldFP(p, (short) 0, (short) p.length);
        pub_key.setA(a, (short) 0, (short) a.length);
        pub_key.setB(b, (short) 0, (short) b.length);
        pub_key.setG(G, (short) 0, (short) G.length);
        pub_key.setR(r, (short) 0, (short) r.length);

        return key;
    }
    // Parameters for elliptic curve cryptography from Digital Signature Standard (DSS)
    // Used Secp256r1 NIST Recommended Elliptic Curve.
    private static final byte[] p =
    {
        (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x01,
        (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00,
        (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF,
        (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF
    };

    private static final byte[] a =
    {
        (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x01,
        (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00,
        (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0x00, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF,
        (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFF, (byte) 0xFC
    };

    private static final byte[] b =
    {
        (byte) 0x5A, (byte) 0xC6, (byte) 0x35, (byte) 0xD8, (byte) 0xAA, (byte) 0x3A, (byte) 0x93, (byte) 0xE7,
        (byte) 0xB3, (byte) 0xEB, (byte) 0xBD, (byte) 0x55, (byte) 0x76, (byte) 0x98, (byte) 0x86, (byte) 0xBC,
        (byte) 0x65, (byte) 0x1D, (byte) 0x06, (byte) 0xB0, (byte) 0xCC, (byte) 0x53, (byte) 0xB0, (byte) 0xF6,
        (byte) 0x3B, (byte) 0xCE, (byte) 0x3C, (byte) 0x3E, (byte) 0x27, (byte) 0xD2, (byte) 0x60, (byte) 0x4B
    };
```

Рисунок 3.1 – Програмна реалізація генерації пари ключів на еліптичній кривій

На рисунку 3.1 зображено програмну реалізацію генерації пари ключів на еліптичних кривих для операцій над еліптичними кривими над великими простими полями. Реалізація даного класу реалізована за стандартом Digital Signature Standard (DSS).

Далі були реалізовані криптографічні функції для обміну ключами за алгоритмом Діффі-Хеллмена, функції цифрового підпису та перевірки підпису та функція генерування симетричного ключа шифрування на основі згенерованого спільного секрету.

```
// Elliptic curve Diffie-Hellman key agreement algorithm
public static byte[] ecdh_key_agreement(ECPrivateKey ec_priv_key, byte[] foreign_ec_pub_key, byte[] shared_info)
{
    byte[] secret = ecdh_key_agreement(ec_priv_key, foreign_ec_pub_key);
    /*
        According to BSI TR-03111 4.3.3. Key Derivation Functions
    */
    byte[] counter = {(byte)0x00, (byte)0x00, (byte)0x00, (byte)0x01};
    short input_len = (short)((short)secret.length + (short)counter.length + (short)shared_info.length);
    byte[] concatenated_input = JCSystem.makeTransientByteArray(input_len, JCSystem.CLEAR_ON_DESELECT);

    short offset = 0;
    Util.arrayCopyNonAtomic(secret, (short)0, concatenated_input, offset, (short)secret.length);
    offset += (short)secret.length;

    Util.arrayCopyNonAtomic(counter, (short)0, concatenated_input, offset, (short)counter.length);
    offset += (short)counter.length;

    Util.arrayCopyNonAtomic(shared_info, (short)0, concatenated_input, offset, (short)shared_info.length);

    byte[] hash_array = JCSystem.makeTransientByteArray((short)32, JCSystem.CLEAR_ON_DESELECT);
    MessageDigest sha256 = MessageDigest.getInstance(MessageDigest.ALG_SHA_256, false);
    sha256.reset();
    sha256.doFinal(concatenated_input, (short)0, (short)concatenated_input.length, hash_array, (short)0);

    return hash_array;
}

// HMAC-based Key Derivation Function
public static byte[] hmac_key_derivation(byte[] input_keying_material, byte[] info, short keying_material_length,
    byte[] salt)
{
    // RFC 5869 section 2.2 Step 1: Extract
    byte[] prk = hmac(salt, input_keying_material);

    if (keying_material_length > (short)(255 * prk.length))
    {
        ISOException.throwIt(ISO7816.SW_WRONG_DATA);
    }

    short offset = 0;
    short N = Utils.division_ceil(keying_material_length, (short)prk.length);
    byte[] derivated_key = JCSystem.makeTransientByteArray((short)256, JCSystem.CLEAR_ON_DESELECT);
    byte[] T = JCSystem.makeTransientByteArray((short)prk.length, JCSystem.CLEAR_ON_DESELECT);

    byte[] T1 = null;
    if (info != null)
    {
        T1 = JCSystem.makeTransientByteArray((short)((short)info.length + (short)1), JCSystem.CLEAR_ON_DESELECT);
        Util.arrayCopyNonAtomic(info, (short)0, T1, (short)0, (short)info.length);
        T1[info.length] = (byte)0x01;
    }
    else
    {
        T1 = JCSystem.makeTransientByteArray((short)1, JCSystem.CLEAR_ON_DESELECT);
        T1[0] = (byte)0x01;
    }
```

Рисунок 3.2 – Програмна реалізація алгоритму Діффі-Хеллмана та функції формування симетричного ключа на основі спільного секрету

Після розробки аплета наступним кроком було реалізовано інтерфейс TEE який виконує роль посередника між eSE та операційною системою телефона. Основана задача якого передавати команди та інформацію між eSE та операційною системою телефона.

```
TEE_Result TA_OpenSessionEntryPoint( uint32_t paramTypes, TEE_Param params[4], void **sessionContext )
{
    (void) paramTypes;
    (void) params;
    (void) sessionContext;

    return TEE_SUCCESS;
}


void TA_CloseSessionEntryPoint( void *sessionContext )
{
    (void) sessionContext;
}


TEE_Result TA_InvokeCommandEntryPoint( void *sessionContext, uint32_t commandID,
    uint32_t paramTypes, TEE_Param params[4] )
{
    (void) sessionContext;
    print_log( "Invoke command: %u\n", commandID );

    std::vector< uint8_t > in_buf;
    if( TEE_PARAM_TYPE_NONE != TEE_PARAM_TYPE_GET(paramTypes, in_buf_param_num) )
    {
        assert( TEE_PARAM_TYPE_MEMREF_INPUT == TEE_PARAM_TYPE_GET(paramTypes, in_buf_param_num) );
        if( TEE_PARAM_TYPE_MEMREF_INPUT != TEE_PARAM_TYPE_GET(paramTypes, in_buf_param_num) )
        {
            print_log( "Unsupported param" );
            return TEE_ERROR_BAD_PARAMETERS;
        }
        in_buf.resize( params[in_buf_param_num].memref.size );
        memcpy( in_buf.data(), params[in_buf_param_num].memref.buffer, in_buf.size() );
    }
    print_log( "in buf: %zu", in_buf.size() );
    assert( false == in_buf.empty() );

    return TEE_SUCCESS;
}


static se::Session* open_se_session()
{
    if( nullptr == se_session )
    {
        print_log( "open_se_session" );
        const se::Aid mdl_aid{ 0xA0, 0x00, 0x00, 0x02, 0x48, 0x04, 0x00 };
        se_session = se::Session::create( mdl_aid );
        print_log( "open_se_session OK" );
    }
    assert( nullptr != se_session );
    return se_session;
}
```

Рисунок 3.3 – Реалізація інтерфейсу TEE

Останнім компонентом клієнта для розробки став Android застосунок який виступає центральним елементом системи. Він надсилає команди до eSE через TEE, встановлює з'єднання по NFC з зчитувачем та ініціює систему загалом.

На рисунку 3.4 зображена діаграма класів Android застосунку клієнта яка описує та демонструє загальну структуру системи, описує залежності, змінні, поля, функції, інтерфейси та як вони взаємодіють між собою. Для більш наглядного представлення та розуміння роботи застосунку.

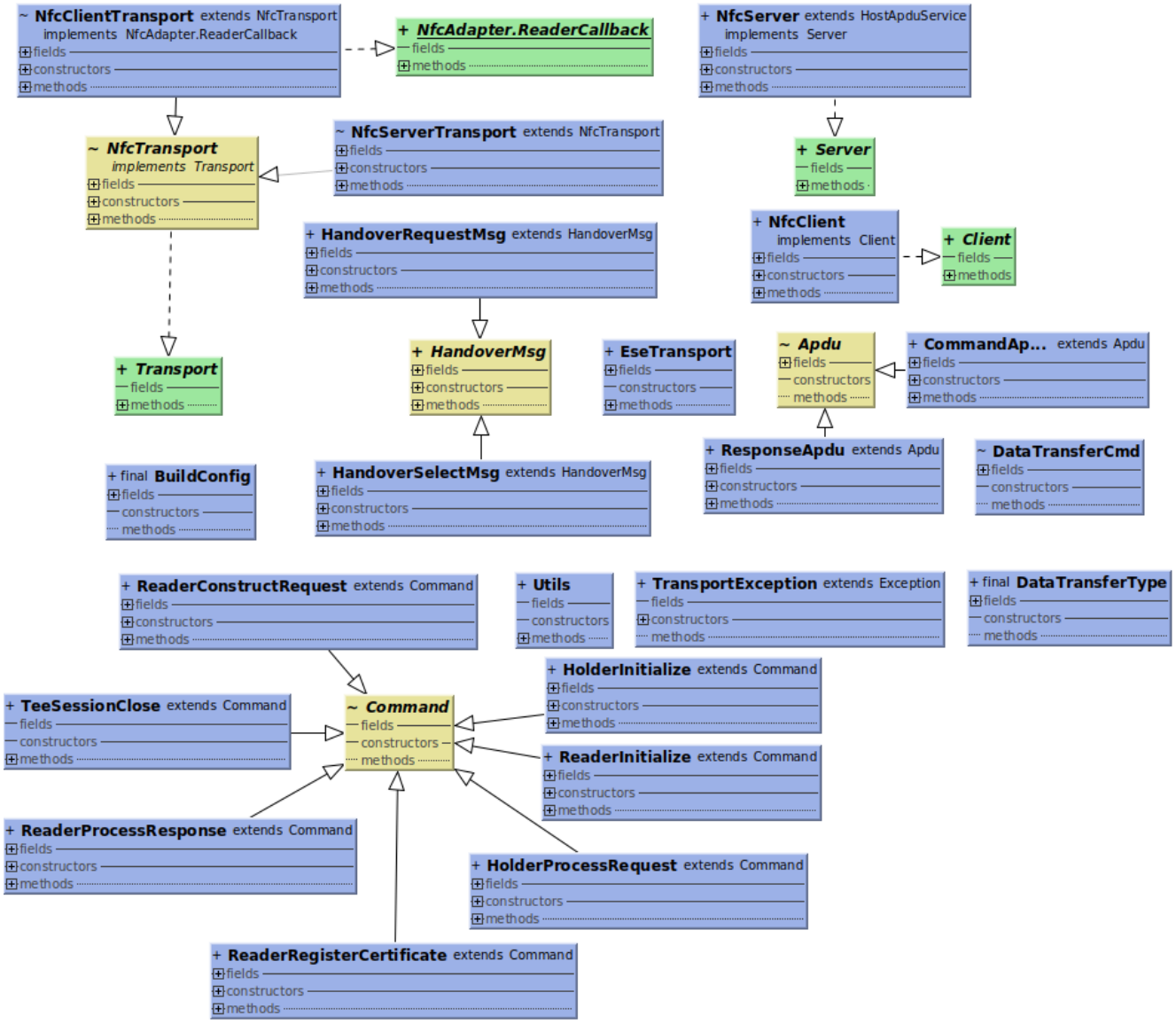

Рисунок 3.4 – Діаграма класів Android застосунку клієнта

Розробка модуля зчитувача складається з двох компонентів: Andorid застосунку та траслета TEE. Andorid застосунок зчитувача майже не відрізняється від Andorid застосунка клієнта, та реалізує такий же функціонал: встановлює

з’єднання по NFC з клієнтом передає дані у TEE та ініціює систему загалом з боку зчитувача загалом, діаграма класів та програмна реалізація використовує той самий функціонал.

Траслет TEE в свою чергу відрізняється від реалізації клієнта, але містить майже однаковий функціонал з аплетом eSE, зокрема містить таку саму реалізацію генерування криптографічних ключів, криптографічних функцій для обміну ключами за алгоритмом Діффі-Хеллмена, функції цифрового підпису та перевірки підпису та функцій генерування симетричного ключа шифрування на основі згенерованого спільного секрету.

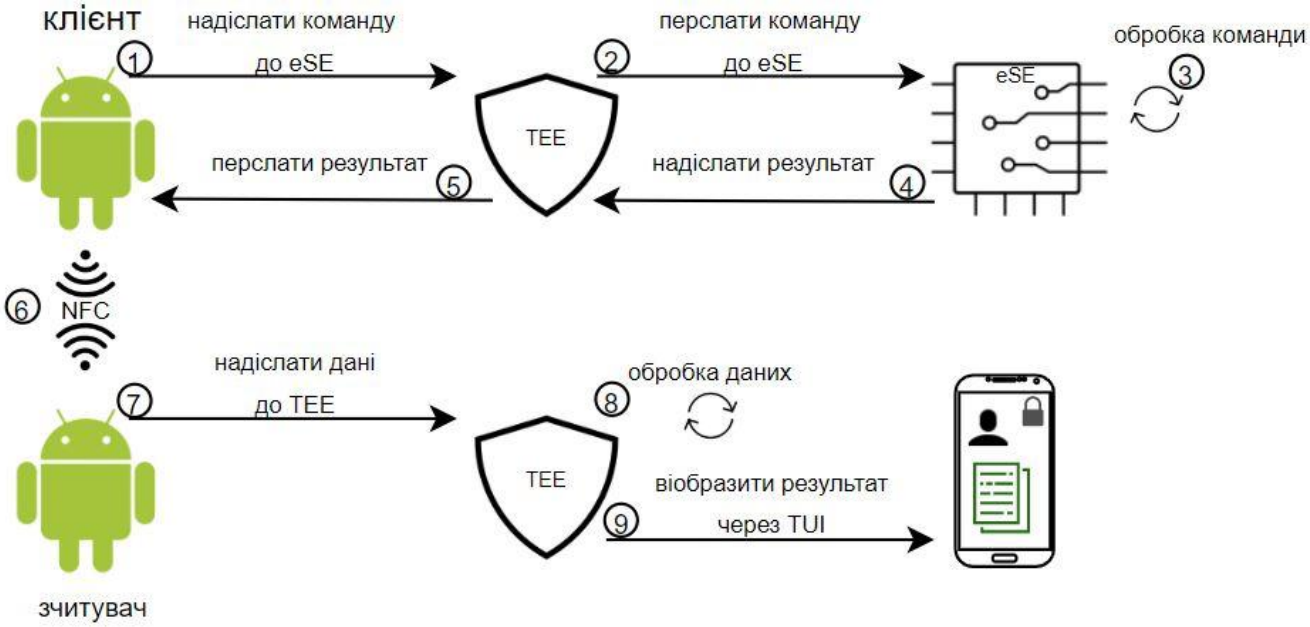

Рисунок 3.5 – Загальна схема роботи

На рисунку 3.5 зображена загальна схема роботи системи цифрових ідентифікаційних документів на мобільних пристроях яка працює за описаною архітектурою в розділі 2.4.3.

На рисунку 3.6 зображена детальна діаграма послідовностей яка описує розроблену систему захисту даних та послідовності дій криптографічних механізмів та функцій яка заснована на розробленій архітектурі в розділі 2.4.3.

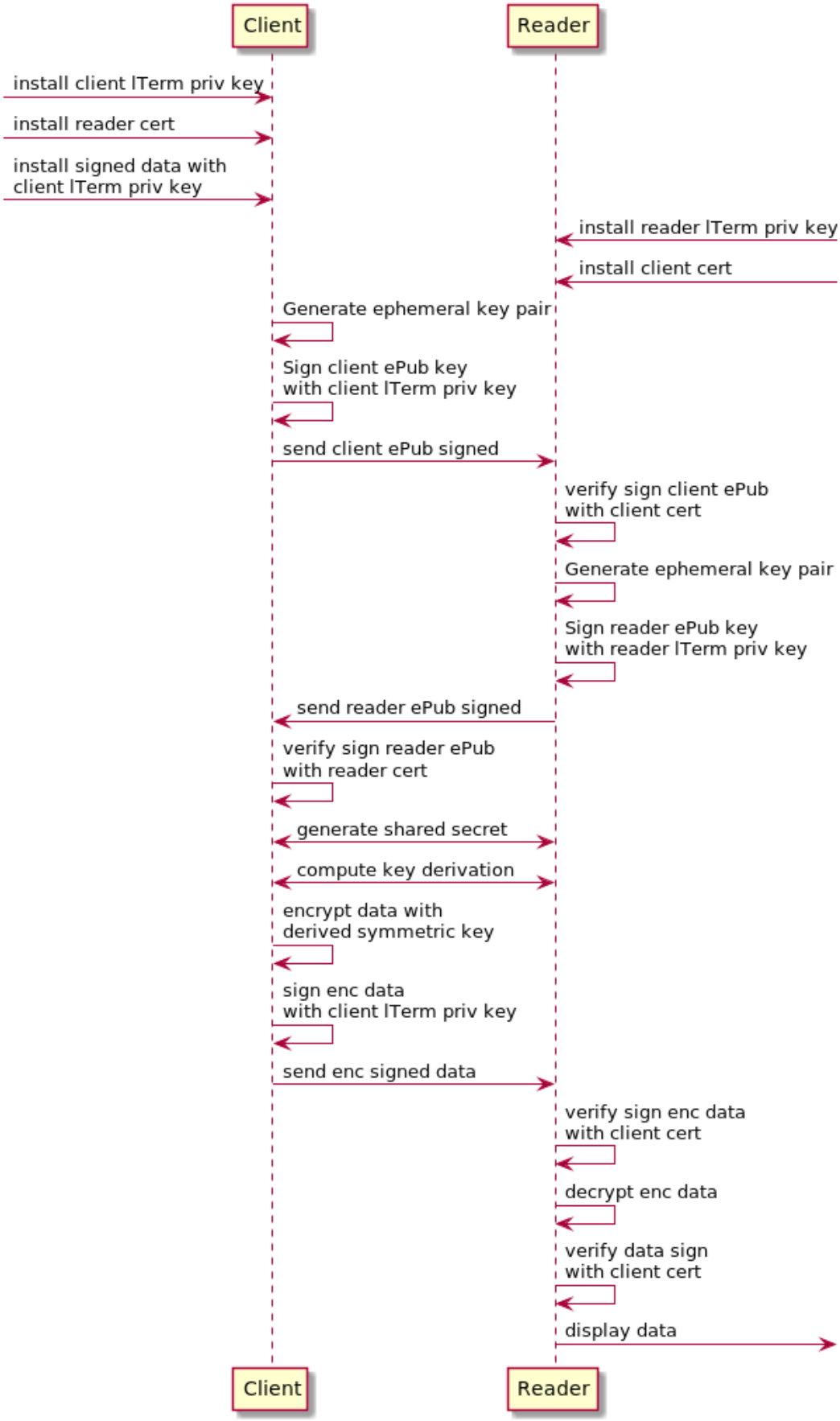

Рисунок 3.6 – Діаграма послідовності яка описує криптографічний механізм системи

3.2 Розробка моделі розгортання системи

Перш за все, коли мова йде про систему, яка буде функціонувати на рівні держави, повинні бути прийняті відповідні закони, що регулюють електронні повноваження і ідентифікацію особистості.

Наступним кроком є досягнення угоди між урядом і виробниками пристроїв (eSE, TEE), для того щоб отримати ключі, щоб мати можливість встановити необхідне програмне забезпечення до eSE і TEE та мати можливість підписувати дані для можливості встановлення їх до аплету та довіреної програми.

Далі слід розгорнути саму систему. Головний елемент такої системою є органом видачі (Issuing authority). Його основне завдання - генерувати і підписувати ідентифікаційні дані користувача, вторинна задача - зберігати всі генеровані сертифікати і діяти в якості сервера для перевірки даних, якщо це необхідно.

Далі, система управління обліковими даними (Credential Management System) запитує зазначені підписані ідентифікаційні дані у Issuing authority певного користувача, і передає їх до довіреного сервіс-менеджеру (Trusted Service Manager). Trusted Service Manager є ключовим елементом системи. Він зберігає всі необхідні ключі від eSE і TEE, щоб мати можливість встановити необхідні дані і необхідне програмне забезпечення.

Останній елемент цієї системи - мобільний пристрій кінцевого користувача. На пристрої буде встановлено необхідне програмне забезпечення і будуть надані підписані облікові дані. Запропонована модель зображена на рисунку 3.7.

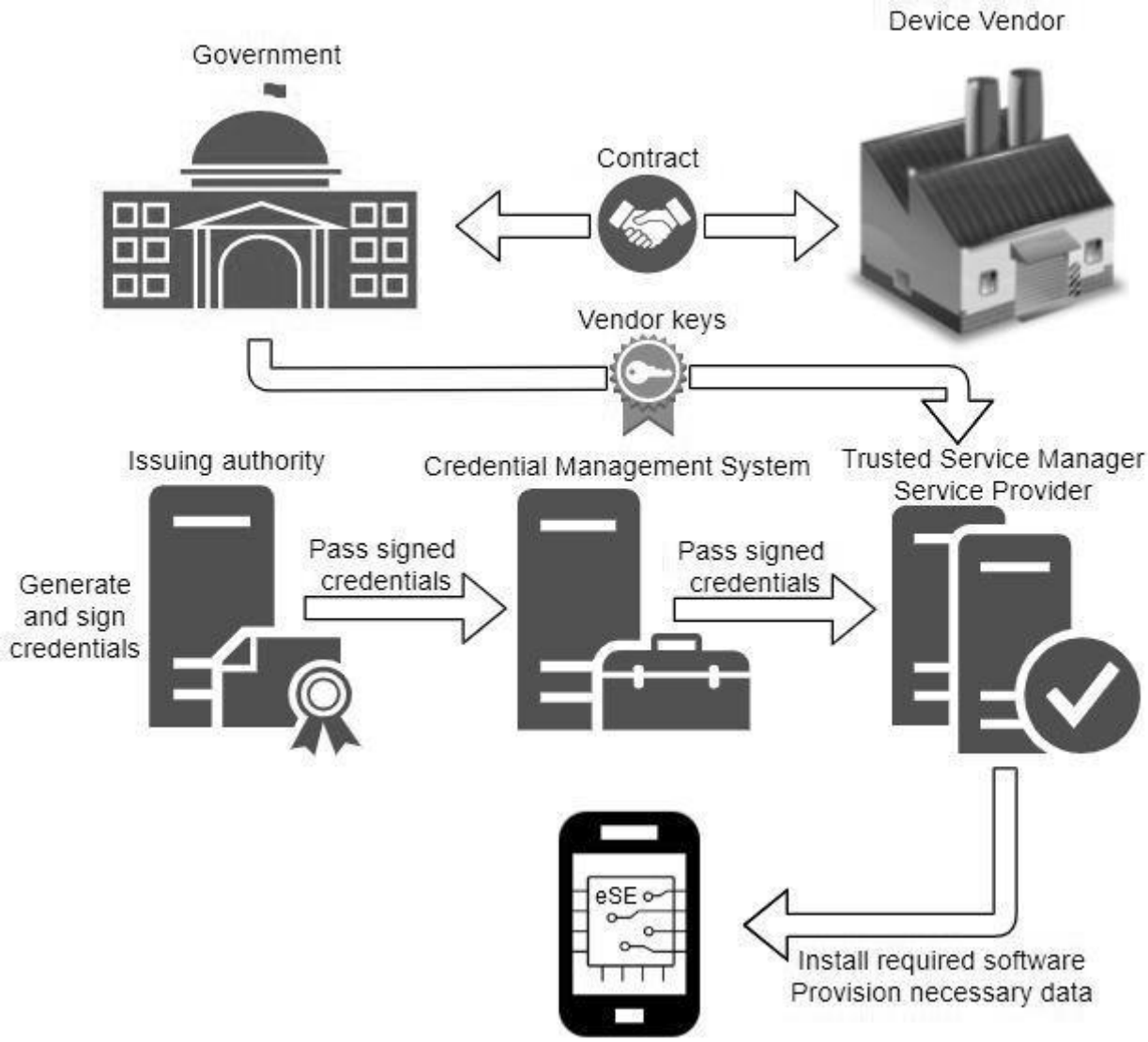

Рисунок 3.7 – модель розгортання системи електронної ідентифікації особистості

3.3 Перевірка захищеності рішення шляхом відтворення NFC Relay Attack

Relay Attack це метод, при якому зловмисник використовує атаку типу man in the middle. Основана ідея в тому що зловмисник здатний в реальному часі перехоплювати, маніпулювати і змінювати транзакцію, щоб використовувати її в своїх інтересах.

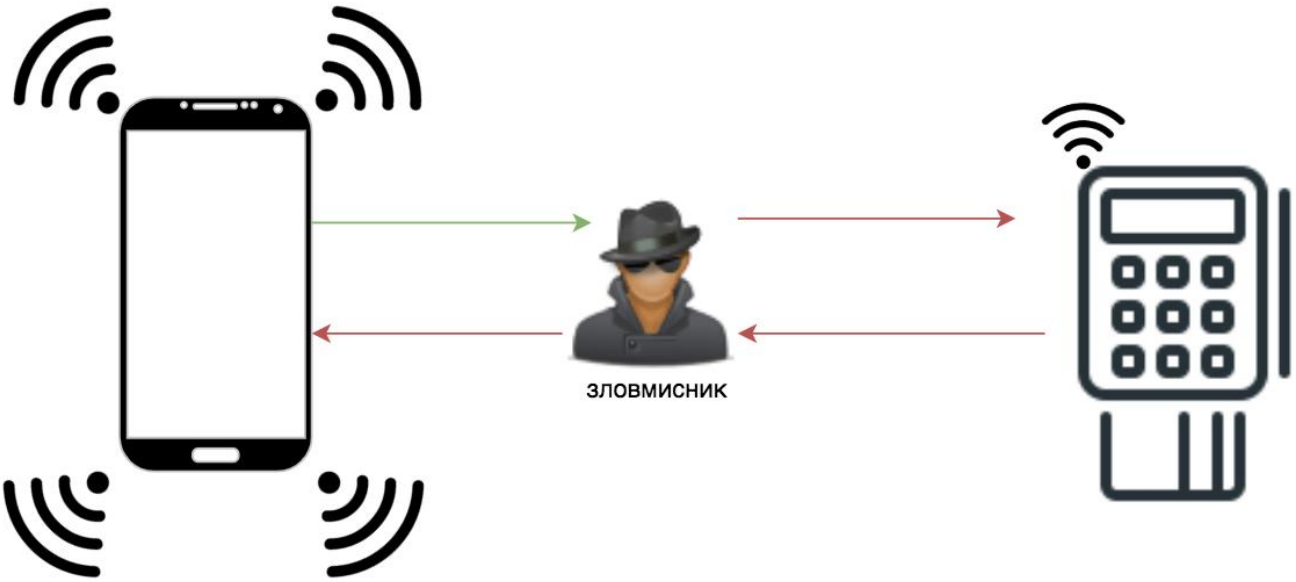

Рисунок 3.8 – Схематичне зображення Relay Attack

На рисунку 3.8 з лівого боку зображено пристрій з технологією NFC, здатний здійснювати цифрові транзакції. У правій частині зображено PoS (Point of Sale System) термінал також з технологією NFC.

Зловмисник для проведення атаки має при собі також пристрій з технологією NFC для зчитування та передачі сигналу. Основна проблема з якою стикається зловмисник це те що необхідний майже безпосередній контакт між телефоном та терміналом або наявність двох пристроїв з технологією NFC які з'єднані між собою наприклад через Wi-Fi для можливості передачі даних на більші відстані.

Отже для проведення атаки було використано два термінали для зчитування карток NXP та JCShell для можливості маніпулювання зчитаними даними. В умовах тестового варіанту був забезпечений безпосередній контакт клієнта і термінала та зчитувача та другого термінала. Дані відправлялись на термінал де передавались на комп'ютер де змінювалось повідомлення та передавалось на інший термінал для передачі через NFC на зчитувач, зчитувач обробляв інформацію та відправляв відповідь в зверненій послідовності.

Так як було використано цифровий підпис для повідомлень, коли зловмисник змінив повідомлення, підпис не був веріфікован на зчитувачі і

зчитувач відіслав у відповідь повідомлення (Status Word) 6982 – що означає SW_SECURITY_STATUS_NOT_SATISFIED, тобто не задовольняє умовам безпеки. Процес та отриманий результат зображено на рисунку 3.9.

Рисунок 3.9 – Результати виконання атаки man in the middle на запропоновану систему

Висновки до розділу 3

В даному розділі за запропонованою архітектурою було розроблено систему цифрових ідентифікаційних документів на мобільних пристроях. Було описано процес розробки необхідних модулів та компонентів системи також було показано процес програмної реалізації та описані технічні деталі реалізації криптографічних механізмів забезпечення безпеки конфіденційних даних.

Було описано повну схему взаємодії компонентів системи. Та побудовано діаграму послідовності для опису розробленої системи захисту даних та послідовності дій криптографічних механізмів та функцій.

Також було запропоновано модель розгортання системи цифрових ідентифікаційних документів на мобільних пристроях з вказанням всіх необхідних сутностей які необхідні для впровадження даної системи в реальному житті.

Останнім було виконано перевірку захищеності рішення шляхом відтворення NFC Relay Attack, яка засвідчує працездатність запропонованого рішення.

4 РОЗРОБКА СТАРТАП ПРОЕКТУ

Розділ має на меті проведення маркетингового аналізу стартап проекту задля визначення принципової можливості його ринкового впровадження та можливих напрямів реалізації цього впровадження.

4.1 Опис ідеї проекту

В цьому підрозділі описується зміст ідеї та можливі базові потенційні ринки, в межах яких необхідно буде шукати групи потенційних клієнтів. Для кого стартап може бути корисним та де ідею можна бути застосувати. Основні вигоди для користувачів описані в таблиці 4.1 та визначення сильних та слабких сторін ідей у таблиці 4.2

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
Мобільний застосунок для можливості легкої ідентифікації людини з гарантуванням автентичності даних	1. Державний рівень, для громадян	1. Простота використання, надійність та безпечність особистих даних
	2. Для державних службовців (поліцейські)	2. Простота використання, швидкість встановлення особистості та гарантування автентичності даних

Кінець таблиці 4.1

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
	3. Будь-які компанії які хочуть впровадити контроль фізичного доступу	3. Швидкість та надійність встановлення особистості

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	*Техніко-економічні характеристики ідеї*	*(потенційні) товари/концепції конкурентів*				*W (слабка сторона)*	*N (нейтральна сторона)*	*S (сильна сторона)*
		Мій проект	*Estonian eID*	*Thales*	*MDL autoMation*			
1.	Безпечність даних які зберігаються	Максимальний рівень надійності завдяки eSE та TEE	Дані знаходяться в хмарному сховищі не є цілком безпечним	Використовує TEE для зберігання та обробки даних не є цілком безпечним	Використовує Android застосунок як сховище, не є безпечним	Складність розгортання подібної системи для користувачів	Швидкість ідентифікації та автентифікації	Максимальний рівень захищеності даних які зберігаються

Кінець таблиці 4.2

№ п/п	*Техніко-економічні характеристики ідеї*	*(потенційні) товари/концепції конкурентів*				*W (слабка сторона)*	*N (нейтральна сторона)*	*S (сильна сторона)*
2.	Інтерфейси для передачі даних	NFC, Wi-Fi, Blueto oth, qr	GSM, web	Blueto oth, NFC	QR	GSM	Bluetoo th, NFC	NFC, Wi-Fi, Bluetoo th, qr
3.	Технології забезпеченн я безпечності, атентичност і	eSE, TEE, TUI	UICC Sim based SE	TEE, TUI	-	-	TEE, TUI	eSE, TEE, TUI

4.2 Технологічний аудит ідеї проекту

В межах даного підрозділу було проведено аудит технології, за допомогою якої можна буде реалізувати ідею проекту та заповнена таблицю 4.3 для визначення технологічної здійсненності ідеї проекту.

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологій*
1	Зберігання конференційних даних в embedded Secure Element	Необхідність мати ключі для доступу до eSE для можливості провіженінгу даних	Наявна майже в усіх сучасних смартфонах преміального класу	Доступ до eSE може мати лише виробник чіпів чи довірені сторони
2	Обробка конфіденційних даних в Trusted Execution Environment	Необхідність мати ключі для доступу до TEE для можливості встановлення необхідного ПО для обробки даних	Наявна в усіх сучасних смартфонах з процесорами Qualcom	Доступ до TEE може мати лише виробник процесорів або довірені сторони
3	Використання Trusted User Interface для безпечного представлення даних	Можна отримати доступ до TUI через TEE, необхідно мати ключі від виробника	Наявна якщо є наявним TEE	Так як і TEE не можливо отримати доступ без дозволу виробника
4	Взаємодія з іншими реалізаціями цифрових ідентифікаційних документів	Використання специфікацій розроблених для можливості взаємодії різних рішень	На даний момент специфікація за стандартом ISO знаходиться в розробці	На даний момент є в закритому доступі

Кінець таблиці 4.3

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологій*
5	Використання API та фреймворків таких як JCOP та androidx.ese для реалізації доступу до необхідних компонентів системи	Використання в вихідному коді для забезпечення результату	Технологія наявна в останніх версіях Android та JavaCard	Знаходяться у відкритому доступі
Обрана технологія реалізації ідеї проекту: деякі з обраних технологій для реалізації ідеї проекту є в закритому доступі але у автора проекту є доступ до них, тому були обрані всі вище описані наявні технології для реалізації.				

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Для даного підрозділу було визначено ринкові можливості які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів які приводяться в таблиці 4.4 та таблиці 4.5.

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1	Кількість головних гравців, од	6 (Thales, Gemalto, Samsung, Google, e-Estonia, *MDL autoMation*)
2	Загальний обсяг продаж, грн/ум.од	500 млн ум. од.
3	Динаміка ринку (якісна оцінка)	Зростає, на даний момент
4	Наявність обмежень для входу (вказати характер обмежень)	Наявність договору між виробниками чіпів/ компонентів та розробниками для можливості отримання ключів
5	Специфічні вимоги до стандартизації та сертифікації	Необхідний стандарт для зберігання, обробки, верифікації та автентифікації даних на мобільних пристроях
6	Середня норма рентабельності в галузі (або по ринку), %	300%

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
	Все більше звичайних процесів можна виконувати за допомогу смартфона, потреба мати при собі лиш телефон для можливості ведення звичайного життя	1. Громадяни (всі у кого наявні смартфони) 2. Державні службовці 3. Компанії які хочуть впровадити систему контроля фізичного доступу	Для кожної цільової групи продукт несе одну і ту саму користь, отже відмінності нехтуються	• Безпечність даних які зберігаються • Надійність процесу встановлення особистості • Простота використання • Швидкість виконання операцій

Після визначення потенційних груп клієнтів також в цьому підрозділі було проведено аналіз ринкового середовища та складено таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають таблиця 4.6 та відповідно таблиця 4.7.

Таблиця 4.6 – Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1	Фінансові вигоди	Рішення конкурентів можуть бути вигіднішими	Представлення більш захищеного рішення на фоні пропозицій конкурентів
2	Не всі технології передачі конфіденційних даних	Конкуренти можуть мати більш широкий спектр технологій передачі даних	Впровадження усіх можливих технологій передачі конфіденційних даних
3	Рішення які не потребують закритих технологій	Конкуренти можуть використовувати відкриті технології що значно полегшить процес розробки	Представлення більш захищеного та надійного рішення на фоні пропозицій конкурентів
4	Проблеми на законодавчому рівні	Можуть бути не прийняті деякі закони щодо регулювання електронних ідентифікаційних документів	Лобіювання необхідних законів, та процес прийняття нових законів щодо регулювання електронних ідентифікаційних документів

Таблиця 4.7 – Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1	Прийняття нових законів що полегшують впровадження системи електронних ідентифікаційних документів	Полегшення та прискорення впровадження системи електронних ідентифікаційних документів на державному рівні	Розгортання системи електронних ідентифікаційних документів на державному рівні
2	Поява нової технології безпечної передачі даних	Збільшення рівня безпеки системи в цілому	Представлення більш захищеного рішення для роботи системи
3	Поява нової технології захищеної обробки конфіденційних даних	Збільшення рівня безпеки системи в цілому	Впровадження нової технології до системи для підвищення рівня безпеки
4	Використання напрацювань партнерів	Прискорення розробки системи	Долучення до проекту вже готових працюючих рішень для Прискорення розробки системи
5	Вихід на ринок нових клієнтів	Додаткові канали збуту продукції та підвищення фінансування	Вихід на міжнародний ринок надання послуг

Надалі проводиться аналіз пропозиції: визначаються загальні риси конкуренції на ринку приведені в таблиці 4.8.

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
Олігополістична конкуренція	Система електронної ідентифікації є складною в розробці та досить дорогою що призводить до того що досить невелика кількість гравців на ринку можуть собі дозволити розробляти подібну систему	Підвищення рівня безпеки системи використовуючи останні напрацювання в сфері мобільної інформаційної безпеки при зниженні кінцевої вартості продукту
За рівнем конкурентної боротьби: локальний	Вихід на ринок в межах однієї держави Україна	Представлення більш надійного за захищеного рівня на фоні конкурентів при зниженні кінцевої вартості продукту
За галузевою ознакою: міжгалузева/	Дане рішення може використовуватися як ІТ компаніями так і держ службовцями	Представлення простого рішення яке б дозволило користуватися всім не залежно від технічних навичок та підготовки

Кінець таблиці 4.8

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
Конкуренція за видами товарів: товарно-видова	Конкуренція між рішеннями які представлять ті ж самі функції але істотно відрізняються за способом виконання.	Застосування технологій до яких конкуренти не мають доступу що призводить до більш захищеного рівня
За характером конкурентних переваг: нецінова	Ціна запропонованого рішення не буде суттєво відрізнятися від конкурентів але якість рішення буду на поряд вище	Застосування технологій до яких конкуренти не мають доступу що призводить до більш захищеного рівня продукції
За інтенсивністю: марочна	Використання партнерів всесвітньо відомих компаній	Збільшення якості рішення та підвищення довіри

Після аналізу конкуренції було проведено більш детальний аналіз умов конкуренції в галузі (за моделлю 5 сил М. Портера) що приводиться у таблиці 4.9.

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	*Потенційні конкуренти*	*Постачальники*	*Клієнти*	*Товари-замінники*
Складові аналізу	*Thales*	*Gemalto, Samsung, Google, e-Estonia, MDL autoMation*	*Великиі IT компанії які вже мають досвід розробки великих комерційних проектів та довіра завдяки часу на рику*	*Держави які потребують високої надійності продуктів та готові добре фінансувати*	*Замінниками можуть виступати фізичні документи*
Висновки:	Конкретність може полягати в більш захищеному рішенні та з меншою кількістю фінансування	На даний момент є можливість вийти на ринок першим адже конкуренти ще працюють над своїми рішеннями	Постачальники не диктують умови адже їх рішення ще находяться в розробці, будуть диктувати умови ті хто перший представить рішення	Клієнти диктують умови тим що їм потрібне просте та надійне рішення яке не буде їм задавати незручностей	Фактичних обмежень немає адже фізичні документи не перешкоджають електронним і навпаки

На основі проведеної роботи було проведено обґрунтування факторів конкурентоспроможності що наведені у таблиці 4.10.

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)*
	Застосування інноваційних технологій в продукті	На даний момент лише обмежена кількість розробників можуть мати доступ до технологій які використані в продукті
	Якість запропонованої продукції	Розроблений продукт по останнім специфікаціям з дотриманням усіх стандартів безпечної обробки конфіденційних даних
	Простота використання	Немає необхідності в спеціальних навичках або знаннях для використання
	Відносно не велика вартість подальшої підтримки продукту	Кінцевий продукт не буде потребувати великих фінансових вливань при подальшій експлуатації

За визначеними факторами конкурентоспроможності у таблиці 4.10 було проведено аналіз сильних та слабких сторін стартап-проекту що приводяться у таблиці 4.11.

Таблиця 4.11 – Порівняльний аналіз сильних та слабких сторін

№ п/п	*Фактор конкурентоспроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з рішенням*						
			–3	*–2*	*–1*	*0*	*+1*	*+2*	*+3*
1	Застосування інноваційних технологій в продукті	20		+					
2	Якість запропонованої продукції	18		+					
3	Простота використання	15				+			

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) що приведень в таблиці 4.12.

Таблиця 4.12 – SWOT- аналіз стартап-проекту

Сильні сторони: Застосування інноваційних технологій, підвищення захищеності системи за рахунок TEE, eSE, простота використання, не велика вартість подальшої підтримки продукту	Слабкі сторони: необхідність прийняти законів що регулюють електроні ідентифікаційні документи, складність розробки, необхідність використовувати закриті технології
Можливості: пропонування рішення до інших держав, вихід на світовий ринок	Загрози: складність монетизації, отримання прибутку, складність впровадження системи на державному рівні

На основі SWOT-аналізу було розроблено альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації наведено в таблиці 4.13.

Таблиця 4.13 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтовний комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
	Укладення договору з урядом країни	Середня ймовірність отримання ресурсів	Приблизно 2 роки
	Долучення нових розробників до проекту	Висока ймовірність отримання ресурсів	2-3 місяці
	Впровадження нових технологій	Велика ймовірність отримання ресурсів	На протязі всього часу
	Заклик нових клієнтів у виді IT компаній	Середня ймовірність отримання ресурсів	1 рік
	Перетворення проекту в відкритий	Мала ймовірність отримання ресурсів	6 місяців

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів наведено в таблиці 4.14.

Таблиця 4.14 – Вибір цільових груп потенційних споживачів

№ п/п	*Опис профілю цільової групи потенційних клієнтів*	*Готовність споживачів сприйняти продукт*	*Орієнтовний попит в межах цільової групи (сегменту)*	*Інтенсивність конкуренції в сегменті*	*Простота входу у сегмент*
	1. Компанії шо хочуть впровадити контроль фізичного доступу	Готові сприйняти продукт але необхідності немає	Середній рівень попиту для деяких компаній	Конкуренція між схожими рішеннями але в кожного рішення є свої перваги та недолілкт	Не велика складність входу адже не потребує великих затрат на впровадження системи в межах підприємства
	2. Громадяни (всі у кого наявні смартфони)	Клієнти готові прийняти продукт та користуватись	Високій рівень попиту		Середня складність входу адже потребується розвинена інфраструктура
	3. Державні службовці (поліцейські)	Зацікавлені в полегшені та прискорені перевірки документів	Середній рівень попиту		Велика складність входу

Кінець таблиці 4.15

№ п/п	*Опис профілю цільової групи потенційних клієнтів*	*Готовність споживачів сприйняти продукт*	*Орієнтовний попит в межах цільової групи (сегменту)*	*Інтенсивність конкуренції в сегменті*	*Простота входу у сегмент*
	4. Онлайн сервіси яким потрібна ідентифікація користувачів	Низький рівень готовності сприйняти продукт	Низький попит тому що існує необхідність впроваджувати складну систему		Не велика складність входу тому що не потрубує багато ресурсів для розгортання
Які цільові групи обрано: для впровадження було обрано цільові групи в яких велика та середня заківленність в продукті а саме: компанії які хочуть впровадити контроль фізичного доступу, Громадяни (всі у кого наявні смартфони), Державні службовці (поліцейські)					

Для роботи в обраних сегментах ринку було сформовано базову стратегію розвитку шо наведена в таблиці 4.15.

Таблиця 4.15 – Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Ключові конкурентоспроможні позиції відповідно до обраної альтернативи*	*Базова стратегія розвитку**
	Інтеграція	Стратегія диференційованого маркетингу	Розширення діяльності підприємства та покращення продукту	Стратегія розвитку продукту

Наступним кроком було обрано стратегії конкурентної поведінки які навеедні в таблиці 4.16.

Таблиця 4.16 – Визначення базової стратегії конкурентної поведінки

№ п/п	*Чи є проект «першопрохідцем» на ринку?*	*Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?*	*Чи буде компанія копіювати основні характеристики товару конкурента, і які?*	*Стратегія конкурентної поведінки**
1	В цілому ні, якщо враховувати використані технології – так	Вихід на інші ринки та канали збуту є пріорітетною заадчею	Основні характеристики будуть однакові але спосіп їх реалізації зовсім інший	Стратегія лідера

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту що наведено в таблиці 4.5, а також в залежності від обраної базової стратегії розвитку яка наведена в таблиці 4.15 та стратегії конкурентної поведінки з таблиці 4.16 було розроблено стратегію позиціонування що наводиться в таблиці 4.17, що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Таблиця 4.17 – Визначення стратегії позиціонування

№ п/п	*Вимоги до товару цільової аудиторії*	*Базова стратегія розвитку*	*Ключові конкурентоспроможні позиції власного стартап-проекту*	*Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)*
1	Ріешення яке повністю відповідає стандартам, має високий рівень захищеності обробки та зберігання конфіденційних данних, не потребує спеціалізованих навичок та знань для використання	Стратегія розвитку продукту	Розширення діяльності підприємства та покращення продукту	Безпечність даних, простота використання, надійність системи, доступінсть системи, полегшення звичайних прцоессів

4.5 Розроблення маркетингової програми стартап проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у таблиці 4.18 було підсумовано результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити*
1	Ідентифікація особистості	Безпечна та швидка Ідентифікація особистості	Використання новітніх технологій які пропунують максимальний рівень захищенності даних
2	Можливість відновити втрачені дані	Можливість легко відновити втрачені конфіденційні дагні	Не має необхідності робити складні запити та довго чекати необхідно лише натиснути одну кнопку
3	Надійність\ автентичність даних	Можливість однозначно встановити особистість	Завдяки використанню новітніх технологій та криптографії автентичність даних не викликає сумніву

Кінець таблиці 4.18

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити*
4	Можливість онлайн доступу автентифікації до ресурсу	Завдяки мобільні ідентифікації можно впровадити онлайн атентифікацію	Можливість використовувати власні ідентифікаційні дані для автентифікації на онлай ресурсах для отримання певних послуг

Надалі було розроблено трирівневу маркетингову модель товару: уточнюєть-ся ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання у таблиці 4.19.

Таблиця 4.19 – Опис трьох рівнів моделі товару

Рівні товару	*Сутність та складові*
І. Товар за задумом	Система однозначної ідентифікації особистості яка гарантує автентичність даних на мобільних пристроях

Кінець таблиці 4.19

Рівні товару	*Сутність та складові*		
	1. Застосування інноваційних технологій в продукті	М	Тл
	2. Швидка ідентифікація	М	Тх
	3. Надійність конфіденцйних даних	М	Тл
	4. Простота використання	Нм	Ор
	Якість: розроблено на основі стандарту ISO 180013-5		
	Пакування: Представлення готового підписанного продукту у вигляді 3 додаків (аплет, траслет, Andriod – застосунок)		
	Марка: Best e-ID inc.		
III. Товар із підкріпленням	До продажу: долучення нових клєнтів та партнерів для розвитку та розгортування системи		
	Після продажу: підтримка готови рішень та вихід на міжнародний ринок		
За рахунок чого потенційний товар буде захищено від копіювання: застосуноки для eSE та TEE (аплет та траслет) будуть встановлені довірениими сторонома, а Andriod застосунок буде підписаний приватним ключем розробника та мати сертифікат			

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів що наведено у таблиці 4.20. Аналіз прово-диться експертним методом.

Таблиця 4.20 – Визначення меж встановлення ціни

№ п/п	*Рівень цін на товари-замінники*	*Рівень цін на товари-аналоги*	*Рівень доходів цільової групи споживачів*	*Верхня та нижня межі встановлення ціни на товар/послугу*
	10000 – 50000	100000 – 200000	300000 – 600000	10000000 500000

Наступним кроком було визначення оптимальної системи збуту, в межах яко-го приймається рішення приводиться в таблиці 4.21.

Таблиця 4.21 – Формування системи збуту

№ п/п	*Специфіка закупівельної поведінки цільових клієнтів*	*Функції збуту, які має виконувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*
	Купити один раз та користуватись постійно	Впровадити можливість збуту товару для кожного	Канал нульового рівня	Через власну систему збуту

Останньою складової маркетингової програми було розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів що приводиться у таблиці 4.22.

Таблиця 4.22 – Концепція маркетингових комунікацій

№ п/п	*Специфіка поведінки цільових клієнтів*	*Канали комунікацій, якими користуються цільові клієнти*	*Ключові позиції, обрані для позиціонування*	*Завдання рекламного повідомлення*	*Концепція рекламного звернення*
	Люди які хочуть зручно та швидко користувати сь новітніми технологіями для ідентифікації особистості	Інтернет, презентації, каталоги	Забезпечення максимального рівня захищенності конфіденційної інформації для ідентифікації особистості	Переконати клієнтів в тому що рішення просте та зручне в використанні і повністю залишає захищенним їх дані	Представлення вигід пропозиції та придання особливості продукту

Висновки до розділу 4

В межах даного розділу було проведено аналіз ринку та розроблено план стартап проекту для виведення його на ринок, було розроблено кроки в межах яких було визначено ринкові перспективи проекту, описано ідеї стартап-проекту, визначено сильних, слабких та нейтральних характеристик ідеї проекту, визначена технологічна здійсненність проекту та характеристика потенційного

ринку стартапу і характеристика потенційних клієнтів, також фактори загроз та можливостей, проаналізовано конкуренції на ринку і проведено порівняльний аналіз сильних та слабких сторін, було обрано цільові групи потенційних споживачів та визначено базової стратегії розвитку, позиціонування та ключових переваг концепції потенційного товару, останнім було сформовано системи збуту та концепцію маркетингових комунікацій.

На даний момент є однозначний попит на продукцію стартап проекту, а тому можлива комерціалізація продукту, динаміка ринку показує позитивний зріст попиту на мобільні послуга а саме на можливість ідентифікації особистості за допомогою смартфонів. Клієнти зацікавлені в простих але ефективних рішеннях тому проект має гарні перспективи впровадження системи на ринку також існує гарна конкурентоспроможність проекту адже конкуренти не пропонують рішення з використанням останніх технологій захисту конфіденційних даних на мобільних пристроях, проекти знаходяться в розробці. Але з іншого боку бар’єром виходу на ринок може бути складність прийняття необхідних законів та норм регулювання електронної ідентифікації. Не зважаючи на бар’єри подальша імплементація проекту є доцільною оскільки рішення є захищеним, простим у використанні та ефективним в сфері технологій ідентифікації особистості.

ВИСНОВКИ

В результаті роботи:

1. Було знайдено та проаналізовано існуючі рішення електронної та мобільної ідентифікації в різних країнах; встановлено що ці рішення базуються на таких технологіях: на основі SIM карт та на основі смарт карт з вбудованим елементом безпеки.

2. Проаналізовано технології які використовуються для реалізації електронної ідентифікації та виявлено наявні вразливості та можливі атаки на існуючих рішення.

3. Було визначено нові технології які забезпечують підвищення рівня безпеки конфіденційних даних на мобільних пристроях.

4. Запропоновано механізми підвищення рівня безпеки конфіденційних даних на мобільних пристроях з використанням визначених технологій та реалізовано модуль, що реалізує цифровий ідентифікаційний документ на мобільному пристрої під ОС Андроїд, взаємодія з пристроєм для перевірки здійснюється по протоколу NFC.

Рішення відрізняється від існуючих підвищеним ступенем захищеності даних за рахунок шифрування даних під час взаємодії “клієнт – зчитувач”, зберігання підписаного документа в embedded Secure Element мобільного пристрою, та захисту від NFC Relay Attack шляхом запровадження ЕЦП передаваних даних між сканером та пристроєм.

7. Виконано перевірку захищеності рішення шляхом відтворення NFC Relay Attack, яка засвідчила працездатність запропонованого рішення.

8. Розроблено модель розгортання системи цифрових ідентифікаційних посвідчень на мобільних пристроях, яка може допомогти в розгортанні системи в реальному житті.

9. Розроблено стартап проект та план для виведення на ринок, було визначено ринкові перспективи проекту, описано ідеї стартап-проекту, визначено сильних, слабких сторін проекту та визначено що рішення має гарні перспективи комерціалізації системи.

Практична значення роботи полягає у можливості використання даного рішення для представлення звичайних, фізичних документів на мобільних пристроях з гарантуванням автентичності, наприклад використовувати мобільний телефон як паспорт або водійське посвідчення. Та можливості використання рішення для систем контролю фізичного доступу до ресурсів або об’єктів. Також представлена модель розгортання даної системи що може допомогти в розгортанні систем цифрових ідентифікаційних посвідчень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Paul James. Despite the Terrors of Typologies: The Importance of Understanding Categories of Difference and Identity. [Елетронний ресурс] // J. Paul. – 2015. – Режим доступу до ресурсу: https://www.academia.edu/11768378/_Despite_the_Terrors_of_Typologies_The_Importance_of_Understanding_Categories_of_Difference_and_Identity_2015_

2. Gemalto. What is digital identity? [Елетронний ресурс] // Gemalto. – 2017. – Режим доступу до ресурсу: https://www.justaskgemalto.com/en/what-is-digital-identity/

3. Telefonica. New Paradigms of Digital Identity: Authentication and Authorization as a Service. [Елетронний ресурс] // Telefonica. – 2016. – Режим доступу до ресурсу: https://www.elevenpaths.com/wp-content/uploads/2015/10/Telefonica_LVTI2N.pdf

4. Ben Quarmby. The Case for National DNA Identification Cards. [Елетронний ресурс] // B. Quarmby. – 2003. – Режим доступу до ресурсу: https://scholarship.law.duke.edu/dltr/vol1/iss1/72/

5. Simone Piunno, Valerio Paolini. The Advantages of the Electronic ID Card, now easier to obtain with the new “CIE Agenda”. [Елетронний ресурс] // S. Piunno. – 2018. – Режим доступу до ресурсу: https://medium.com/team-per-la-trasformazione-digitale/italy-electronic-identity-card-id-cie-agenda-online-booking-system-appointment-municipality-4983dc1abba5

6. European Commission. Electronic Identities – a brief introduction. [Елетронний ресурс] // European Commission. – Режим доступу до ресурсу: https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf

7. Julia Clarka, Mariana Dahana, Vyjayanti Desaia. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. [Електронний ресурс] // J. Clarka. – 2016 – Режим доступу до ресурсу: https://secureidentityalliance.org/publications-docman/public/4-july-2016-report-digital-identity/file

8. PostFinance. Digital Banking. [Електронний ресурс] // PostFinance. – 2019 – Режим доступу до ресурсу: https://www.postfinance.ch/en/private/products /digital-banking.html

9. GSMA Mobile Identity team & Turkcell. Mobile Signature in Turkey A case study of Turkcell: MobilImza. [Електронний ресурс] // GSMA. – 2012 – Режим доступу до ресурсу: https://www.gsma.com/identity/wp-content/uploads/2012/09/MI_Turkcell Report_print_FINAL.pdf

10. E-estonia. E-identity. [Електронний ресурс] // E-estonia. – 2019 – Режим доступу до ресурсу: https://e-estonia.com/solutions/e-identity/id-card/

11. DigiDoc. DigiDoc software. [Електронний ресурс] // DigiDoc. – 2019 – Режим доступу до ресурсу: https://www.ria.ee/en/state-information-system/eid/digidoc-software.html

12. Detailed voting result. [Електронний ресурс] // E-estonia. – 2014 – Режим доступу до ресурсу: http://ep2014.vvk.ee/detailed.html

13. Gemalto. eID in Finland: A new card design for 2017. [Електронний ресурс] // Gemalto. – 2019 – Режим доступу до ресурсу: https://www.gemalto.com/govt/customer-cases/finland

14. Globaldata Consortium. Electronic Identity Verification in Norway. [Електронний ресурс] // Globaldata. – 2019 – Режим доступу до ресурсу: https://globaldataconsortium.com/ electronic-identity-verification-norway/

15. Bolagsverket. Swedish e-identification. [Електронний ресурс] // Bolagsverket. – 2018 – Режим доступу до ресурсу: https://bolagsverket.se/ en/fee/e-services/swedish-e-identification-1.16393

16. Globaldata Consortium. Electronic Identity Verification in the UK. [Елетронний ресурс] // Globaldata. – 2019 – Режим доступу до ресурсу: https://globaldataconsortium.com/electronic-identity-verification-uk/

17. Mobile World Capital. Mobile Identity Delivering secure, accessible and trusted services to the public. [Елетронний ресурс] // Mobile World Capital. – Режим доступу до ресурсу: http://mobileworldcapital.com/ID_M/mIDENG/MWCapital_mID_vENG.pdf

18. Infotech. Electronic Identity. [Елетронний ресурс] // Infotech. – 2018 – Режим доступу до ресурсу: https://www.x-infotech.com/markets/electronic-identity/

19. DIGITAL INDIA, TECHNOLOGY. Digital Identity: The Pros, The Cons & Everything In-Between. [Елетронний ресурс] // DIGITAL INDIA. – 2018 – Режим доступу до ресурсу: https://www.indiamobilecongress.com/digital-identity-the-pros-the-cons-everything-in-between/

20. Zhiqun Chen. JavaCard Technology for SmartCards [Текст] / Lisa Frindly, Tim Lindholm, Ken Arnold, Jim Inscor // Architecture and Programmer's Guide. – 2000. – С. 178 – 201.

21. Isabelle Attali. Smart Card Programming and Security [Текст] / Thomas P. Jensen // International Conference on Research in Smart Cards, E-smart 2001. – 2001. – С. 19 – 28.

22. Oracle. JAVA CARD SPECIFICATION. [Елетронний ресурс] // Oracle. – 2019 – Режим доступу до ресурсу: https://www.oracle.com/technetwork/java/embedded/javacard/downloads/index.html

23. Eduardo Simonetti. Mobile ID in Physical Access Control Applications [Текст] // Smartphones integration into security solutions and access control systems PACS. – 2016. – С. 10 – 19.

24. Atul Kumar. Security Analysis of Mobile Payment Systems [Текст] / F.E. Kargl, Jordi van den Breekel, Eleonora Petridou. – 2015. – С. 37 – 39.

25. Margaret Rouse. Evaluation Assurance Level (EAL). [Елетронний ресурс] // M. Rouse. – Режим доступу до ресурсу: https://www.oracle.com/technetwork/java/embedded/javacard/downloads/index.html

26. Zaheer Ahmad. Enhancing the Security of Mobile Applications by using TEE and (U)SIM [Текст] / Lishoy Francis, Tansir Ahmed, Christopher Lobodzinski. Dev Audsin, Peng Jiang. . – 2013. – С. 2 – 5.

27. Don Felton. What is TrustZone? [Елетронний ресурс] // Trustonic. – 2019 – Режим доступу до ресурсу: https://www.trustonic.com/ news/technology/what-is-trustzone/

28. Richard Hayton. The Benefits of Trusted User Interface (TUI). [Елетронний ресурс] // Trustonic. – 2019 – Режим доступу до ресурсу: https://www.trustonic.com/news/blog/benefits-trusted-user-interface/

29. AOSP. Trusty TEE. [Елетронний ресурс] // AOSP. – 2019 – Режим доступу до ресурсу: https://source.android.com/security/trusty

30. Vedat Coskun. Overview of Near Field Communication [Текст] / Kerem Ok, Busra Ozdenizci // PROFESSIONAL NFC Application Development for Android. – 2013. – С. 5 – 22.

31. Mobiil-ID. Что такое Mobiil-ID? [Елетронний ресурс] // Mobiil. – 2019 – Режим доступу до ресурсу: https://www.id.ee/index.php?id=36904

32. MinID. MinID. [Елетронний ресурс] // MinID. – 2019 – Режим доступу до ресурсу: http://eid.difi.no/nb/minid

33. Lakatos. #WIBattack: Vulnerability in WIB sim-browser can let attackers globally take control of hundreds of millions of the victim mobile phones worldwide to make a phone call, send SMS to any phone numbers, send victim’s location, launch WAP browser, etc. [Елетронний ресурс] // Ginno Security Laboratory. – 2019 – Режим доступу до ресурсу: https://ginnoslab.org/2019/09/21/wibattack-vulnerability-in-wib-sim-browser-can-let-attackers-globally-take-control-of-hundreds-of-millions-of-

the-victim-mobile-phones-worldwide-to-make-a-phone-call-send-sms-to-any-phone-numbers/

34. Zak Doffman. New SIM Card Attacks: Both Android And iOS Impacted—Are You Vulnerable? [Елетронний ресурс] // Z. Doffman. – 2019 – Режим доступу до ресурсу: https://www.forbes.com/sites/zakdoffman/2019/09/28/ how-many-millions-of-phones-risk-sim-based-attacks-new-report-provides-answers/#6275ff9e32ea

35. Антон Кочуков. Атака на протокол SS7: как перехватить чужие звонки и SMS. [Елетронний ресурс] // networkguru .– Режим доступу до ресурсу: https://networkguru.ru/ataka-na-protokol-ss7/

36. Oliver K¨ommerling. Design Principles for Tamper-Resistant Smartcard Processors [Текст] / Markus G. Kuhn. – 2012. – С. 1 – 11.

37. Orlin Grabbe. Smart Cards and Private Currencies [Текст] / Anderson, Ross, Markus Kuhn// International Financial Markets. – 1999. – С. 98 – 105.

38. Ross Anderson. Low Cost Attacks on Tamper Resistant Devices [Текст] / Markus Kuhn. – 2010. – С. 3 – 8.

39. Simon Blythe. Layout Reconstruction of Complex Silicon Chips [Текст] / Beatrice Fraboni, Haroon Ahmed // IEEE Journal of Solid-State Circuits. – 1993. – С. 138 – 145.

40. Ross Anderson. Tamper Resistance — a Cautionary Note [Текст] / Markus Kuhn // Sixth USENIX Security Symposium Proceedings. – 1996. – С. 65 – 73.

41. WolfgangRankl. Overview about attacks on smart cards [Текст] // Information Security Technical Report Volume 8, Issue 1. – 2003. – С. 3 – 18.

42. Michael Roland. Practical Attack Scenarios on Secure Element-enabled Mobile Devices [Текст] / Josef Langer, Josef Scharinger // Information Security Technical Report. – 2012. – С. 4 – 6.

43. Salvador Mendoza. Intro to NFC Payment Relay Attacks. [Елетронний ресурс] // salmg. – 2018 – Режим доступу до ресурсу: https://salmg.net/2018/12/01/intro-to-nfc-payment-relay-attacks/