INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Host Card Emulation with Tokenisation

Security Risk Assessment

Luís Manuel Pereira da Fonte

2019

INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Mestrado em Engenharia de Segurança Informática

Host Card Emulation with Tokenisation

Security Risk Assessment

Elaborado por:

Luís Manuel Pereira da Fonte

Orientado por:

Engenheiro Valentim Vieira de Oliveira, SIBS, S.A.
Professor Doutor João Paulo Mestre Pinheiro Ramos e Barros, IPBeja

Dissertação de Mestrado realizada na empresa Sociedade Interbancária de Serviços, S.A. (SIBS, S.A.), apresentado na Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Beja

2019

Resumo

Host Card Emulation with Tokenisation

Security Risk Assessment

Host Card Emulation (HCE) é uma arquitetura que possibilita a representação virtual (emulação) de cartões *contactless*, permitindo a realização de transações através dispositivos móveis com capacidade de realizar comunicações via Near-Field Communication (NFC), sem a necessidade de utilização de um microprocessador chip, Secure Element (SE), utilizado em pagamentos NFC anteriores ao HCE.

No HCE, a emulação do cartão é efetuada essencialmente através de software, geralmente em aplicações do tipo *wallet*. No modelo de HCE com Tokenização (HCEt), que é o modelo HCE específico analisado nesta dissertação, a aplicação armazena tokens de pagamento, que são chaves criptográficas derivadas das chaves do cartão original, críticas, por permitirem a execução de transações, ainda que, com limitações na sua utilização. No entanto, com a migração de um ambiente resistente a violações (SE) para um ambiente não controlado (uma aplicação num dispositivo móvel), há vários riscos que devem ser avaliados adequadamente para que seja possível materializar uma implementação baseada no risco.

O presente estudo descreve o modelo de HCE com Tokenização (HCEt) e identifica e avalia os seus riscos, analisando o modelo do ponto de vista de uma aplicação *wallet* num dispositivo móvel, que armazena tokens de pagamento para poder realizar transações *contactless*.

Palavras-chave: *Host Card Emulation, Tokenização, Análise de Risco, Near-Field Communication; Dispositivo Móvel.*

Abstract

Host Card Emulation with Tokenisation

Security Risk Assessment

Host Card Emulation (HCE) is an architecture that provides virtual representation (i.e., emulation) of contactless cards, enabling transactional communication for mobile devices with NFC support without the need of Secure Element (SE) hardware. In contrast to NFC payments prior to HCE, card emulation is performed mainly by software, usually in wallet-like applications.

In the HCE with Tokenisation (HCEt) model, which is the specific HCE model analysed in-depth in this dissertation, the application stores payment tokens, which are cryptographic keys derived from the original and critical card keys. These enable the execution of transactions, yet, are limited in their utilisation. However, with the migration from a tamper-resistant to an uncontrolled environment (i.e., an application on a mobile device), there are several risks that need to be properly evaluated in order to be able to materialise a risk-based implementation.

This study describes the HCEt and proposes the identification and assessment of its risks, analysing the model from the point of view of a wallet application on a mobile device that has payment tokens stored to be able to perform contactless transactions.

Keywords: *Host Card Emulation, Tokenisation, Risk Assessment, Near-field Communication, Mobile Device.*

Agradecimentos

A realização desta dissertação deve-se ao contributo, apoio e confiança, de inúmeras pessoas. A todos em geral, gostaria de prestar o meu agradecimento por terem tornado este estudo possível.

Agradeço ao meu coordenador e orientador, Engenheiro Valentim Vieira de Oliveira, por me ter aceitado como seu aprendiz, pelas várias horas de lições de imensurável valor, pela constante disponibilidade e interesse na condução deste estudo, pela paciência e amizade prestadas.

Ao Professor Doutor João Paulo Barros, por ter aceitado ser o meu orientador no Instituto Politécnico de Beja (IPBeja), pelo importante e determinante apoio, dedicação, por ter estado sempre disponível, e pelo interesse em contribuir sempre no sentido de tornar o produto final no melhor possível.

À Sociedade Interbancária de Serviços (SIBS), aos colegas (na SIBS) Gonçalo Pereira, Jerónimo Ferreira e João Cruz, aos colegas e Professores do Mestrado em Engenharia de Segurança Informática (MESI), bem como ao IPBeja e à Escola Superior de Gestão de Beja (ESTIG).

Por fim, dedico esta dissertação à minha família, sem a qual acima de tudo, a realização desta dissertação não teria sido possível. Aos meus pais, Manuel e Maria, à minha companheira Sofia, e ao meu irmão Manuel.

O meu sincero agradecimento a todos.

Contents

List of Figures

List of Tables

Abreviations

AAC	Application Authentication Cryptogram
AC	Application Cryptogram
APDU	Application Data Unit
ARQC	Authorisation Request Cryptogram
CDA	Combined Data Authentication
CVM	Cardholder Verification Methods
DoS	Denial of Service
EC	Existing Controls
EMV	Europay, MasterCard and VISA
HCE	Host Card Emulation
HCEt	Host Card Emulation with Tokenisation
IT	Information Technology
MAC	Message Authentication Code
MFA	Mobile Financial Applications
MFS	Mobile Financial Services
MNO	Mobile Network Operator
NFC	Near-Field Communication
ODA	Offline Data Authentication
OS	Operating System
P2P	Peer-to-Peer
PAN	Primary Account Number
PIN	Personal Identification Number
POS	Point-of-Sale
RFID	Radio-Frequency Identification
SDA	Static Data Authentication
SE	Secure Element
SIM	Subscriber Identity Module
SP	Service Provider
TC	Transaction Certificate
TSP	Token Service Provider
UICC	Universal Integrated Circuit Card
VTE	Virtual Target Emulation

Chapter 1

Introduction to the Study

Host Card Emulation along with Tokenisation has become a game changer for the mobile payments ecosystem, combining the virtualisation of payment, loyalty and ticketing contactless cards on mobile devices enabling them to be used through NFC. Along with the capabilities of this technology, many threats have emerged and this dissertation proposes to assess the risks.

1.1 Introduction to the Problem

The usage of payment cards as a universal payment method, and in particular the Europay, Mastercard and VISA (EMV) card[1] [1], which has greatly enhanced the security of card payments (see Chapter 2), along with the development of the contactless card[2] technology (see 2.1.2), has created a slew of new use cases based on portability and convenience for the users. Similarly, the growth in the usage [2] and in the capabilities of smartphones [3] has also made it possible to virtualise essential physical objects in people's lives, such as banking cards, likewise the mobile banking services already accessible through smartphones for several years.

For many years, the emulation of cards in mobile devices has been used by financial entities and to this day various forms of emulation have been used (see 3.2). All of the emulation methods have advantages and disadvantages at the business and operability level, as well as associated risks. One of these implementations is Host Card Emulation based on Tokenisation (see 3.3.2), in which the emulation of the banking card is made by software in a mobile application, storing inside cryptographic keys (tokens) derived from the original keys of the physical cards. Thus, the processes of key provisioning and management for the execution of payments (via NFC) is simpler, compared to implementations based on SE, which by design has a high level of security[3] [4].

[1] Represents more than 50% of the cards in the world

[2] Taking advantage of the NFC technology

[3] SEs are tamper-proof microprocessor chips

Emulating a secure microprocessor chip with cryptographic keys on an application that can authenticate financial transactions in a general purpose device, places a challenge in keeping the risks at acceptable levels.

1.2 Background of the Problem

Chip cards are designed having a set of various strong security controls [4] at multiple levels[4] such as hardware memory encapsulation, security logic (sensors), encrypted connections between on-chip elements, application separation and restricted file access.

Although smartphones were not designed having security as their main concern, they do have some basic security mechanisms [5] such as multiple authentication methods[5], sandboxing and application specific permissions. Yet, many threats subsist [6], such as the lack of control of software that is placed in the devices and in app stores[6], unauthorised user location tracking by the applications installed and a significant exposure to malware attacks [7] allied to the rates of unpatched devices and published vulnerabilities [8].

These threats represent some of the challenges related to the security of smartphones that need to be evaluated for the HCEt model, considering, for example, the storage of cryptographic keys within the mobile application, and the communications exchanged between the smartphone and the Point of Sale (POS) terminal for payment acceptance, establishing direct dependency on the security of the device.

1.3 Statement of the Problem

Performing and managing the emulation of chip cards by software, storing the keys (tokens) in the application as well as other critical data, necessarily creates dependency on the security levels of the application, the mobile device, the service support infrastructure, as well as the level of awareness in information security of the user.

All these dependency factors, which are also points of failure, represent exposure to several threats that pose different risks to the security of the solution and its assets.

Emulating a secure cryptographic device, such is the chip card, on a smartphone rises the risks of performing financial transactions. Although some controls have been implemented, a clearer view of subsisting risks should be evaluated.

1.4 Aims and Objectives of the Study

This dissertation seeks to perform a risk assessment regarding the HCEt model, in which card cryptographic keys derived from the physical Universal Integrated Circuit Card

[4] Human-readable, smart card chip, operating system and network

[5] For example, PIN, pattern or biometric

[6] Leading to malware and rogue application attacks

(UICC) keys are stored within the application for performing the emulation of contactless cards when in communication with payment terminals through NFC.

1.5 Statement of Purpose and Research Question

The purpose of this dissertation is to determine the most relevant risks in the HCEt model implemented on a mobile device and classify them in terms of likelihood and impact of exploitation, from the perspective of Security IT professionals in specific and IT professionals in general.

1.6 Definition of Terms

The following key terms are used along the study:

Host Card Emulation (HCE):
Architecture that provides virtual representation (e.g. emulation) of contactless cards[7] by software, enabling transactional communication for mobile devices through NFC.

Tokenisation:
The process of replacing the Primary Account Number (PAN) by a surrogate number (token) for a specific or limited replacement of card data, keeping a cryptographic link to the initial PAN.

Host Card Emulation with Tokenisation (HCEt):
Combining HCE and Tokenisation, HCEt consists in the same as HCE, but instead of using the original PAN numbers of the physical contactless cards for performing transactions, it uses tokens[8], stored inside the mobile application. Through HCEt, merchant terminals that accept contactless cards may accept payments from HCE devices with no need to change terminal software or hardware.

1.7 Research Method

The research method for this dissertation was to conduct a survey in order to determine risks and its levels for the HCEt model, administered through a questionnaire answered by the participants.

Being a relatively recent technology and still in consolidation in the tech world, there are yet no relevant studies on the specific related risks. Given this, and in order to solve the lack of existent documentation, it was important to base the risk estimation on the opinion

[7] Payment, loyalty and ticketing cards

[8] Limited in its use, due to risk management

of Information Security and Information Technology (IT) experts with qualifications and experience, to ensure that the risk estimation is executed as impartially and assertively as possible.

For the mentioned, a survey was conducted in order to gather informed opinions about a risk classification based on the threats identified in the study "Risk Management in Mobile Financial Services - The Risk Review" [9] conducted by the entity Mobey Forum and regarding the mobile environment in a collaboration that included several experts in banking solutions and risk management of various renown financial entities.

1.8 Contributions

With the results obtained from the survey, the risk levels for each threat were identified and presented as well as a brief analysis profiling the answers, by categories. As the last step of the assessment, the Risk Evaluation is presented, ranking the identified risks by their levels of severity.

1.9 Description of Thesis Organisation

The following chapter, "Chapter 2: Description of EMV and Chip Transaction Types", will look into the EMV history and its main features such as operation modes[9], security controls[10] and the specifications of contactless cards.

In "Chapter 3: Host Card Emulation", the HCE technology is described, starting with the background and history of HCE, from the first types of card emulation based in SEs and the first HCE implementations, to the detailed explanation of the main HCE models.

"Chapter 4: Risk Assessment Methodology" defines the structure and the methodology for the risk assessment performed on Chapters 5 and 6, according to the industry's good practices. The concepts, processes, sub processes, evaluation variables and methods are described, as well as the matrix used to calculate the risk levels.

"Chapter 5: Conducted Survey for Host Card Emulation with Tokenisation Risk Analysis" presents a survey conducted in order to perform the HCEt Risk Analysis based on the opinion and evaluation of Information Security and IT experts.

In "Chapter 6: Host Card Emulation with Tokenisation: Security Risk Assessment", the risk assessment to HCEt is performed, supported by the results obtained from the survey described in Chapter 5. Furthermore, a brief analysis of the answers obtained is performed in order to profile the opinions of the specialists by subjects and answer types.

Finally, "Chapter 7: Consolidated Risk Evaluation" summarises the study and draws final conclusions and recommendations for future research.

[9] Contact and contactless

[10] Which represent security enhancements to the card industry

Chapter 2

Description of EMV and Chip Transaction Types

EMV is the leading global standard set of specifications[1] for chip card payments and acceptance devices. This Chapter describes the essential about its operation modes, security controls and specifications of contactless cards in order to convey a basic, but solid understanding about the chip cards emulated in the HCEt architecture.

2.1 History and Background

The EMV specifications are managed by EMVCo and its development started in 1994 by the founding entities Europay (acquired by MasterCard in 2002), MasterCard, and VISA. These specifications were developed to define a set of requirements that ensure interoperability (between terminals and chip-based payment cards) and acceptance of secure transactions. Chip-based payment cards (Figure 2.1) contain embedded microprocessors that provide strong transaction security features and other capabilities not possible with traditional magnetic stripe cards. The primary purpose was to define a single global standard chip-based specification for credit and debit payment cards. Currently, EMVCo is composed by the north american companies American Express, Discover, MasterCard and VISA, the japanese JCB, and the chinese UnionPay.

According to latest EMV statistics from 2017 [15], which can be seen in Figure 2.2, there are over 7 Billion active EMV chip cards in the world. These numbers are increasing more prominently in the USA[2], with a massive adoption increase of approximately 578% since September of 2015 [16].

[1] Referring to the main EMV books: Book 1, Book 2, Book 3, and Book 4 [10, 11, 12, 13]

[2] But also in Asia as statistics reveal

Figure 2.1: EMV Card Mockup (image from [14])

2.1.1 Main Features

EMV standards define protocols and data formats for the communication exchange between a chip card and a terminal, which can be an ATM[3], a POS, or hand-held internet banking token [18].

The design of EMV has as its main achievements the interoperability and a higher level of security for card payments resulting in a reduction of counterfeit cards and subsequent fraud losses [19]. EMV chip cards have security distinguishing features, since the payment application inside the secure chip has, for example, the ability to perform processing functions, cryptographic processing, and store confidential information securely.

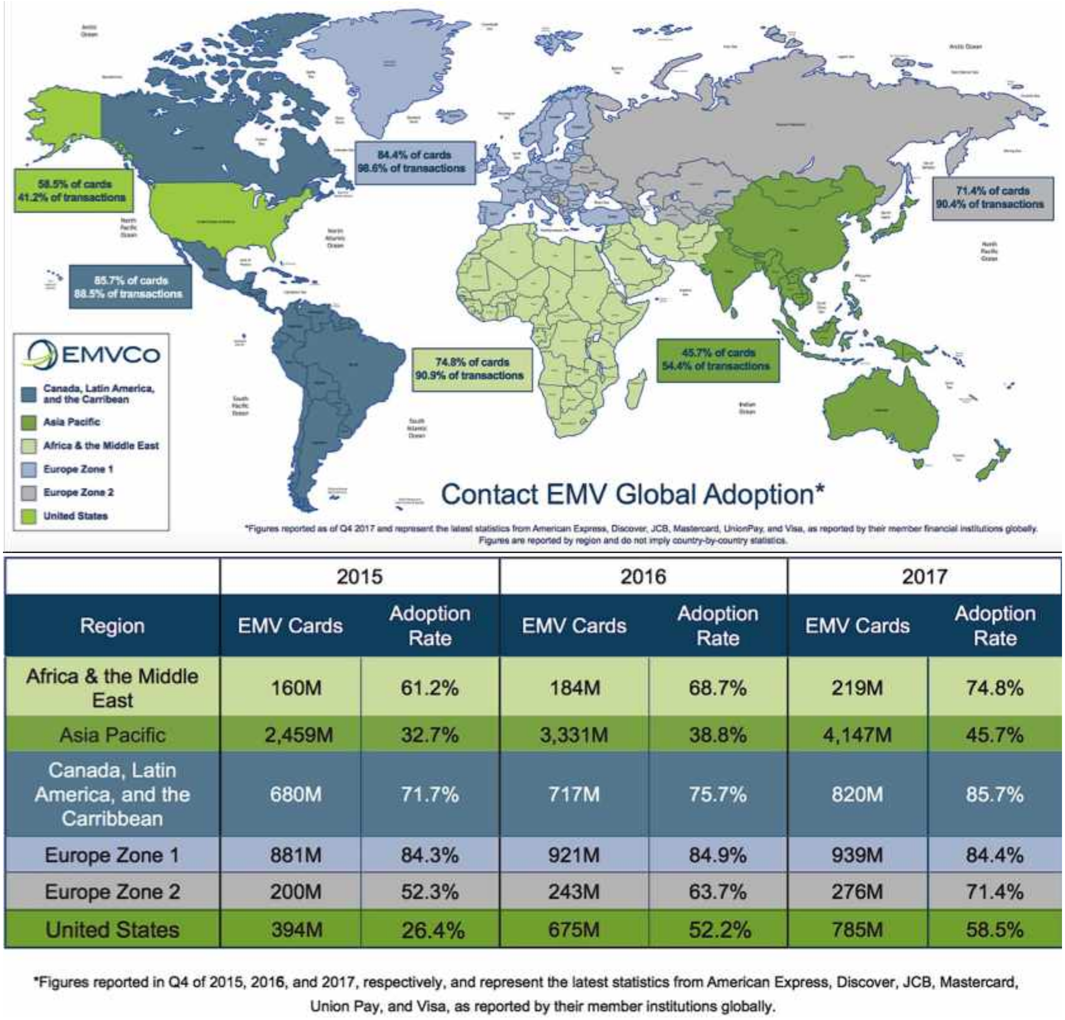
The main features [20] defined by EMV are:

- **Authentication of the chip card** to verify the card is genuine so as to protect against counterfeit fraud for both online authorised transactions and offline transactions. For the online transactions, the card can be validated by the issuer using a dynamic cryptogram, and offline with the terminal using Offline Data Authentication (ODA) methods (see Section 2.2.1);

- **Risk management and authorisation controls** to define the conditions under which the issuer will permit the chip card to be used offline or force transactions online for authorisation under certain conditions (such as, offline limits being exceed);

- **Digitally signed payment data** for transaction authentication and integrity, and more robust **Cardholder Verification Methods (CVM)** to protect against lost and stolen card fraud for EMV transactions.

[3] Automated Teller Machine



Contact EMV Global Adoption*

*Figures reported as of Q4 2017 and represent the latest statistics from American Express, Discover, JCB, Mastercard, UnionPay, and Visa, as reported by their member financial institutions globally. Figures are reported by region and do not imply country-by-country statistics.

	2015		2016		2017	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Africa & the Middle East	160M	61.2%	184M	68.7%	219M	74.8%
Asia Pacific	2,459M	32.7%	3,331M	38.8%	4,147M	45.7%
Canada, Latin America, and the Carribean	680M	71.7%	717M	75.7%	820M	85.7%
Europe Zone 1	881M	84.3%	921M	84.9%	939M	84.4%
Europe Zone 2	200M	52.3%	243M	63.7%	276M	71.4%
United States	394M	26.4%	675M	52.2%	785M	58.5%

*Figures reported in Q4 of 2015, 2016, and 2017, respectively, and represent the latest statistics from American Express, Discover, JCB, Mastercard, Union Pay, and Visa, as reported by their member institutions globally.

Figure 2.2: Worldwide EMV Chip Card Deployment and Adoption - EMV Chip Deployment Stats 2017 [17]

2.1.2 EMV Operation Modes

EMV has defined two different technologies for cards:

1. **Contact:**
    - Chip is embedded in a card;
    - A chip card is inserted into a smart card reader;
    - Communication is established by the contact between the contact points on the chip, making contact with the card reader;
    - The card must remain in the slot for the duration of the transaction.

2. **Contactless:**
   - The chip has a connected antenna that enables wireless communication with a contactless reader for transaction execution;
   - Both the chip and the reader have an antenna and use Radio-Frequency Identification (RFID) technology;
   - The chip may be embedded in cards, key fobs, stickers, mobile phones, etc.;
   - A contactless chip requires close proximity to a reader ("tap and go"), to a maximum distance of 10cm[4] (approximately);
   - The transmission of information between the chip and the terminal is faster due to the capability of performing some steps of the transaction after the card has left the proximity of the reader.

EMV cards typically support contact technology or both contact and contactless technology (dual-interface).

Contactless Cards

Although similar to the contact cards[5], contactless cards (Figure 2.3) have the capability of working through RFID technology and to perform some of the transaction steps after the chip has left the proximity of the reader, which results in faster transactions. They have an embedded antenna in the plastic that enables wireless communication with a contactless reader for the data exchange.

Due to the fact that for contactless communication no physical contact is needed, the concept of payment cards can be extended from "card" to "device", due to the multifunctionality of both RFID and NFC. This means that contactless payments can be performed not just by contactless cards, but other devices such as:

- Mobile phones;
- Key fobs;
- Watches.

2.1.3 Key Infrastructure

Regarding cryptographic keys, and based on [23], the setup of a regular EMV card complies with the following key setup, which is illustrated in Figure 2.4:

- Every card has a unique symmetric key MK_{AC} derived from the issuer's master key IMK_{AC}. Using this key (MK_{AC}), a session key SK_{AC} can be computed, based

[4] According to ISO/IEC 14443

[5] Its specifications [21] also refer to the contact specifications

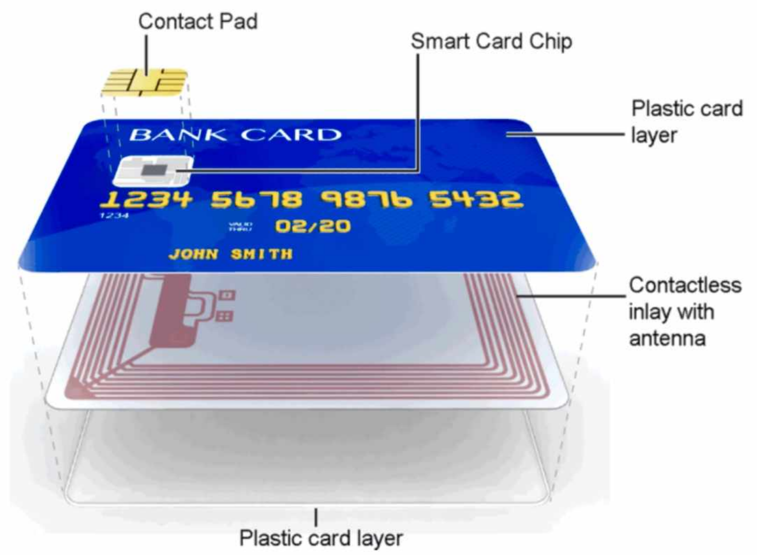


Figure 2.3: Representation of a Contactless Card with Antenna (image from [22])

on the Application Transaction Counter (ATC) or other variables, depending of the algorithm used - step 1 of Figure 2.4;

- The issuer has a public-private key pair (P_I, S_I), and has the P_I key signed by the payment system's private key S_{PS} - steps 2 and 3 of Figure 2.4;

- The terminals know the payment system's public key P_{PS}, which is sent by the payment systems to acquirers (step 5), and then distributed to the terminals and ATMs - step 6 of Figure 2.4;

- Cards that support asymmetric cryptography have a public-private key pair, P_{IC} and S_{IC}. The P_{IC} is signed by the issuer's private key S_I, and the issuer's public key P_I is signed by the payment system's private key S_{PS} - step 4 of Figure 2.4;

This key setup is the basis of trust between the different parties, providing cards with two mechanisms to prove the authenticity of the data:

1. All EMV cards can calculate Application Cryptograms (AC) using the shared symmetric key with the issuing bank. The issuer can check these ACs to verify the authenticity of the messages;

2. Cards that support asymmetric cryptography can also digitally sign data to prove their authenticity to the terminal, as well as to the issuer.

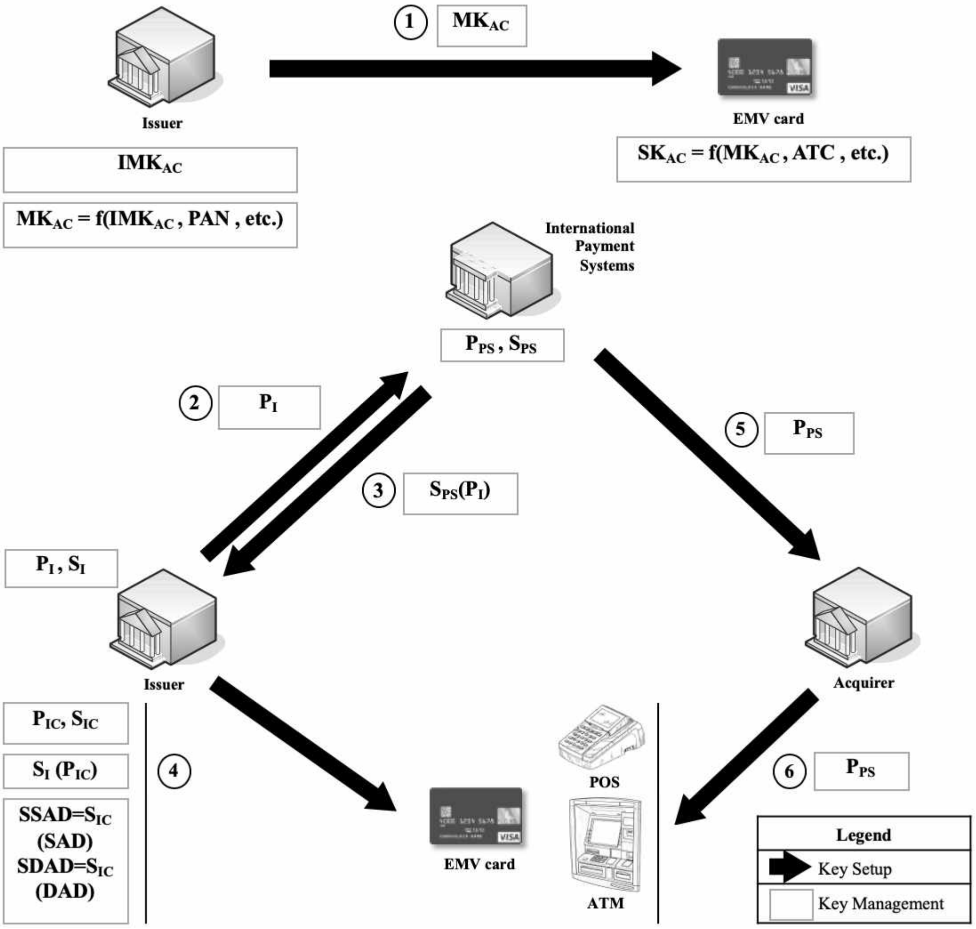


Figure 2.4: EMV Key Setup

2.2 EMV Chip Features

As mentioned in 2.1, EMV was created with the goal of significantly reduce the levels of card fraud [19, 20]. That is mainly achieved through the following security controls.

2.2.1 Application Cryptogram

The EMV Application Cryptogram (EMV AC) is generated using double-length[6] Triple-DES algorithm. The critical data elements in the card are used for the generation of the signature of any online authorisation request, Authorisation Request Cryptogram (ARQC), sent to the card issuer, or the Transaction Certificate (TC), which is the cryptogram generated in the final step of an EMV transaction confirming the payment approval for clearing and settlement. The EMV AC is used in the following procedures [20]:

- Messages between the card and the issuer;

[6] Two-key

- Online authentication of card and issuer;
- Authentication and integrity of transaction data elements.

As the card defines the transaction method to be performed, it only has to communicate to the terminal the results of its decision, generating one of three possible cryptograms:

1. **Authorisation Request Cryptogram (ARQC)**:
    - Request for online approval by the issuer;
2. **Transaction Certificate (TC)**:
    - Confirmation of an approved offline transaction;
3. **Application Authentication Cryptogram (AAC)**:
    - Transaction Declined.

Issuer performs the validation and sends back an authorisation response called Authorisation Response Cryptogram (commonly referred as ARPC), which allows the card to confirm the approval was received from the actual issuer host. After the authorisation process, any counters or offline limits may be reset.

In order to confirm the data elements are not altered, the recipient must validate the cryptograms.

2.2.2 Offline Data Authentication (ODA)

ODA is a security control that characterises an EMV card. ODA is a process by which the terminal authenticates the card, using asymmetric cryptography to confirm its authenticity. The card informs the terminal which methods it supports and the terminal chooses the "best"[7] method that both support. When ODA is not performed, the transaction must go online in order to be authorised.

There are essentially three ODA types:

- Static Data Authentication (SDA);
- Dynamic Data Authentication (DDA);
- Combined Data Authentication (CDA).

Using public key cryptography to perform payment data authentication ends the need for the transaction to go online to be authenticated by the issuer. This card capability increases the security of offline transactions by implementing an additional security layer to the offline authentication process that is performed by offline card acceptance terminals.

[7] The best method, in terms of security. From the less to the most: SDA-DDA-CDA.

For this purpose, terminals are "loaded" with P_{CA}[8] keys from payment schemes.

As mentioned, there are three main types of ODA:

1. **Static Data Authentication (SDA)**:

   SDA ensures the authenticity of the data on the card, but being this data, static, it doesn't ensure that a card is unique;

2. **Dynamic Data Authentication (DDA)**:

   On DDA, which is stronger than SDA, the terminal performs the same steps as in SDA. However, it also challenges the card to confirm the card is original and not a copy, using unique data for every transaction;

3. **Combined Data Authentication (CDA)**:

   CDA is based on DDA, but adds the generation of an EMV AC, followed by signature verification by the terminal. CDA is designed to prevent fraud by exploring an attack at the terminal in which the attacker uses a valid chip card for ODA and from then, for the rest of the transaction, he simulates card actions in order to obtain a valid authorisation.

2.2.3 Cardholder Verification Processing

In order to prove the rightful holder of the card, there are some verifications implemented by EMV, named Cardholder Verification Methods (CVM), as well as continuing to support the methods available in the magnetic stripe cards. CVMs are lists defined by the issuer in the chip card that provides flexibility and enforces the cardholder verification, specifying by priority the verification methods to be applied in particular acceptance conditions, and when supported by the terminal but providing an alternative when the preferred CVM is not supported. The EMV verification methods are:

- **Offline PIN**: The Personal Identification Number (PIN) is encrypted and verified online by the card issuer;

- **Offline Enciphered PIN**: Public key cryptography is used to protect the PIN as it is sent from the acceptance terminal to the card for verification. The result is returned to the terminal;

- **Offline Plaintext PIN**: Where the PIN is sent in clear text from the acceptance terminal to the card for verification. The card responds whether the PIN was correct or how many failed PIN attempts there are left before the card blocks;

[8] CA's Public Key

- **Signature**: where the cardholder signature on the receipt is compared to the signature on the back of the card;
- **No-CVM**: No CVM is performed (typically for low value transactions or for transactions at unattended POS).

The results from the Cardholder Verification can be:

- Cardholder verification was not successful;
- Unrecognised CVM;
- PIN try limit exceeded;
- PIN entry required and PIN pad not present or not working;
- PIN entry required, PIN pad present, but PIN was not entered;
- Online PIN entered.

2.2.4 Risk Management and Authorisation Controls

The risk management process is defined out of EMV scope. This means, that at the time of the card production, the transaction rules and limits are set by the issuer, as they may be changed during the card validation and consequent lifetime. These rules and limits may be, for example, the offline and below floor limit transactions, international operational functionality at many levels, and others, defined by the issuer. It may be depending of many factors, such as clients or card types, for example.

Many of these controls are dynamic and can be changed by the issuers through the EMV support for script commands, returning scripts to chips in online responses, setting new controls as card offline limits or even blocking chips, providing dynamic protection and risk management against use of lost and stolen or fraudulent cards. Yet, risk management is performed at the terminal side as well, as the payment system needs to be protected from fraud.

There is interest in doing online approval for transactions that are directly verified and authorised by issuers. In order to take the decision of going offline or online for a transaction, the terminal verifies three aspects:

- If the transaction is above the offline floor limit;
- Whether it pretends to randomly select this transaction to go online;
- Or, if the card has not had an online authorisation in a while.

2.3 EMV Chip Transaction

An EMV transaction, whether be it contact or contactless, consists in the interaction between the chip and the terminal, and the processing of information under certain predefined rules[9]. The EMV transaction is defined by the EMV Chip Specifications and is described below in a high-level perspective.

2.3.1 EMV Contact Chip Transaction

Figure 2.5 represents the official EMV processing steps for a contact chip transaction [20]. There are two actions that precede the Application Selection step which are important to refer to. Having both card and terminal EMV enabled, the first action, which can be named as the **Card Detection**, is performed by the card interface (the chip) directly on the chip card reader incorporated on the terminal. At this stage, the terminal establishes the electromagnetic contact between the two interfaces and starts the power supply to the card. The second action consists in the terminal resetting the card, and as a result the card responds with a sequence of bytes known as *Answer to Reset (ATR)*, in which the card specifies how the terminal must interact with it.

The EMV transaction can be divided into four steps:

1. **Initialisation**: Application selection, initialisation and reading of necessary data from the chip;

2. **Data Authentication (optional)**: Selection of data authentication method to be performed, which means SDA, DDA or CDA (described in Section 2.2.2);

3. **Cardholder Verification (optional)**: Selection, supported by the terminal and agreed by the chip, of the method for verify the cardholder (by PIN or Signature);

4. **Transaction Processing and Completion**: The transaction can be performed offline or online. The terminal chooses which authentication it wants to perform, but the card may refuse offline transactions and force the terminal to perform online transactions instead.

   One or two cryptograms are generated for each transaction: one for offline transactions, and two for online transactions:

   - In an offline transaction, the card sends a TC to the terminal as a proof of the performed transaction, that the terminal sends later to the issuer;
   - In an online transaction, the card sends an Authorisation Request Cryptogram (ARQC) to the issuer, which responds with an Authorisation Response Cryptogram to the card.

[9] Defined by the issuer

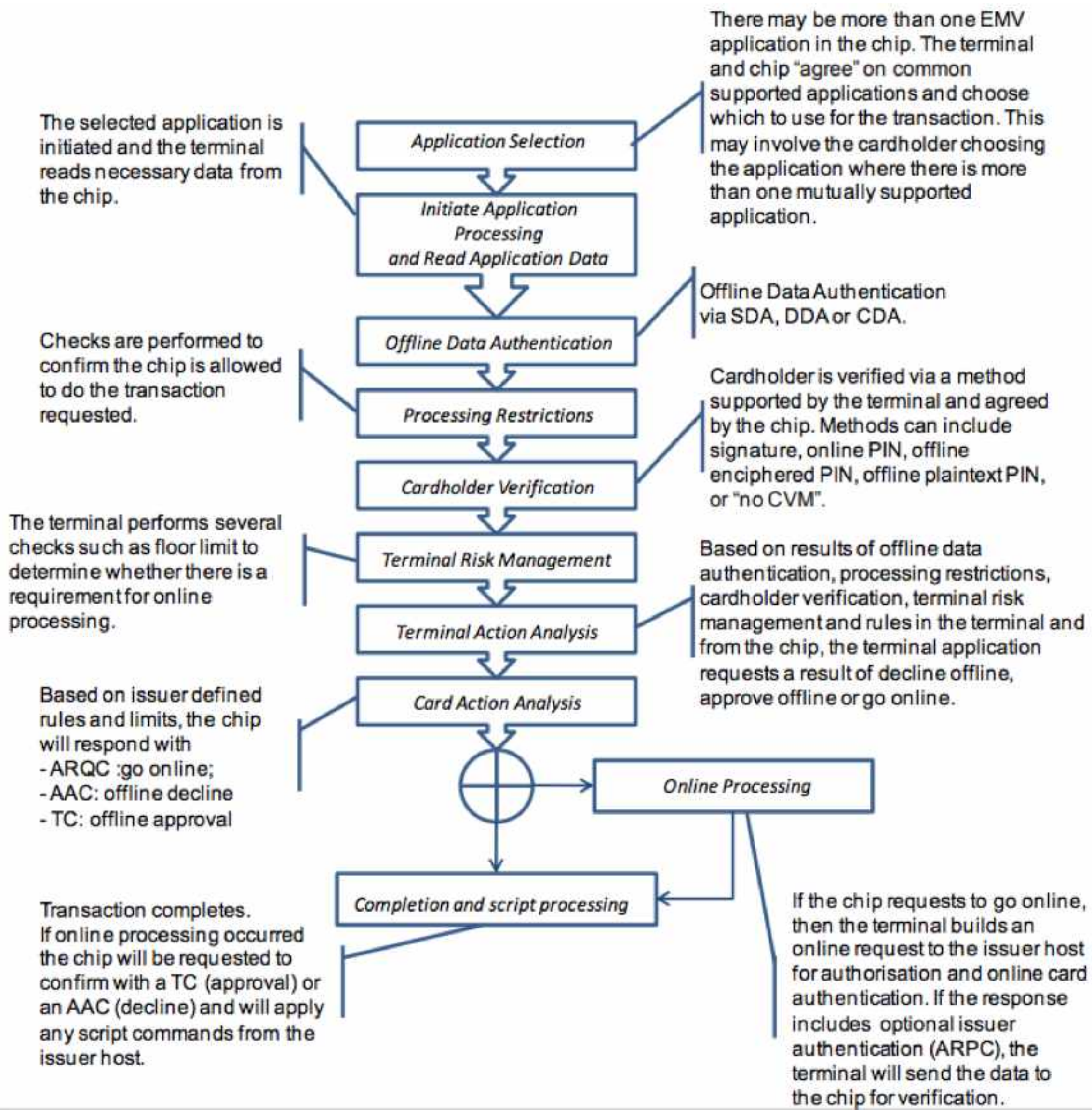

The selected application is initiated and the terminal reads necessary data from the chip.
Application Selection
There may be more than one EMV application in the chip. The terminal and chip "agree" on common supported applications and choose which to use for the transaction. This may involve the cardholder choosing the application where there is more than one mutually supported application.
Initiate Application Processing and Read Application Data
Offline Data Authentication
Offline Data Authentication via SDA, DDA or CDA.
Checks are performed to confirm the chip is allowed to do the transaction requested.
Processing Restrictions
Cardholder Verification
Cardholder is verified via a method supported by the terminal and agreed by the chip. Methods can include signature, online PIN, offline enciphered PIN, offline plaintext PIN, or "no CVM".
The terminal performs several checks such as floor limit to determine whether there is a requirement for online processing.
Terminal Risk Management
Terminal Action Analysis
Based on results of offline data authentication, processing restrictions, cardholder verification, terminal risk management and rules in the terminal and from the chip, the terminal application requests a result of decline offline, approve offline or go online.
Card Action Analysis
Based on issuer defined rules and limits, the chip will respond with
- ARQC :go online;
- AAC: offline decline
- TC: offline approval
Online Processing
Completion and script processing
Transaction completes. If online processing occurred the chip will be requested to confirm with a TC (approval) or an AAC (decline) and will apply any script commands from the issuer host.
If the chip requests to go online, then the terminal builds an online request to the issuer host for authorisation and online card authentication. If the response includes optional issuer authentication (ARPC), the terminal will send the data to the chip for verification.

Figure 2.5: Protocol Steps for an EMV Contact Transaction. Image from official EMV documentation [20]

In the case of refusing or abort the transaction, the card sends an AAC to the terminal instead of a TC or an ARQC.

2.3.2 EMV Contactless Chip Transaction

The EMV contactless chip transaction was designed with the goal of minimising the amount of time the chip must be within the proximity of the reader. The EMV contactless chip transaction is faster, with faster exchange of information between the chip and the terminal, and with the capability of performing some of the transaction steps after the chip has left the proximity of the reader (i.e., online authorisation). This results in a reduced amount of time the device must be held within the proximity of the reader.

Issuers are issuing EMV cards that support contact and/or contactless EMV transactions. Although providing specifications [21] for contactless EMV payments, they do not specify all functionality for payment application. Payment networks can implement contactless payments for EMV transactions to function in both offline and online transaction environments. The validation and authentication of the device are left to be performed by the EMV cryptogram verification, similar to contact EMV chip contact transactions.

International Payment Systems (IPS) have developed their own EMV contactless specifications [18]. The contactless development has occurred in a competitive direction, in opposite to the contact card environment, having each EMVCo member its own and different card scheme:

- Kernel 1 for Visa and JCB;
- Kernel 2 for MasterCard;
- Kernel 3 for Visa;
- Kernel 4 for American Express;
- Kernel 5 for JCB;
- Kernel 6 for Discover;
- Kernel 7 for UnionPay.

Although being similar to an EMV Contact transaction, there are some important differences between the two types of transactions [18]:

1. In order to support the older infrastructure that do not support the EMV transactions, the EMV contactless specifications specify a Mag-stripe mode;
2. Online contactless transactions usually involve only one cryptogram. In contact mode there are two cryptograms. This reduces the amount of time that the card has to be held close to the reader, being the cryptogram validation performed after the card has left the proximity of the reader;
3. The specifications for EMV contactless chip transactions has an additional CVM method called *Consumer Device CVM*. This method is used for identity verification of the cardholder when performing the contactless transaction with an NFC enabled device.

From a high-level perspective, the **EMV contactless transaction** has three main phases:

1. Contactless interaction between device and reader interaction:

   a) Verification of supported kernels by the reader, and kernel activation;

2. Terminal processing after card removal:
   a) Offline data authentication;
   b) Processing restrictions:
      i. Application version number checking;
      ii. Application utilisation control checking;
      iii. Effective/expiry dates checking;
   c) Terminal risk management (not performed in all kernels):
      i. Floor limit checking;
      ii. Other optional checks;
   d) Cardholder Verification;
3. Terminal decision:
   a) Approval;
   b) Decline (transaction may be reverted to contact);
   c) Go online.

In the next Chapter, HCE technology is presented as its architecture and models of contactless card emulation in mobile devices, taking advantage of NFC capabilities.

Chapter 3

Host Card Emulation

Host Card Emulation (HCE) is an architecture that provides virtual representation (e.g. emulation) of contactless cards[1], enabling transactional communication for mobile devices with NFC support without the need of SE hardware used in NFC payments prior to HCE, being the card emulation performed mainly by software.

Through the adoption of this technology, merchant terminals that accept contactless cards may accept payments from HCE devices[2] with no need to change the terminal software or hardware.

3.1 NFC and SE Technical Aspects

Based on RFID, NFC is a specification for contactless short-range communication [24]. NFC is standardised in ISO/IEC 18092 [25] and ISO/IEC 21481 [26] and incorporates ISO/IEC 14443 [27].

NFC uses magnetic field induction to enable communication between electronic devices up to a distance of 20 cm (but usually between 0 and 4 cm), limited to a 424 kilobits per second data transfer rate with no native encryption, and has three operation modes [28] represented in Figure 3.1:

1. **Read/Writer**:
   An active NFC device can read and write data from, or to, a tag or a smartcard[3];

2. **Peer-to-Peer (P2P)**:
   Two battery powered devices establish a bidirectional half duplex channel between them in order to exchange data;

3. **Card Emulation**:
   The NFC interface works as a smartcard based on industry's standard communica-

[1] Payment, loyalty and ticketing cards

[2] Devices HCE-enabled

[3] Data rate up to 106 Kbit/s

tion interfaces[4] (this enables smartcard emulation and has as its main advantage the compatibility with the existent smartcard industry).

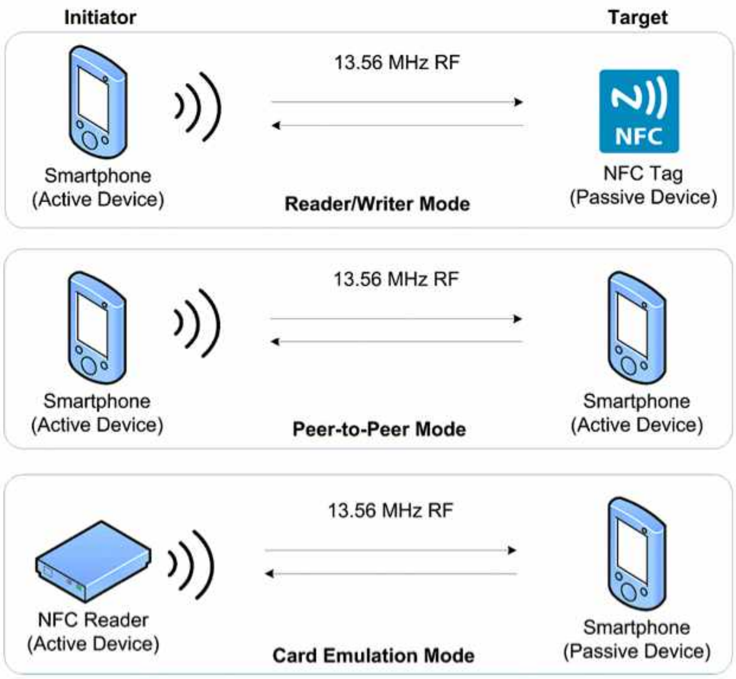


Figure 3.1: NFC Operating Modes and Interactions (image from [29])

Secure Element

The first practical implementations of NFC on mobile devices consisted on having a physical SE assembled on the device, functioning exactly as a smart card when in communication with an NFC reader [30]. Similar to a Subscriber Identity Module (SIM) card, an SE is a secure and tamper-resistant "System on Chip" (SoC) [31]. The NFC reader sends and receives Application Data Unit (APDU) commands to and from the application inside of the SE.

There are three forms of SE implementations on handsets [32]:

1. **UICC**[5]: Making use of the traditional SIM card to embed the SE;

2. **Embedded SE**: SE based on a hardware chip assembled on the device, independent of the SIM card;

3. **SD-card**: Using an application inside the SD card as an SE.

Each of these strategies of implementing an SE on a handset has advantages and disadvantages, depending on the participating party:

[4] ISO/IEC 14443 Type a, Type b and Felica

[5] Universal Integrated Circuit(s) Card

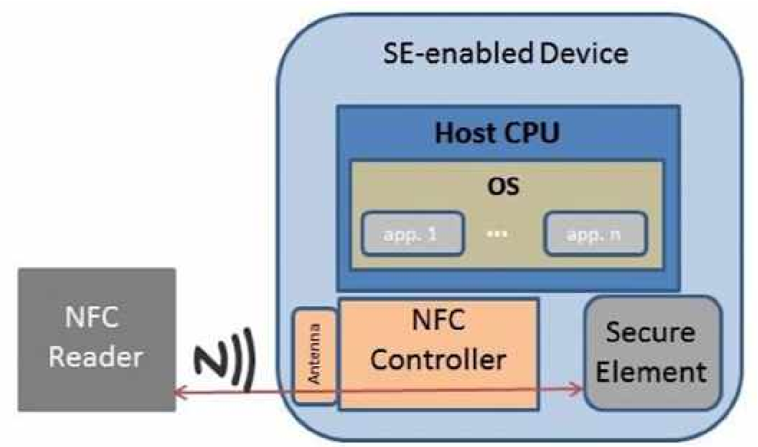


Figure 3.2: NFC Device with SE-based Card Emulation (image from [30])

- The UICC strategy was most favoured by the Mobile Network Operators (MNO) given that this would give them the opportunity to supply these critical personalisation services in the payment's arena. The advantages of this strategy were the speed of coverage of handsets that could be obtained given that all handsets have a SIM slot, and substituting SIMs with these added features or personalising them over-the-air could be achieved at a low cost and reasonably quickly. Difficulties are related to the security of card's critical data, being provided by Issuers to MNOs;
- The Embedded SE was favoured by the handset manufacturers, however, the time necessary to migrate all users from older handsets to new handsets supporting the integrated SE was a burdensome challenge;
- The SD-card implementation was strongly limited because handsets had to support SD-card readers and because of its provisioning, done practically by only one Service Provider (SP)[6] for each SD-card, which does not allow a user to use emulated cards from multiple SP's in the same SD-card. Additionally, the NFC capable SD-cards[7] in some handsets were placed in locations where RF signals were suppressed by metallic enclosures.

Given the problems described for these three strategies, the concept of HCE emerged.

3.2 History of Host Card Emulation

In 2011, Blackberry launched Virtual Target Emulation (VTE) [33] technology in Blackberry OS 7[8] and kept it through Blackberry OS version 10 [34]. Despite of the different

[6] Bank or financial entity

[7] For handset devices without NFC antenna

[8] The Blackberry Bold 9900 series came with the Java SDK 7.1 which included a API for Card Emulation

acronym, VTE represents the same technology as HCE. With this capability, the NFC readers on the Blackberry mobile devices routed the messages from the POS directly to an app through the Operating System, to be interpreted and responded by the app itself. This is the opposite to the previous architecture based on a SE physically assembled on the mobile device, previously selected by the terminal through the Application Identifier.

In 2012, the start-up SimplyTapp allegedly created HCE[9], adding a patch to the Android customized version called CyanogenMod [35], discontinued in 2015 and rebranded as LineageOS [36] after a fork that took place in 2016. In 2013, at a Mobey Forum's member meeting, Bankinter [37] publicly introduced its own solution, which raised interest among the other attending banks.

Later on, in late 2013 [32], Google launched the Android version 4.4.1, under the name "KitKat". This version introduced the Android support for the recent NFC feature called "Host Card Emulation" that allowed the smartphone to emulate a chip card by software without the need of a hardware SE (see Figure 3.3).

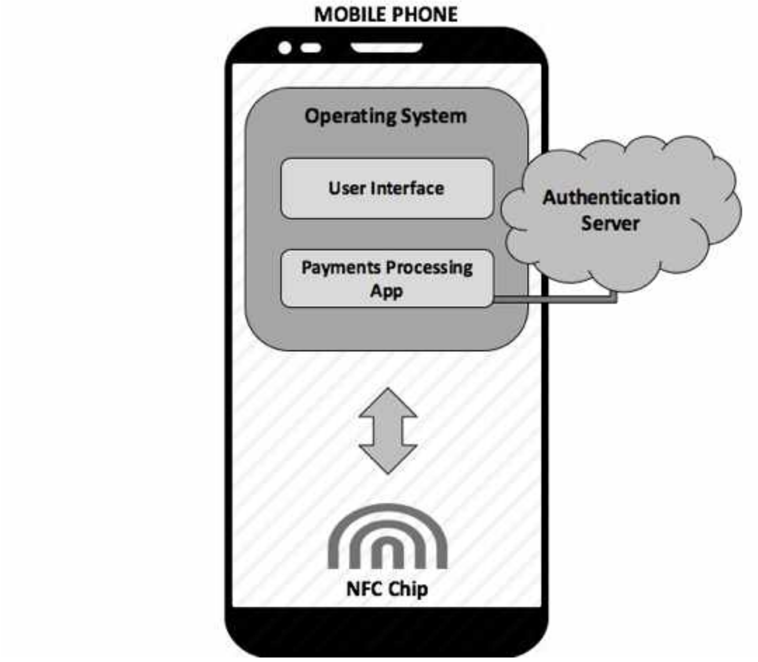


Figure 3.3: HCE - Implementation on a Mobile Device (modified from the original figure from [38])

During 2013, Android 4.4.1 KitKat and Blackberry 10 were the only [38] Operating Systems offering HCE support, plus CyanogenMod, as mentioned. At that time, 500 million NFC-enabled handsets were estimated [32] to be in the market. While every version of Android supports HCE since then, Blackberry recently adopted Android as the OS for its smartphones. Since early 2014, Google Wallet can only be used on smartphones

[9] General Architecture as VTE, but called Host Card Emulation

with NFC support. At that time, Apple used a different approach for NFC payments, that was a unique implementation [39] of a physical embedded-SE, which is currently exclusive for its Apple Pay [40] service.

VISA and MasterCard also embraced HCE [30]. In 2014, and in order to enhance its contactless payment application, PayWave, VISA started to support HCE-based mobile payment services, by introducing a new standard called ”VISA Cloud-Based Payments”[10], which is a set of specifications and requirements. Shortly after, MasterCard also introduced its own standard[11] for Cloud-Based Payments, with the collaboration from the banks Capital One and Bank Sabadell.

3.3 Host Card Emulation Models

In the HCE ecosystem, a card can be emulated in two different ways:

1. **Cloud-Based HCE** - a remote machine (i.e. Cloud Server) in communication with the NFC-enabled mobile device;

2. **HCE with Tokenisation** - Directly on the NFC-enabled mobile device to be presented to the acceptance terminal.

Hence two models for implementing HCE were adopted and are described in the following two sections.

3.3.1 Cloud-Based HCE

With the card emulation being performed in the Cloud and both payment credentials and flow logic residing in a remote server, this is considered a full Cloud HCE architecture.

In this case, the app communicates with the cloud system authenticating the user and providing user interface, and then the transactional processing is done through APDU commands sent and received through a secure connection and passed to and from the NFC controller of the acceptance device. For each transaction, the server has to access to card data (keys and other data) for generating the cryptogram (see Section 2.2.1) to send to the app.

In comparison to the SE architecture, this architecture (Figure 3.4) is based on the emulation of the SE data and its behaviour on a remote server.

While not having any credentials stored in the device enhances security, there are challenges to consider, like the hardening of the remote server and the communication channel, as well as the need for ”going always online” combined with the possible latency of network communications, depending on the MNO service availability.

[10] VISA’s confidential documentation

[11] MasterCard confidential documentation

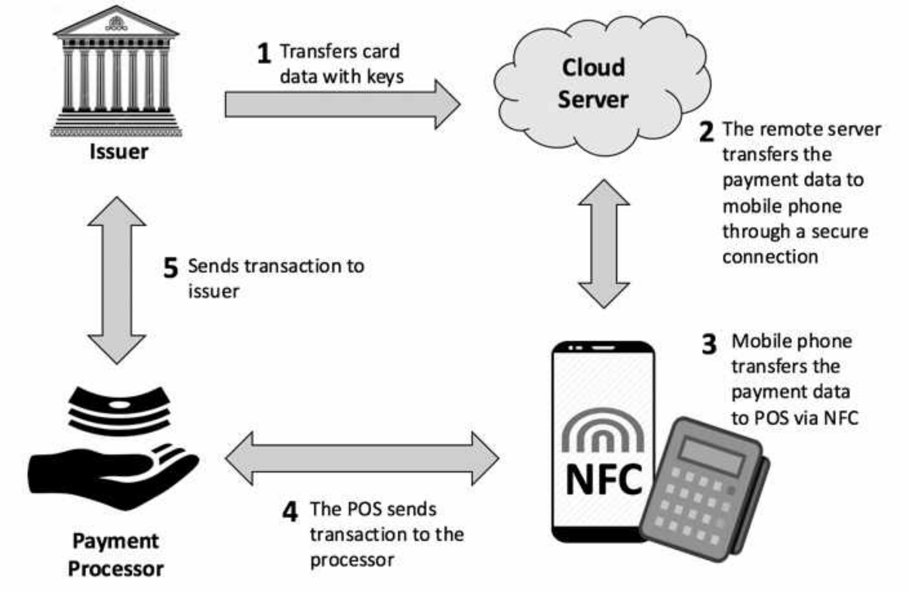

1 Transfers card data with keys
Cloud Server
Issuer
2 The remote server transfers the payment data to mobile phone through a secure connection
5 Sends transaction to issuer
3 Mobile phone transfers the payment data to POS via NFC
NFC
4 The POS sends transaction to the processor
Payment Processor

Figure 3.4: Cloud-Based HCE - Transaction Flow (modified from the original figure in [38])

3.3.2 Host Card Emulation with Tokenisation

In this HCE model, instead of having the card emulation being performed by a remote server (see Section 3.3.1), the application performs the card emulation in its entirety. It stores the keys needed to generate the EMV AC, mandatory to perform an EMV transaction. These keys are not the actual card keys stored in the UICC of the physical cards. They are cryptographic keys and tokens with which the EMV AC can be generated as if it was a physical card and so the terminal will recognise them as such[12].

Token

A token is a surrogate or alternative value that replaces the PAN[13] in the payment ecosystem. Its characteristics may vary such as format, utilisation and applicability[14]. In order to be processed by the systems without modifications it should have the structure and abide to the same rules that a PAN has.

Tokenisation

The process of replacing the PAN by a token for a specific or limited replacement of card data.

[12] Before terminal decision, these tokens will be validated (offline by the terminal or online by the issuer) and the acceptance of the transaction will depend of this validation

[13] In practice, it refers to the card number

[14] For instance, for an Issuer Tokenisation, the token domains can be the channel, the merchant, or a specific digital wallet

The *EMV Payment Tokenisation Specification* [41], published in 2014, established standardisation and worldwide interoperability for all stakeholders by providing detailed description of Payment Tokenisation ecosystem and its key roles, token issuance, provisioning, processing during a transaction, and required and optional data for related transaction flows, among other technical aspects and requirements. For specific security requirements, PCI SSC[15] has published dedicated specifications and guidelines [42, 43].

HCE with Tokenisation (represented in Figure 3.5) introduced innovative capabilities to NFC payments allowing the use of multiple emulated cards per device, and the capability of performing offline transactions due to the in-app generated EMV AC. Online communication through an MNO is only requested when the tokens need to be replaced (e.g. expiration) or when the implementation only performs or accepts online transactions.

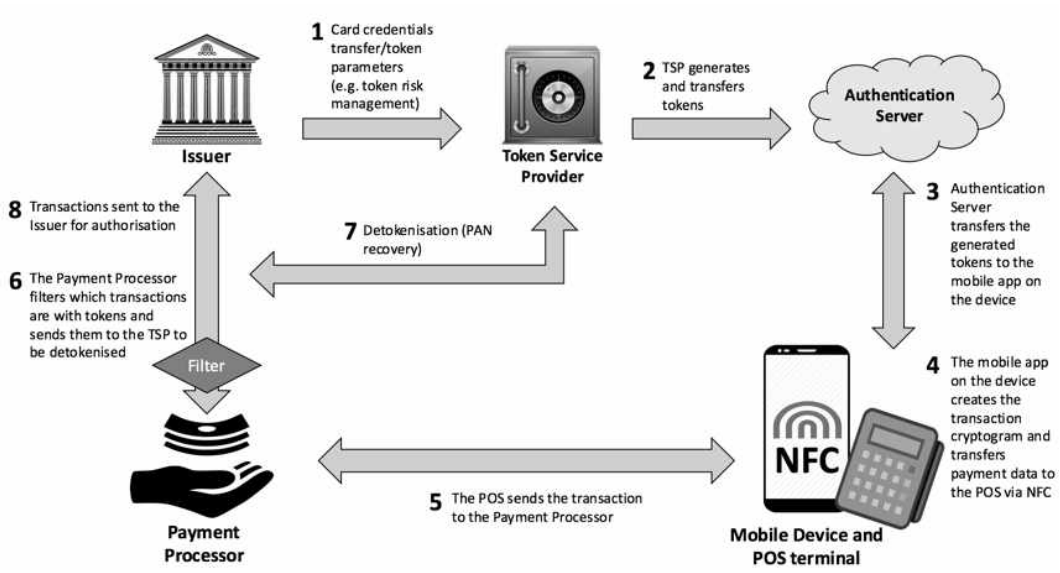

Issuer
1 Card credentials transfer/token parameters (e.g. token risk management)
Token Service Provider
2 TSP generates and transfers tokens
Authentication Server
3 Authentication Server transfers the generated tokens to the mobile app on the device
8 Transactions sent to the Issuer for authorisation
7 Detokenisation (PAN recovery)
6 The Payment Processor filters which transactions are with tokens and sends them to the TSP to be detokenised
Filter
4 The mobile app on the device creates the transaction cryptogram and transfers payment data to the POS via NFC
NFC
5 The POS sends the transaction to the Payment Processor
Payment Processor
Mobile Device and POS terminal

Figure 3.5: HCE with Tokenisation - Transaction Flow (image modified from the original in [38])

The HCEt ecosystem is composed of the following components:

- **Mobile Application and POS terminal**:
  - Mobile app that communicates with an acceptance device (e.g. POS terminal) through APDU commands and has tokens stored for generating EMV ACs. Also communicates with the Token Service Provider for token provisioning and authenticates the user to the remote system of the mobile app provider;

[15] `https://www.pcisecuritystandards.org`

  - The POS terminal is the acceptance device that establishes communication with the mobile device in order to perform the transactions generated in the mobile app;

- **Token Service Provider (TSP)**: Responsible for token management, namely, token issuance, provisioning and detokenisation;

- **Payment Processor**: A card network entity (e.g. VISA, MasterCard), a processor (e.g. SIBS), or another payment processing provider. The transaction data is sent to the POS via NFC and the Payment Processor verifies[16] the token-based payment and sends it to the TSP to be detokenised[17] before sending it on to the issuer to authorise the transaction. Optionally the issuer may request the detokenisation instead of the Payment Processor;

- **Issuer**: The issuer's system that accepts or denies the transaction.

The next chapter will focus on the the structure and methodology of the Risk Assessment presented in Chapter 6, which is based on the aspects studied and presented about the EMV cards and HCEt architecture in this dissertation.

[16] Whether it is a token-based transaction or not

[17] To return to the original PAN Value

Chapter 4

Risk Assessment Methodology

A Risk Assessment identifies assets, applicable threats, vulnerabilities, existing controls and evidences which lead to the determination and comprehension of the inherent risks. The main factors that contribute for their existence are identified and ranked according to the risk evaluation criteria, namely the likelihood and impact, and therefore the results contribute to:

- The identification and implementation of adequate treatment and/or acceptance actions;
- Give support to the establishment of priorities;
- A better and more accurate decision-making.

The methodology for the Risk Assessment performed to the HCEt architecture and presented in this study in the next Chapter, is aligned with the ISO/IEC 27005 [44], the international standard for the information security risk management process.

The study performed is restricted to the Risk Assessment process presented in Figure 4.1. No Risk Treatment was performed since the study is not applied to a specific implementation and/or design. It represents an assessment of the general risks that may be considered before the implementation or design of an HCEt solution, and during its life cycle.

The assessment describes the applicable threats and vulnerabilities for the identified assets and subsequently the risk for these threats in order to classify the related impact and likelihood of each one, considering the existing controls. The derived risks are prioritised and ranked according to the evaluation criteria (defined in Section 4.2.3).

4.1 Context Establishment

As the first step in the information security risk management process, the context establishment consists in the statement of the purpose and the identification and delimitation

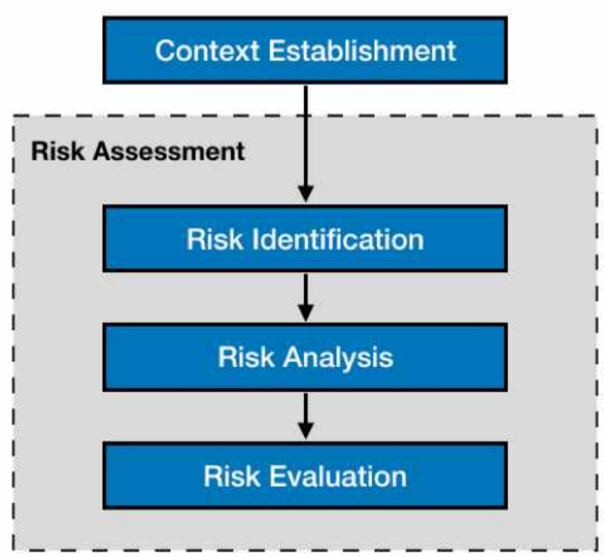


Figure 4.1: ISO/IEC 27005 (2018) Risk Assessment Process [44]

of scope and boundaries of the assessment. This is established in Section 6.1.

4.2 Risk Assessment

The Risk Assessment process is composed of sub-processes that consist specifically in the Identification, Analysis, and Evaluation of the risks that the model is subject to.

4.2.1 Risk Identification

This process is applied to discover, list and characterise elements of risk. The Risk Identification is intended to determine what risks exist or are expected within the defined context, what their characteristics are, their duration and consequences.

The Risk Identification is composed of the following steps:

1. **Identification of Assets**:

   Something that has value and thus requires protection. Assets can be tangible or intangible;

2. **Identification of Threats**:

   Threats represent circumstances with potential to adversely impact organisational assets, be they operational, financial, human, or others;

3. **Identification of Existing Controls**:

   Existing or planned controls to address previously identified risks or to avoid unnecessary work or cost in duplication of controls. Existing controls are evaluated as to their effectiveness;

4. **Identification of Vulnerabilities**:

   Existent design weaknesses, or implementation errors that can lead to an unexpected/undesirable event compromising the security of a system, network, application, or protocol [45].

4.2.2 Risk Analysis

Risk Analysis determines the likelihood of an undesirable event and its impact on an asset, identifying the incident scenarios. Impact can be of various types and the likelihood of occurrence of an event can be influenced by factors that should be considered:

- **Impact:** The magnitude of harm expected to result from the consequences of threat occurring. The impacts can be of several types, namely:
  - Financial;
  - Legal and Regulatory;
  - Operational;
  - Reputational.
- **Likelihood:** Probability that a threat event will occur. Multiple factors may contribute to the likelihood of an identified threat, such as:
  - Exploitable vulnerabilities;
  - Existing controls (and their effectiveness);
  - Motivations (fanaticism, financial gain, ego, espionage, revenge, terrorism, etc.);
  - Experience and applicable statistics;
  - Risk of being detected and persecuted;
  - The necessary effort to initiate an attack;
  - The benefits of a successful attack;
  - The potential number of attackers.

Table 4.1: Matrix for Risk Determination

Impact	Very High	5	5	10	15	20	25
	High	4	4	8	12	16	20
	Medium	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Very Low	1	1	2	3	4	5
Risk Determination			1	2	3	4	5
			Very Low	Low	Medium	High	Very High
			Likelihood				

4.2.3 Risk Evaluation

Based on the assigned values for Impact and Likelihood in the Risk Analysis process, the risk level for each threat is determined by calculating the *Product* of the two factors. It is assigned a value between 1 and 5 for both classification variables, resulting in a matrix of values as can be seen in Table 4.1.

In order to obtain a consolidate risk evaluation, all risks are prioritised from the highest to the lowest and summarised in a table as follows (Table 4.2 as an example):

Table 4.2: Example of a Representation for Consolidated Risk Evaluation

Threat ID	**Name**	**Likelihood (L)**	**Impact (I)**	**Risk Level (L x I)**
T1	Name1	5	5	25
T2	Name2	4	4	16
T3	Name3	3	3	9
T4	Name4	2	2	4
T5	Name5	1	1	1

This chapter described the methodology followed to perform the risk assessment on HCEt, which is presented on Chapter 6. As already mentioned in ”Chapter 1: Introduction to the Study”, one important fact of this assessment is that the Risk Analysis was performed through a survey conducted to IT and Information Security specialists. This survey is presented in the following ”Chapter 5: Conducted Survey for Host Card Emulation with Tokenisation Risk Analysis”.

Chapter 5

Conducted Survey for Host Card Emulation with Tokenisation Risk Analysis

As stated at the beginning of this dissertation in Section 1.4, the objective is to measure the risk inherent to the HCEt architecture, through a risk assessment.

After studying the available scientific documentation, it was clearly found that the lack of documentation to be able to analyse and carry out a duly supported risk analysis together with the fact that the subject matter was very specific and relatively recent, would be concrete obstacles to the execution of the study. In these cases, where documentation is scarce, the best way of assessing an opinion or reality is through an inquiry [46], and as such, it was decided to classify the risk based on the opinion of IT specialists and Information Security specialists.

An online survey [47] was conducted to measure the risk levels to the threats of HCEt model, based on a recent risk analysis on mobile financial services (study conducted by Mobey Forum[1]). This study identifies the various threats inherent to this type of mobile applications, also applicable to the HCEt model, given that it is a specific form of a mobile financial service. The survey can be found in Annex II.

5.1 Methodology, Preparation and Execution

The survey, which is based on the best practices described in the documentation consulted [48], was conducted on the Google Forms[2] online platform from the 21st August 2018 to the 30th September 2018, and respondents were invited by email (Annex I) to respond. A

[1] `https://www.mobeyforum.org`

[2] `https://www.google.com/forms/about`

document with the presentation and description of the HCEt architecture was added to the survey, as well as the description of the inherent threats.

The survey, consisting of 34 questions, has the following four parts structure:

1. **Personal and Professional (questions 1 to 6)**:

   Although the survey was anonymous, responses were collected on personal and professional indicators of the respondents, such as their age span, nationality, current profession and years of experience in IT and/or Information Security. The questions were asked in order to profile the response tendencies according to the characteristics of the respondents.

2. **User Background, Experience and Trust in the Security of Smartphones, Financial Applications and HCE (questions 7 to 21)**:

   This group of questions sought to establish levels of experience and knowledge regarding mobile Operating Systems (OS), mobile financial services applications in general and mobile card emulation solutions in particular. Respondents were also asked to compare the safety of contactless cards with respect to HCE solutions, and whether in the past they had any security incidents related to these technologies.

3. **Risk Classification for HCEt Threats (questions 22 to 32)**:

   This group of questions is the core of the survey and it seeks to meet its objective, which is the classification of risk by the respondents, taking into account the analysis of the threats to the HCEt. For each threat, it was requested to classify them on impact and likelihood by assigning integer values from 1 to 5 for each of the two variables. As support to this classification, each threat was accompanied by a description and documentation on HCEt, as set out in Annex II, as already mentioned.

4. **Suggestions for Improvement (questions 33 to 34)**:

   At the end of the survey respondents were asked, in questions of free response, to indicate whether they considered that there were other threats to the HCEt architecture beyond those already presented for classification. If so, they were asked to describe and classify them as to their likelihood and impact (just as the rest). It was also requested the respondents make suggestions they would consider relevant for the improvement of the study in progress.

5.2 Characterisation of the Reporting Population

Taking into account the technical specificity of the subject under analysis and the result of this dissertation being a risk assessment, the target public would have to be restricted to the technical areas related to HCEt, i.e. IT and Information Security, preferably with professional experience in financial solutions or related to bank cards.

The population of this survey corresponds to 32 respondents. Initially, a number of respondents were expected to be between 20 and 25 given the special nature of the theme and the difficulty in reaching the target audience. Given the heterogeneity of positions among the respondents (although they were all or specialists in Information Security or IT professionals), it was necessary to group together (see Figure 5.1) the different positions/professions in order to categories the respondents by professional profile, creating groups of professional profiles.

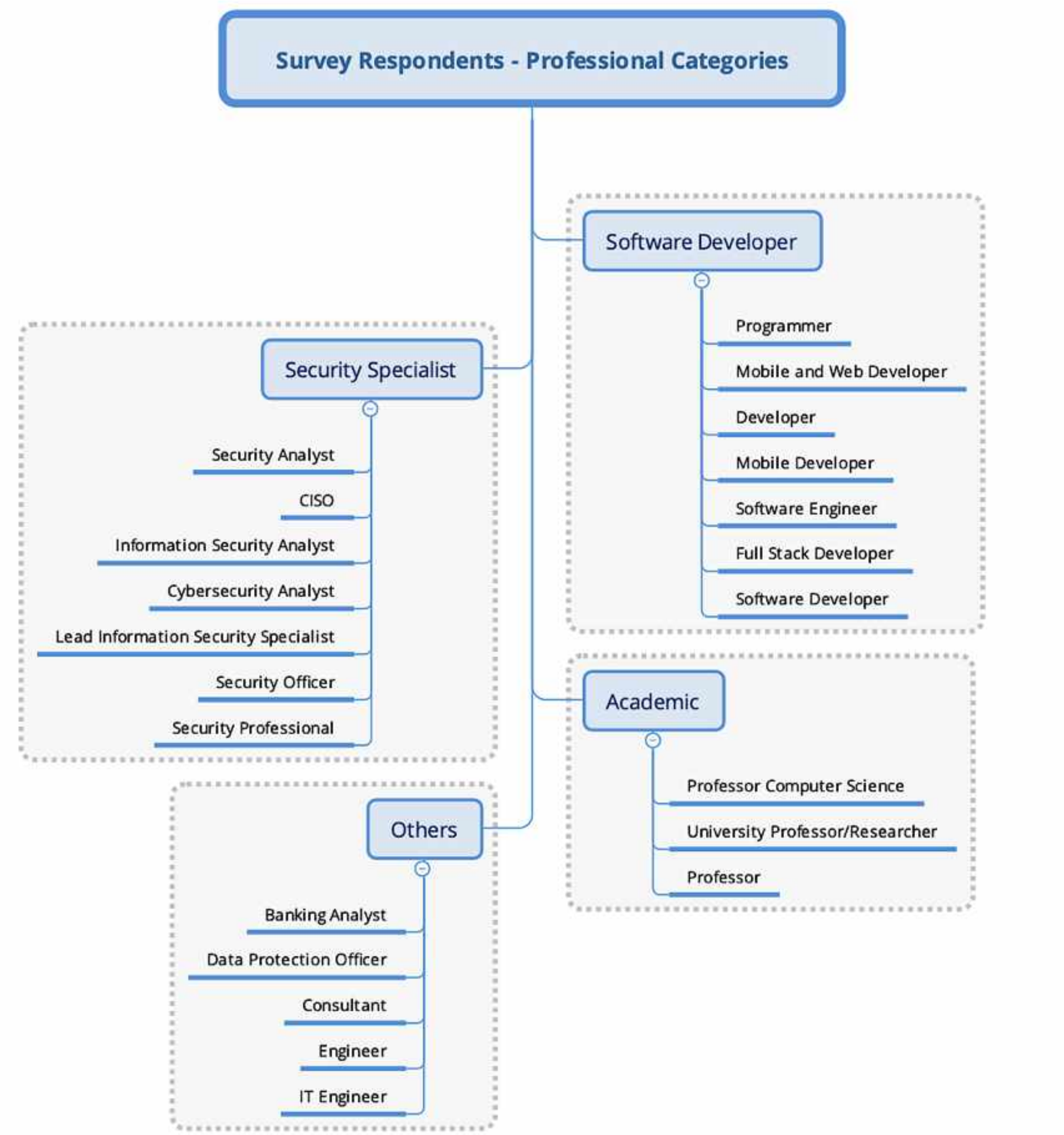


Figure 5.1: Professional Categories of Survey Respondents

Through the analysis of the similarities between professions the following categories were identified:

- Software Developer;
- Security Specialist;
- Academic;
- Others (what does not fit into the rest).

5.2.1 Residence and Age Distribution of Respondents

Responses were obtained from, approximately, 84% residents in Portugal and 16% from other countries as can be seen in Figure 5.2.

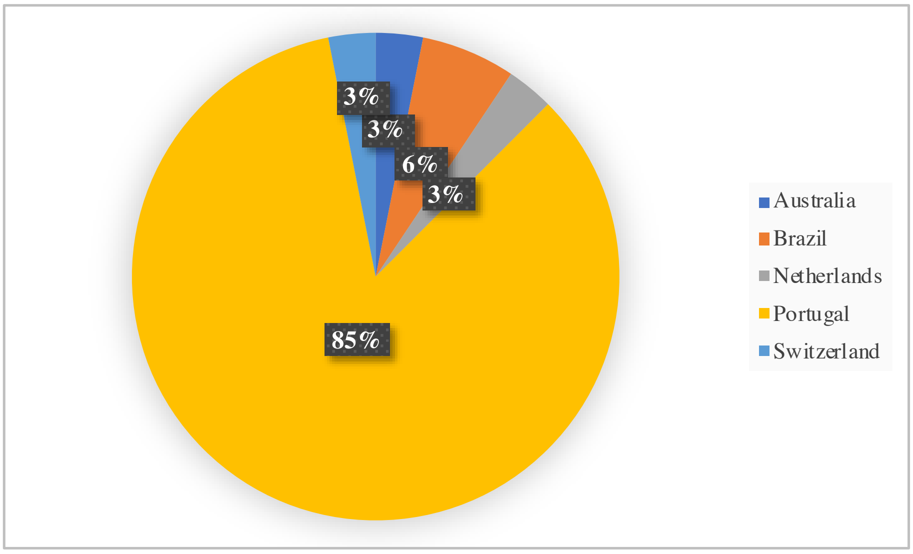


Figure 5.2: Percentage of Respondents by Country Where Living

Regarding the age of the respondents, the distribution was quite uniform (Figure 5.3), with the prevalence of the "21-30 years" and "41-50 years" age groups, and there were no respondents Under 20 years and Over 60 years. This fact can be justified by the target audience targeting experienced professionals, which is difficult to combine with the "Under 20 years" age group. On the other hand, "Over 60 years" includes the retirement age and increases the distance to the recent technology under study.

5.2.2 Experience by Professional Area

Among respondents in the areas of IT and Information Security, positions were grouped into 4 groups (see Section 5.2). Respondents were asked about their professional experi-

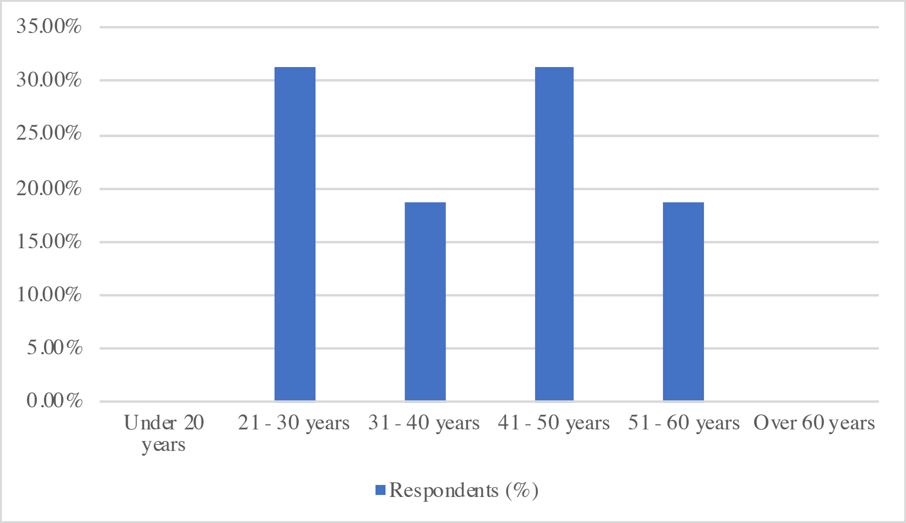


Figure 5.3: Percentage of Respondents by Age Span

ence, and the distribution (Years of Experience) can be consulted in Figure 5.4 and Figure 5.5.

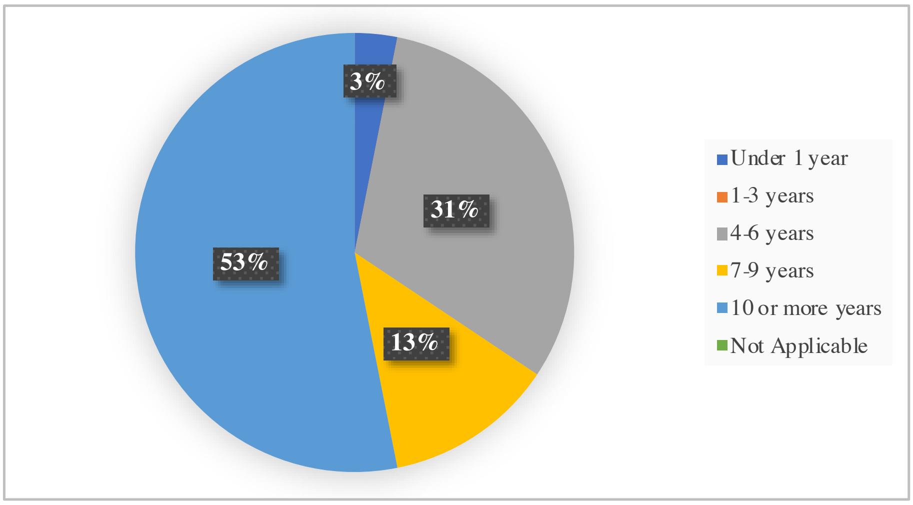


Figure 5.4: Percentage of Respondents with Experience in IT by Number of Years

Most respondents have ”10 years or more” of IT experience (Figure 5.4). Given that 66% of respondents have at least 7 years of experience and only 3% have less than 4 years of experience, this is an indicator that represents the good level of IT experience on the part of the respondents.

By analysing Figure 5.5, it can be concluded that only 19% of the entire sample has no experience in Information Security, which is an excellent indicator taking into account the purpose of the survey. In addition, 34% of respondents have been in Information Security for “10 years or more”, representing 51.5% of all respondents with Information Security

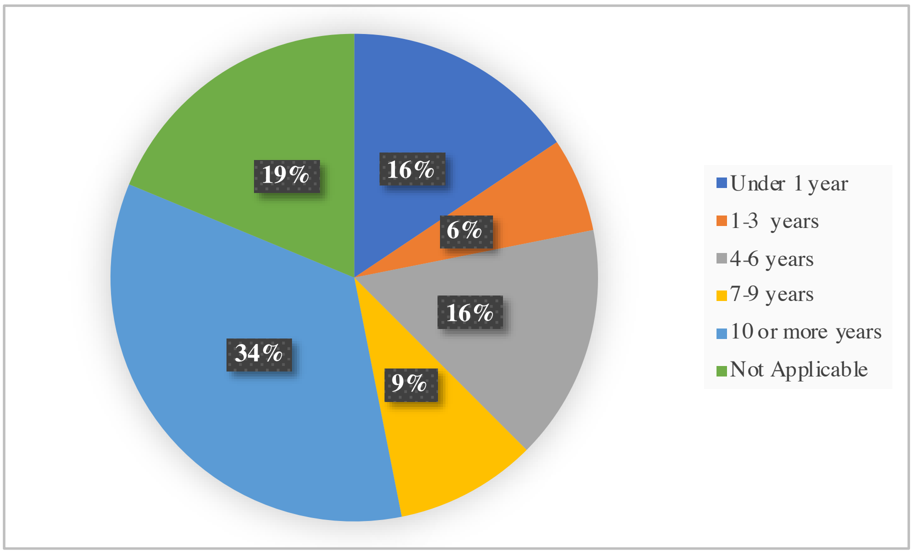


Figure 5.5: Percentage of Respondents with Experience in Information Security by Number of Years

experience, which indicates a high level of experience in this area.

5.3 Analysis of the Results

As mentioned in Section 5.1, the questions are grouped by themes, from the experience of the respondents on different technologies to their opinion on the classification of the risk for the different threats to the HCEt model. The results of the answers to these questions are presented and analysed below, seeking, whenever possible, to draw enriching conclusions from them.

5.3.1 Experience with Mobile Operating Systems, Smartphones, Mobile Financial Services, Host Card Emulation, and the Trust in their Security

One of the groups of questions (see Section 5.1) performed aimed to define the respondents experience, knowledge and trust in Smartphones, Mobile Financial Services (MFS) and HCE. Based on their answers, it is possible to measure the most popular mobile operating systems and compare the respondents' confidence in the security of these technologies.

Experience regarding Mobile Operating Systems

The assessment of respondents' experience regarding mobile operating systems is an indicator of the level of expertise for risk classification on HCEt threats. Respondents were asked about their experience with the most popular and used mobile operating systems, and the results can be seen in Table 5.1.

Table 5.1: Respondents Experience with Mobile Operating Systems

Operating System	% of Respondents with Experience (NRE / Total Respondents)
Android	93,75%
Blackberry OS	1,09%
iOS	43,75%
Windows Phone	21,87%
Others[3] : Symbian	0,31%

Android is the operating system that respondents have more experience with, having been selected in more than 93% of the answers. Nearly half (43,75%) of respondents reported having experience with the iOS operating system and nearly a fifth with Windows Phone. The percentage of respondents' experience of the Blackberry OS and Symbian operating systems is practically insignificant, although they're older operating systems than the rest and 47% of respondents have 10 or more years of experience with Smartphones (see Figure 5.6).

Experience with Smartphones and Confidence Level in its Security by Default

Analysing the number of years of smartphone usage, as can be seen in Figure 5.6, almost half (47%) of the respondents said to have "10 or more years" of smartphone usage, having only 6% of the respondents less than four years. It can be also seen as a representation of 94% of the respondents with 4+ years of smartphone usage and 75% for 7+ years.

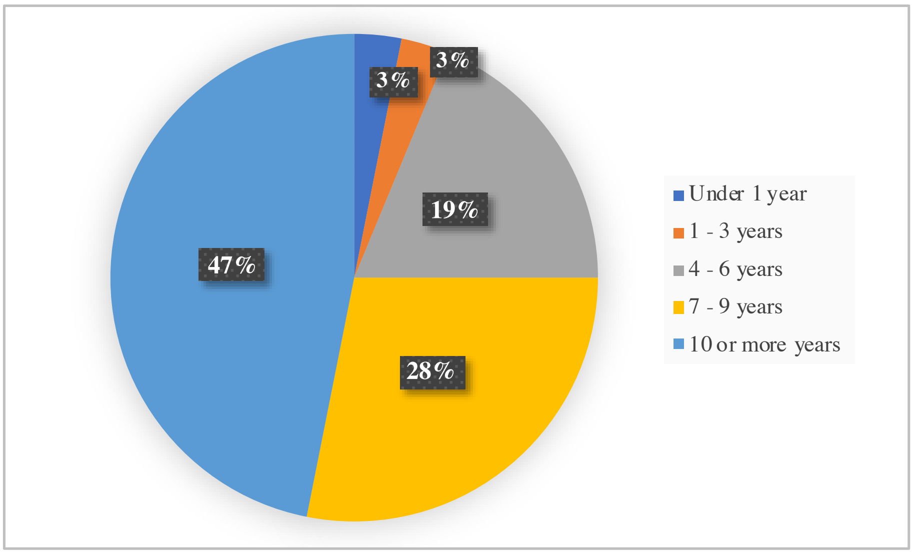


Figure 5.6: Percentage of Respondents by Years of Smartphone Usage

By analysing the number of years of use of smartphones by respondents (Figure 5.6), it shows that there are two major age groups: less than 10 years of use (53%) and 10 or more years of use (47%). It is possible to conclude that the years of smartphone usage were not an influential factor in their classification of confidence in respect to their security, as can be seen in Figure 5.7.

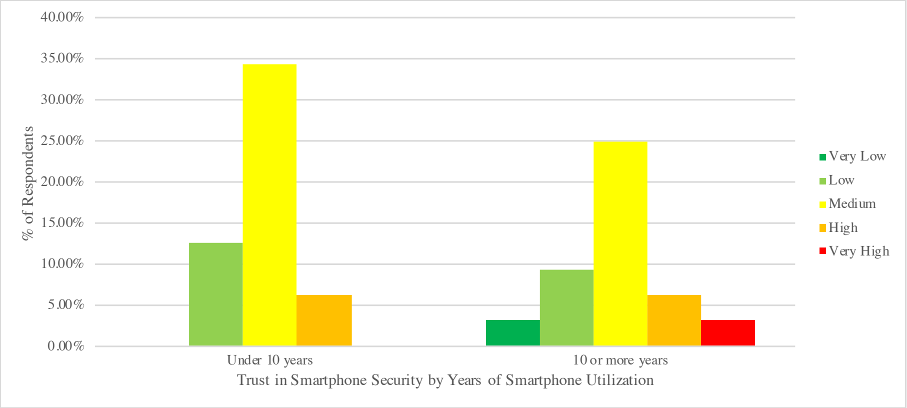


Figure 5.7: Trust in Smartphone Security by Years of Smartphone Usage

Despite the grouping of age groups, the classification as ”Medium” by of the majority (59.38%) of the respondents regarding the classification of their confidence on the safety of smartphones in general, is very clear.

5.3.2 Use of Mobile Financial Applications and Mobile Card Emulation Applications, and Confidence Levels in their Security

In this section the results for the questions addressed exclusively about MFA and Mobile Card Emulation Applications are presented. These questions sought to determine the experience of the respondents with these applications and the trust in their security.

Mobile Financial Applications (MFA)

With regard to the number of years of usage of MFA, the results (Table 5.2) are fairly distributed. Although the most chosen response (mode) by the respondents was ”1-3 years”, there was an almost equal distribution by ”Never Used”, ”1-3 years” and ”4-6 years”.

It can be concluded that the majority of respondents have experience with MFA (75%) and 40,63% have at least 4 years of experience.

When questioned about their experience with MFA (Figure 5.8), the majority of respondents using these applications (75% of the total sample) have reported using 2 to 3, representing 58% of respondents.

Table 5.2: Percentage of Respondents by Years of Usage of Mobile Financial Applications

Number of Years	**Respondents (%)**
Never used	25,00%
Under 1 year	6,25%
1-3 years	28,13%
4-6 years	25,00%
7-9 years	9,38%
10 or more years	6,25%

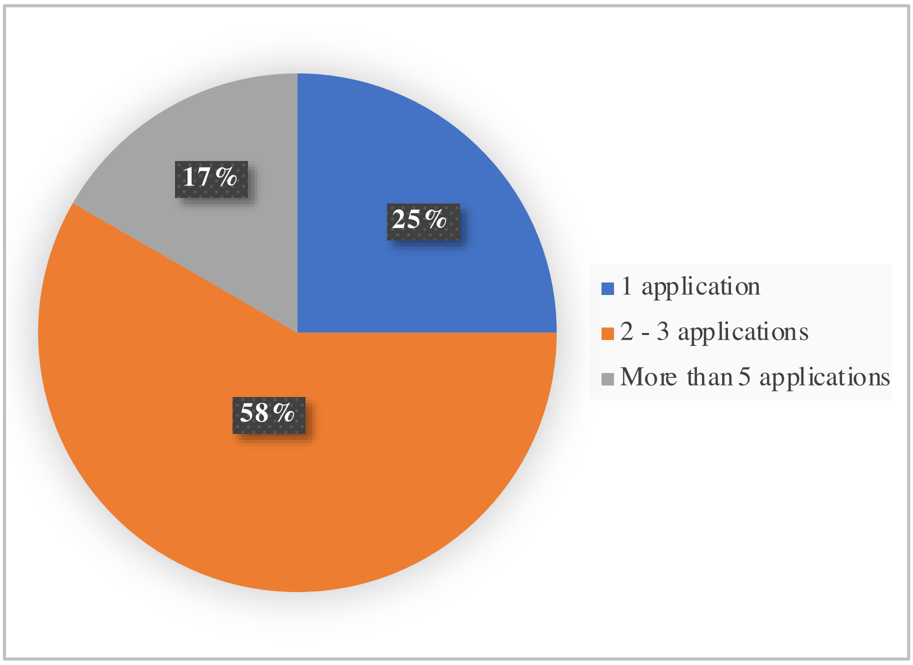


Figure 5.8: Percentage of Mobile Financial Applications Used by Responders

Mobile Card Emulation Applications

According to the results obtained and as shown in Table 5.3, the majority (65,21%) of the respondents are users of Mobile Card Emulation Applications.

Table 5.3: Percentage of Respondents Using Mobile Card Emulation Applications

User of Mobile Card Emulation Applications?	Respondents (%)
Yes	65,21%
No	34,79%

Regarding the percentage of respondents using of Mobile Card Emulation Applications, it is possible to verify (see Figure 5.9) that the majority of those respondents (that are users of this type of applications) are not using them for more than three years.

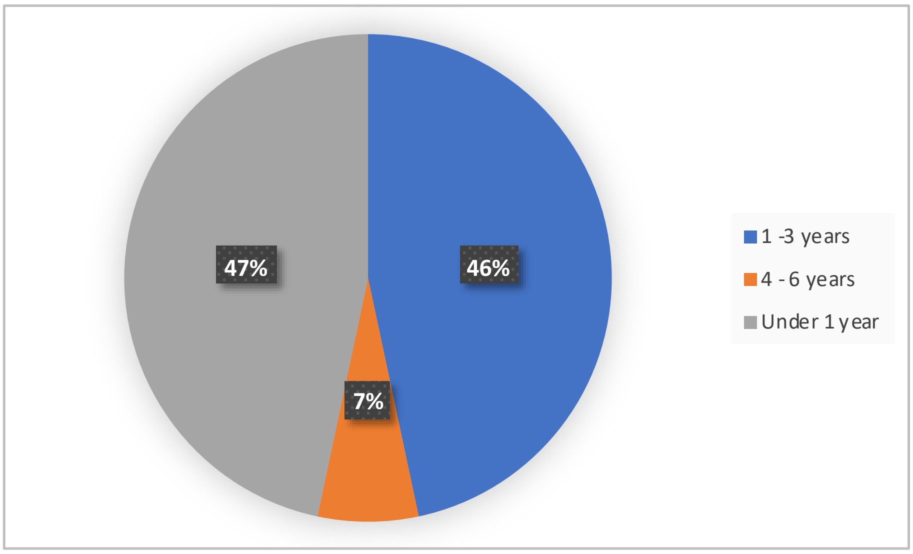


Figure 5.9: Percentage of Mobile Card Emulation Applications Usage, by Years of Usage

Security of Mobile Card Emulation Applications in comparison with Security of Contactless Cards

When asked to compare the safety of contactless cards with Mobile Card Emulation Applications, responses were clear as can be seen in Figure 5.10, with 73% of respondents having rated Mobile Card Emulation Applications as equivalent or more secure than contactless cards. Opinions to the contrary represent only 20%.

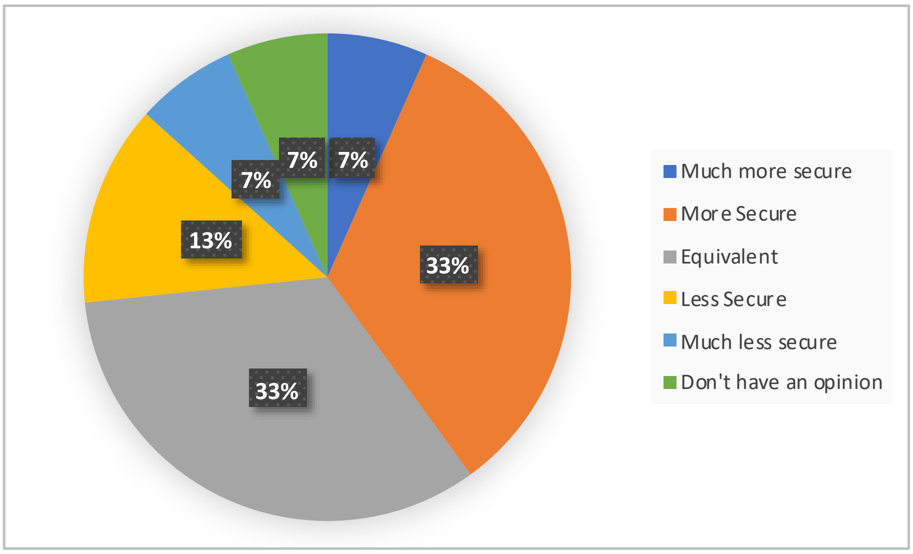


Figure 5.10: Respondents' Security Comparison of Mobile Card Emulation Applications with Contactless Cards

Comparison of Confidence in Mobile Financial Applications Security with Mobile Card Emulation Applications Security

Figure 5.11 presents the comparison of the respondents' level of trust in MFA and Mobile Card Emulation Applications security. Regarding the MFA, 87.5% of the respondents were divided between a classification of the security level between "Medium" and "High". Regarding Mobile Card Emulation Applications, most respondents (64%) rated the security as "Medium" while opinions on other ratings were not concrete.

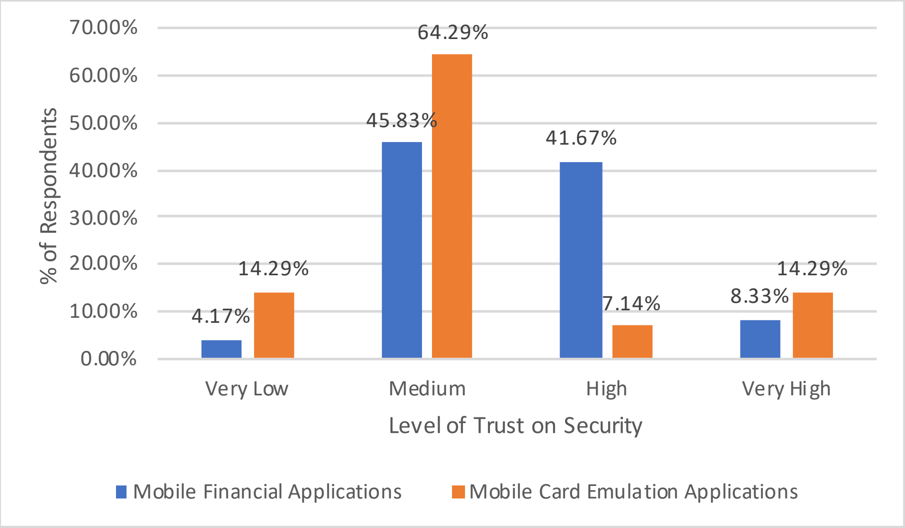


Figure 5.11: Comparison of Levels of Trust in Mobile Financial Applications and Mobile Card Emulation Applications Security

Based on this data, it is possible to conclude that, in general, respondents consider that MFAs are more secure than Mobile Card Emulation Applications.

5.3.3 Security Incidents with Mobile Financial Applications and Card Emulation Applications

Of all respondents, only one (3.13% of the sample) responded positively when asked if they had any incident related to MFA, having classified their impact as "Low" as can be seen in Table 5.4:

Table 5.4: Respondents Related Incidents by Mobile Application Type

Mobile Application Type	Respondents (%)
Financial	3,13% (1 answer)
Card Emulation	0%

Based on this, it can be concluded that the occurrence of incidents related to these types of mobile applications are not common.

5.3.4 Suggestions of Other HCEt Threats and Improvement for the Study

None of the responses obtained indicated other threats to the HCEt architecture (other than those presented in the survey).

Regarding additional information and suggestions for improvement by the respondents, there were two proposals:

1. *"What was my incident and what was the harm caused"*

   The respondent referred to the question *"Have you ever experienced a security incident related to a Mobile Financial Application?"*, for which there was a positive response. In the case of a positive response, the respondent was asked to rate the impact/damage caused by the incident. In his view, it would have been good if the incident had been questioned and the actual damage that had occurred, too.
   In this survey the focus was on obtaining generic and statistical indicators with the concern of not to be intrusive in collecting too specific information on the respondents or on their experience, hence it was considered that there was no need to detail the incident and its specific damage but rather only request a generic rating on a scale of values.

2. *"Instead of tokenization-based HCE, it could be a solution based on elliptic curve cipher similar to the used in the SQRL protocol (https://www.grc.com/sqrl/sqrl.htm)"*

   Secure Quick Reliable Login (SQRL) is an authentication method for web sites based on public-key cryptography which also uses QR Codes. This suggestion the respondent presents can be considered as a valid possibility of future work, also, for example, as a risk assessment. There is already, at least, one commercial mobile wallet solution[4] that performs payments based on reading QR Codes, which would be an interesting case of study, for example.

This survey represents a fundamental component of this study by giving reliable information to the Risk Assessment to HCEt, which is presented in the next Chapter.

[4] MB WAY: `https://www.mbway.pt`

Chapter 6

Host Card Emulation with Tokenisation: Security Risk Assessment

The possibility of emulating smart cards on a mobile device without the need of an SE turns the NFC payment ecosystem simpler while adds value to payment service providers by improving factors such as time-to-market and development costs. Additionally, the need to cooperate with other parties is no longer necessary given that the role of SE issuers and manufacturers is eliminated. On the other hand, payment service providers will have to accept or externalise the additional risk or put in place controls in order to mitigate or eliminate the risks.

Paradigm Shift

The paradigm has changed with HCE. Before, the security of the architecture (traditional chip card + PIN) was ensured at the hardware level with cryptographic keys being stored in tamper-proof chips (SE) embedded in physical cards, which provided a high level of security, assuring the critical data within the chip is trustworthy and the transactions authenticated by the chip are legitimate. With HCE, the critical data is stored on software and the key provisioning is performed by a Token Service Provider (see 3.3.2) and sent over-the-air, via mobile or Wi-Fi. It cannot be assumed that the data or the transaction are legitimate *per se*. In order to mitigate this increment in risk, further security controls should be implemented. The mobile ecosystem is increasingly complex, and plenty of security challenges where the mobile device is only the "user facing component" of a much wider ecosystem consisting of app stores, services and content providers [9]. For instance, entities offering these types of mobile payments need to develop applications for multiple operating systems and for many distinct device models and types[1]. This fact requires

[1] The architecture of each mobile device represent distinct and specific security threats

specialised knowledge about the security threats [49] of each of them and that adequate risk mitigation measures be implemented. This constitutes a constant and continuous effort to maintain an acceptable risk level.

6.1 Context Establishment

This risk assessment is intended to determine the risks related to the HCEt architecture, as well as evaluating them by their severity levels.

In line with ISO/IEC 27005 International Standard for Information Security Risk Management, it is specified from Sections 6.1.1 to 6.1.3 the method and criteria for the risk assessment, along with its scope and boundaries, and from then the risk assessment itself is presented.

6.1.1 Risk Assessment Method and Criteria

Being HCEt a recent technology and still in consolidation and adoption, there are yet no relevant studies on the specific related risks. Given this, it was decided to base the risk evaluation of HCEt on the opinion of Information Security and Information Technology (IT) experts with qualifications and experience. This method seeks to solve the lack of existent documentation and ensure that the risk estimation is executed as impartially and assertively as possible.

A survey (presented in Chapter 5) was conducted to gather informed and specialised opinions about the HCEt risk classification. It was based on the threats (see in Section 6.3) identified in the study “Risk Management in Mobile Financial Services - The Risk Review” conducted by the entity Mobey Forum and relating to the MFS in a collaboration that included several experts in banking solutions and risk management of various renown financial entities.

Criteria

The Risks were estimated by the respondents as to the Likelihood and Impact for each threat, according to the matrix defined in Section 4.2.3.

6.1.2 Scope

The scope of this risk assessment is the architecture of HCEt (see Section 3.3.2), which comprises the following items of its groups of Assets and Processes/Phases:

Assets:

- Application;
- Communications;

- Customer;
- Data;
- Mobile Device;
- Service Infrastructure;
- Transaction.

Processes/Phases:

- App Installation:

  The customer installs the wallet app in his device to enrol his smartcards and perform transactions;
- Provisioning:

  During the enrolment of a smartcard in the wallet app, the app will request payment tokens[2] to be able to perform transactions, online or offline. These tokens are stored in the app and are derived from the original card's PAN, provided by the issuer and sent to the TSP, who performs the tokenisation and sends it to the frontend server for card provisioning over-the-air[3];
- Mobile Transaction:

  The customer performs the transaction (a payment) by approaching his smartphone to the POS terminal;
- Detokenisation:

  After receiving the transaction from the POS terminal, the payment processor verifies if it was performed using a token, and if so, sends it to the TSP for performing detokenization to the original PAN[4]. After detokenisation, the TSP sends it back to the payment processor;
- Issuer Authorisation:

  The issuer receives the transaction from the payment processor and performs its validation, returning the response to the terminal which will present the result of the validation to the customer that performed the payment.

6.1.3 Boundaries

The context of this risk assessment is limited to the concept of the architecture presented and the scope previously defined. It is not applied to any specific real and/or commercial implementation. For those cases, each model or implementation needs to be specifically evaluated.

[2] A number of payment tokens previously defined by the app provider

[3] Wireless data transfer

[4] PAN recovery

6.2 Identification of Assets

Assets represent something that has value for an organisation, an entity, etc., and which therefore requires protection. Table 6.1 identifies the assets for HCEt model.

Table 6.1: Identification of Assets

Asset	Description
Credentials	Personal data that characterises the customer as to his individuality or that may be used as security credentials, which shall not be disclosed. Credentials can be for example, payment tokens, cell phone number, card numbers or PINs.
Data	Data related or supporting the business or personal identity that if disclosed could constitute an advantage to competitors or violate regulations (e.g., privacy requirements). Examples: • Operational data; • Personal data; • Transactional data.
Funds	Monetary value eligible to be transacted.
Infrastructure	Continuous reliability, availability and trust of the infrastructure systems. Degradation of the correct functioning of the infrastructure systems may lead to costs. Examples: • Security systems; • Communication systems; • Storage systems; • Applicational systems.

Asset	Description
Payment Tokens	As EMVCo[5] describes a Payment Token [41]: *"...surrogate value for a PAN, that is a 13 to 19-digit numeric value that must pass basic validation rules of an account number, including the check digit. Payment Tokens are generated within a BIN range that has been designated as a Token BIN Range and flagged accordingly in all appropriate BIN tables. Payment Tokens must not have the same value as or conflict with a real PAN."* In accordance with most known card schemes, Payment Tokens vary from the real PAN both by its numeric representation and its date expiration or purchase limit.
Reputation	Intangible and subjective global evaluation as being a trustful, reliable and credible organisation.
Services	Continuous availability and reliability of the service provided, and the inherent costs related to the failure of the service provision.

6.3 Identification of Threats

As mentioned in Section 6.1.1, the threats identified in the study "Risk Management in Mobile Financial Services - The Risk Review" by Mobey Forum, are applied to MFS, in whose HCEt are included. Given this, the applied threats for HCEt environment (described bellow) to be analysed and evaluated within this risk assessment are the same as the identified in the Mobey Forum's study, except of "Man-in-the-Browser", which were not considered for this risk assessment. Plus, for the threat "Attacks on Secure Element", the mode applied to the HCEt environment is the Software SE mode.

The threats for HCEt are described below, and can be grouped as shown in Figure 6.1:

T1 – Customer Impersonation
"Customer impersonation occurs when an attacker poses as the customer. Impersonation of the customer may happen during the registration for, or installation of, the MFS service or during the MFS transaction."

Social engineering and phishing
"Social engineering is a non-technical method that normally relies on user interaction and often tricks people to break normal security procedures in order to disclose confidential information or create a channel that an attacker can get access to (e.g. [50]).

[5] The company who manages the EMV specifications for chip cards, as described in Chapter 2

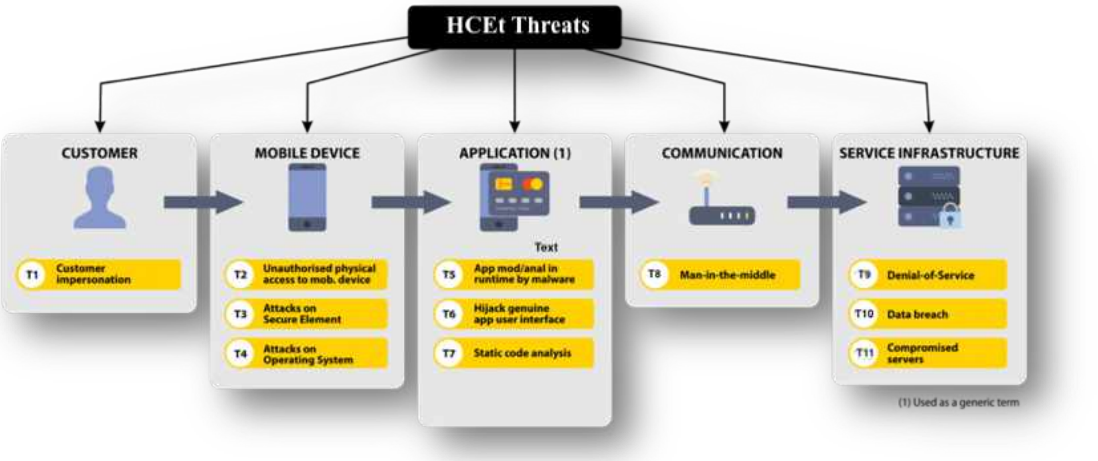

HCEt Threats
CUSTOMER
MOBILE DEVICE
APPLICATION (1)
COMMUNICATION
SERVICE INFRASTRUCTURE
T1 Customer impersonation
T2 Unauthorised physical access to mob. device
T3 Attacks on Secure Element
T4 Attacks on Operating System
Text
T5 App mod/anal in runtime by malware
T6 Hijack genuine app user interface
T7 Static code analysis
T8 Man-in-the-middle
T9 Denial-of-Service
T10 Data breach
T11 Compromised servers
(1) Used as a generic term

Figure 6.1: Identification of HCEt Threats (adapted from the original image from [9])

Some examples of this technique are the typical email that tricks the victim to click on a malicious link that explores some vulnerability on the system, or presents a clone of the banking web site misleading the victim to enter his credentials (e.g. [51]).

Phishing attacks can also be performed through phone calls (vishing – Voice phishing) or SMS (smishing – SMS phishing). Some vishing attacks instruct the victim to enter some commands on the computer to 'avoid being infected by a virus' but is actually creating a channel for the attacker or installing a virus.

It should further be noted that social engineering and phishing are very often employed as a first step to launch other specific attacks. As an example, phishing plays a key role in carrying out targeted digital attacks. Some users are not able to recognise phishing e-mails. As a consequence, phishing continues to be a low-threshold and effective method for attackers. Phishing is also sometimes linked to the distribution of malware, which may, for example, be activated when victims are intentionally misdirected to an infected website."

Synthetic Identities

"Synthetic identity fraud involves the creation of one or more identities using false identity information, typically towards establishing an account with a bank and then gradually building credit, with a plan to ultimately default. Creating a synthetic identity is often achieved by collecting data through social media mining, phishing, and data breaches; and then aggregating it into an identity

designed to avoid detection measures. One or several synthetic identities can be used in interactions with the bank without detection more easily using a mobile device, particularly with a prepaid SIM/UICC card."

T2 – Unauthorised Physical Access to Mobile Device

"An attacker may obtain physical access to the mobile device. According to LATimes, in 2013 more than 12,000 mobile phones were lost or stolen every day in the US. The protection configured on each mobile device is crucial in these situations. As an example, an attacker can easily read a mobile device with confidential information without encryption. An attacker having access to a mobile device, even if only for a limited amount of time, can change the settings of the mobile device (e.g., the user preferences) or request applications to dump data, load any data or load any malicious application on it (e.g., create a hidden channel to the attacker)."

T3 – Attacks on Software Secure Element[6]

"...An SE may take different forms including a UICC (Universal Integrated Circuit Card), a microSD Card, an eSE (Embedded Secure Element) or even an SSE (Software Secure Element). (...) For the MFS service, the SE may be an important component. This element can be used to store a dedicated MFS application, sensitive information (e.g., credentials) for the MFS service or for the identification of the customer. It is, therefore, very susceptible to attack."

T4 – Attacks on Operating System

"...the operating system (OS) is vulnerable to certain types of attacks. If infected, the system can force the application to perform unwanted actions or even control the whole mobile device. The risk or this type of attacks is clearly higher with jailbroken/rooted devices."

T5 – Application Modified in Runtime by Malware

"If a mobile device is already infected with malware (e.g. by another malicious installed application or an infected operation system component/module), depending on the user's privileges, even if the customer's mobile device has the genuine financial application, it can be susceptible to attacks. As an example, the malware could be injected into the genuine application that might, for instance, result into retrieving sensitive data such as customer keys or credentials or even change the content that the genuine application presents to the customer.

[6] In Mobey Forum's study, it referred to many SE types, but for HCEt, it refers to Software Secure Element (SSE)

Rather than deploying malware to modify an application, an attacker could also directly install the application onto a mobile phone or emulator they control, and then manually modify the execution of the application. This allows the attacker to understand an application. The learnings of which could be exploited as a mass attack deployed through means such as malware.

An attacker does not always need to modify an application to learn its secrets. Simply observing the application running through standard development tools such as debuggers and memory analysers could also allow the attacker to retrieve 'secret' information.

To perform these attacks, normally, the attacker has to exploit some vulnerability in the system. As an example, an attacker could root the victim's mobile device and then install a hidden channel to steal the customer's credentials. Another vulnerability might be caused by mobile remote control. If an attacker gains remote access to a victim's mobile device, he might be able to bypass some controls such as device fingerprinting or geo-location and thus steal credentials or customer data.

Another threat is the download of a fake or modified application. It is an application that from a customer's perspective is similar to the original one, but in reality, behaves differently in the background (e.g., a trojanised app). This threat is different from those previously described because here, for example, an application can be available in the application store with an icon similar to the genuine one, or in third party application stores with the same icon all with the same interfaces but in reality, they behave differently.[7]

One way of executing this type of attack would be to download the genuine application, unpack it, modify the code and then repackage it. To the user, it would appear to be behaving as the genuine application (because most of it is genuine) but some malicious code would be executed in the background."

T6 – Hijack Genuine Application User Interface

"Similar to the previous threat, malware on a mobile device can for example hijack the user interface. This attack may require few privileges since it does not need to access the genuine application process information, but can, for example, when a victim opens the genuine application, present a cloned interface, where it could fool the victim into introducing their credentials."

T7 – Static Code Analysis

"By making static code analysis, an attacker can retrieve information about the application or steal data (e.g. cryptographic keys) from the application. This

[7] As an example, see [52]

information could be critical given that vulnerabilities may be found. Without access to the original source code, code analysis has to be performed by reverse engineering the application.

Applications are often built from "library" components - effectively plugging together different software modules to make a complete application. If one of those library components was lifted out of the application, it could be used outside the originally intended context. This could allow an attacker to have access to data and services they were not meant to have access to."

T8 – Man-in-the-Middle

"Man-in-the-middle are attacks where, as the name implies, an attacker is in the middle of the communication between the parties independently of the communications type, such as remote or proximity interaction (e.g., in an NFC communication, an attacker can perform such an attack by using a proxy channel between the proximity communications).

With these attacks, a customer assumes that he/she is interacting directly with the intended component/service, but the attacker "in the middle" is eavesdropping or changing the information to their benefit.

Typically, such an attack could be launched through vulnerabilities in the communication protocols used. By analysing the communication, an attacker can re-engineer the protocol. The communication protocol is fundamental for any MFS. If an attacker understands how the communication protocol works, they can discover and exploit its vulnerabilities."

T9 – Denial of Service (DoS)

"A Denial-of-Service (DoS) attack is an attempt to make a service unavailable to its users for its intended purposes. This can be realised in a number of different ways such as resetting or exhausting its resources, the bandwidth, the processing capacity or the memory. A successful DoS attack directly affects the availability of a network system.

"From the various forms of attacks, the Distributed Denial-of-Service (DDoS) is the most dangerous, where multiple systems are used to carry out a coordinated attack."

T10 – Data Breach

"Data breaches are the intentional or unintentional release of critical information to an untrusted environment. The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data. However, if an unauthorised person views or misuses confidential information,

that should also be considered as a form of data breach. Such breaches typically happen due to hacktivism, dissatisfied employees or careless behaviour with confidential data."

T11 – Compromised Service Provider Servers[8]

"A compromised server at a service provider can be very dangerous because it can infect the company itself or their customers through data breaches or malfunctioning operations. If the service provider is the intended target, the attackers can leak sensitive information, impersonate the company or even mess with the lifecycle process of the operations (e.g. change authorisation parameter settings). Therefore, it is very important to maintain every single service and machine at a service provider with proper security, with special attention to the ones that are exposed to the internet.

Like any secure service the operation lifetime of the service is very important, but the initialisation and termination phase of the equipment are of extreme importance as well (e.g., if a server processes payment card numbers during its service, it is important to have a secure data wiping methodology to guarantee that nobody can recover sensitive data from an 'old server left in the trash')."

6.4 Identification of Existing Controls

Existing Controls (EC) [44] are controls that are already implemented in order to mitigate risks while avoiding unnecessary work or cost in extra mitigation measures.

Table 6.2 presents the existing controls that are common for HCEt assets that contribute to mitigate the likelihood and ease of exploiting a vulnerability, or the impact of an incident.

[8] Modified name from the original "Compromised Servers", in order to be more specific

Table 6.2: Description of HCEt Existing Controls

ID	Description of the EC
[EC1]	**Title**: Mobile OS Common Security Features **Description**: • Sandbox for application's execution; • Device and data access control options (PIN, passcode, fingerprint, face or retina recognition); • Full Device Encryption; • Remote Wipe. **Threats Addressed**: • T5 – Application Modified/Analysed in Runtime by Malware; • T6 - Hijack Genuine Application User Interface; • T2 - Unauthorised Physical Access to Mobile Device; • T1 - Customer Impersonation.
[EC2]	**Title**: Communication Security in Transport (SSL / TLS) Between Financial Entities **Description**: Mandatory control by PCI-DSS [53] international standard. **Threats Addressed**: • T8 - Man-in-the-Middle; • T1 - Customer Impersonation.

ID	Description of the EC
[EC3]	**Title**: Payment Tokens Limited Utilisation for Major Contactless Payment Schemes, by Design **Description**: • VISA tokens are limited by number of transactions; • MasterCard tokens are limited by expiry date. **Threats Addressed**: • T3 – Attacks on Software Secure Element; • T7 – Static Code Analysis; • T8 – Man-in-the-Middle; • T10 – Data Breach; • T11 - Compromised Servers.

The following threats are not addressed by the ECs:

- **T4 - Attacks on Operating System**: By default, mobile devices don't have built-in anti-malware software to protect them from being compromised. On the application side, there are ways of hardening applications to self-protect from compromised and/or rooted devices but they're costly and it is easier for the organisations to accept the risk and chargeback the customer victim of an attack, instead of investing on the protection of the application;
- **T9 - Denial of Service (DoS)**: Delaying server responses to client requests based on their volume in certain periods of time[9] or distributing the server bandwidth load by multiple servers are good practices that should be put in place for the type of infrastructure that HCEt is. However, it depends always on the specific implementation and it is not a mandatory control.

6.5 Identification of Vulnerabilities

Vulnerabilities are related to flaws or weaknesses in the design or implementation that can be exploited by threats (intentionally or unintentionally) to adversely cause harm to an

[9] Also known as *Throttling*

asset or group of assets. Below, in Table 6.3, the vulnerabilities identified for the HCEt architecture are described.

Table 6.3: Description of HCEt Vulnerabilities

ID	Vulnerability Description
[V1]	**Title**: Software Vulnerabilities **Description/Consequence**: Non-alignment with Security by Design principles [54] and lack of Secure Code Practices [55] result in applications with high numbers of vulnerabilities. **Exploitable by**: • T2 - Unauthorised Physical Access to Mobile Device; • T3 - Attacks on Software Secure Element; • T4 - Attacks on Operating System; • T5 - Application Modified/Analysed in Runtime by Malware; • T9 - Denial of Service (DoS); • T10 - Data Breach.
[V2]	**Title**: Lack of Awareness and Security Information Training **Description/Consequence**: The lack of awareness and training on information security may increase the susceptibility to social engineering attacks. **Exploitable by**: • T1 - Customer Impersonation; • T2 - Unauthorised Physical Access to Mobile Device; • T5 - Application Modified/Analysed in Runtime by Malware.

ID	Vulnerability Description
[V3]	**Title**: Lack of Code Obfuscation and/or Encryption **Description/Consequence**: This vulnerability gives a greater probability of success and/or less effort in reverse engineering apps. **Exploitable by**: • T3 - Attacks on Software Secure Element; • T5 - Application Modified/Analysed in Runtime by Malware; • T7 - Static Code Analysis.
[V4]	**Title**: Lack of Implementation of Defensive and Preventive Mechanisms **Description/Consequence**: The lack of implementation of defensive controls against bandwidth exhaustion (e.g. throttling), may lead to DoS situations. **Exploitable by**: • T9 - Denial of Service (DoS).
[V5]	**Title**: No Encryption Set for Sensitive Data Inside the Wallet App **Description/Consequence**: This vulnerability, in the case of successful reverse engineering of the application, may compromise sensitive information such as Payment Tokens. **Exploitable by**: • T3 - Attacks on Software Secure Element; • T5 - Application Modified/Analysed in Runtime by Malware; • T7 - Static Code Analysis.

ID	Vulnerability Description
[V6]	**Title**: Server Misconfiguration **Description/Consequence**: Server misconfigurations such as forgotten open ports, default passwords, directories with wrong access permissions or operating systems with missing patches may lead to a complete compromise of the infrastructure of HCEt. **Exploitable by**: • T8 - Man-in-the-Middle; • T9 - Denial of Service (DoS); • T10 - Data Breach; • T11 - Compromised Servers.
[V7]	**Title**: Use of Communication Protocols Without Encryption **Description/Consequence**: For example, RFID communications have no encryption by default. The use of communication protocols without encryption (or deprecated) may lead to communication interception attacks. **Exploitable by**: • T5 - Application Modified/Analysed in Runtime by Malware; • T8 - Man-in-the-Middle; • T10 - Data Breach.

ID	Vulnerability Description
[V8]	**Title**: Lack of Control in Published Apps by App Stores **Description/Consequence**: Disguised as genuine apps[10], these apps include malicious software (usually trojans) to perform malicious actions (steal personal data, credit card data, etc.). These applications are published on major app stores [56, 57], which are reliable to most users. **Exploitable by**: • T1 - Customer Impersonation.

6.6 Risk Analysis

As mentioned in Section 6.1.1, the Risk Analysis for HCEt was performed through a survey (see Chapter 5) conducted specifically to Information Security and Information Technology (IT) experts. These experts estimated the likelihood and impact for the identified threats (see Section 6.3) based on their knowledge and experience with HCEt[11], assigning them with values from 1 to 5 (according to methodology described in Chapter 4), from the most to the least likely and harmful, respectively.

The estimation for the risk of HCEt threats, obtained from the answers to the survey, is presented in Section 6.1.1, as well as the answer distribution for the likelihood and impact values assigned for each threat.

Note: Empty answers were not considered for the calculation. The likelihood and impact estimation are represented by the mean value from all valid answers.

6.6.1 Risk Estimation Summary

Based on the results of the Risk Estimation presented below in Figure 6.2, it is possible to observe that for the great majority of the threats, the respondents attributed a higher impact when compared to the likelihood of occurrence.

It should be noted that only one of the eleven threats (representing 9%) had an estimated value lower than 3 (Medium) for impact.

[10] For example, malware scanning tools

[11] And information about HCEt given with the survey

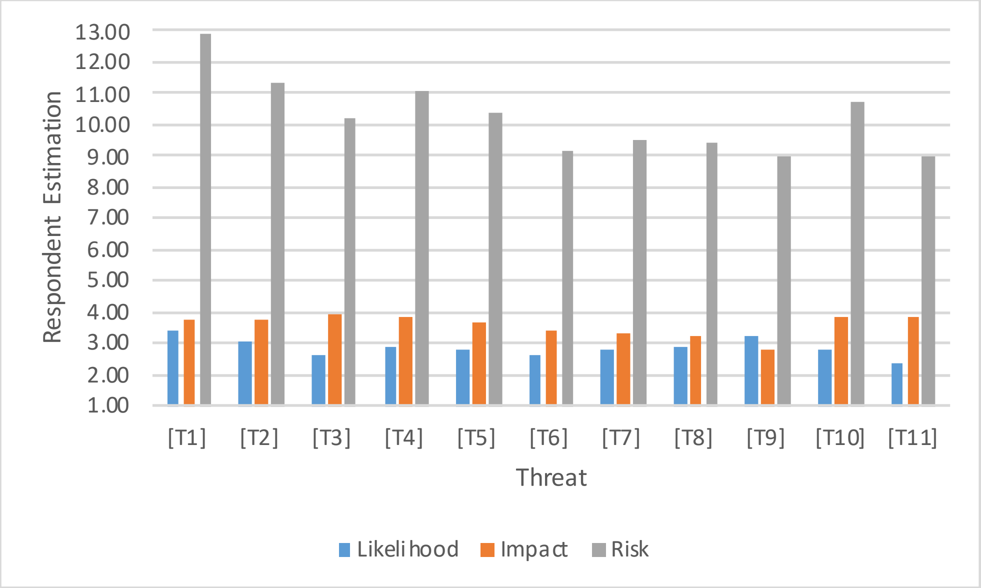


Figure 6.2: Risk Estimation for HCEt Threats with Answer Distribution

Table 6.4: Summary of Risk Estimation

ID	Title	Likelihood (1 to 5)	Impact (1 to 5)	Risk (L x I)
[T1]	Customer Impersonation	3,45	3,73	12,89
[T2]	Unauthorised Physical Access to Mobile Device	3,03	3,74	11,35
[T3]	Attacks on Software Secure Element	2,58	3,97	10,24
[T4]	Attacks on Operating System	2,87	3,87	11,11
[T5]	Application Modified/Analysed in Runtime by Malware	2,81	3,71	10,41
[T6]	Hijack Genuine Application User Interface	2,65	3,45	9,13
[T7]	Static Code Analysis	2,84	3,35	9,52
[T8]	Man-in-the-Middle	2,90	3,26	9,46
[T9]	Denial of Service (DoS)	3,19	2,81	8,96
[T10]	Data Breach	2,77	3,87	10,74
[T11]	Compromised Servers	2,32	3,87	8,99

Table 6.4 presents the mean values for Risk Estimation, Likelihood and Impact, for each threat identified in Section 6.3.

The calculation of the mean value of the results is very linear, being all threats classified with Medium probability of being exploited (except for T11), and impact values for its exploitation varying from 3 (Medium) to 4 (High) for every threat according to the opinion of the respondents. No Low impact was identified for any threat, being the majority of the threats expected to be likely to be exploited.

From the analysis of results, it can be concluded that **all threats were classified with “Medium” risk score**.

In order to allow a more direct view and summarise in terms of likelihood, impact and risk for the threats to the HCEt model, the Top 3 of threats was compiled in Table 6.5 for the three variables:

Table 6.5: Top 3 Threats for Likelihood, Impact and Risk

Top 3 - Likelihood	Top 3 - Impact	Top 3 - Risk
[T1] – Costumer Impersonation	[T3] – Attacks on Software Secure Element	[T1] - Customer Impersonation
[T9] – Denial of Service	[T4] – Attacks on Operating System	[T2] - Unauthorised Physical Access to Mobile Device
[T2] – Unauthorised Physical Access to Mobile Device	[T10] – Data Breach	[T4] - Attacks on Operating System

Respondents considered that the threats most likely to be exploited are non-technical (except for T9), consisting in exploring human vulnerabilities, and the threats capable of causing more harm are the more technical and with less ease of exploitation, requiring highly advanced hacking abilities and deep knowledge about the implementation and operation of HCEt.

6.7 Consolidated Risk Evaluation

Risk Evaluation seeks to understand and provide conclusions about the results obtained from the Risk Analysis, in order to identify future actions to take.

Figure 6.3 shows risks ordered by severity, from the highest to the lowest. All risks are at an average level of severity (between 8.96 and 12.89) with about 50% of risks presenting values slightly above “Medium” according to the matrix for the risk determination, previously defined in Section 4.2.3. The main conclusion to be drawn from the Risk Assessment is that respondents conclude that the main risks (T1 and T2) for HCEt model are based on the exploitation of the human flaws or, on the other hand, that the greatest threats lie in exploiting vulnerabilities on humans, in which the most determinant is the previously identified in Section 6.5: ”[V2] - Lack of Awareness and Security Information Training.” Given the experience and knowledge of the professional areas in which respondents are (see Section 5.2.2), this risk assessment clearly portrays the perceived lack of user awareness, above any risk of technology-based attack.

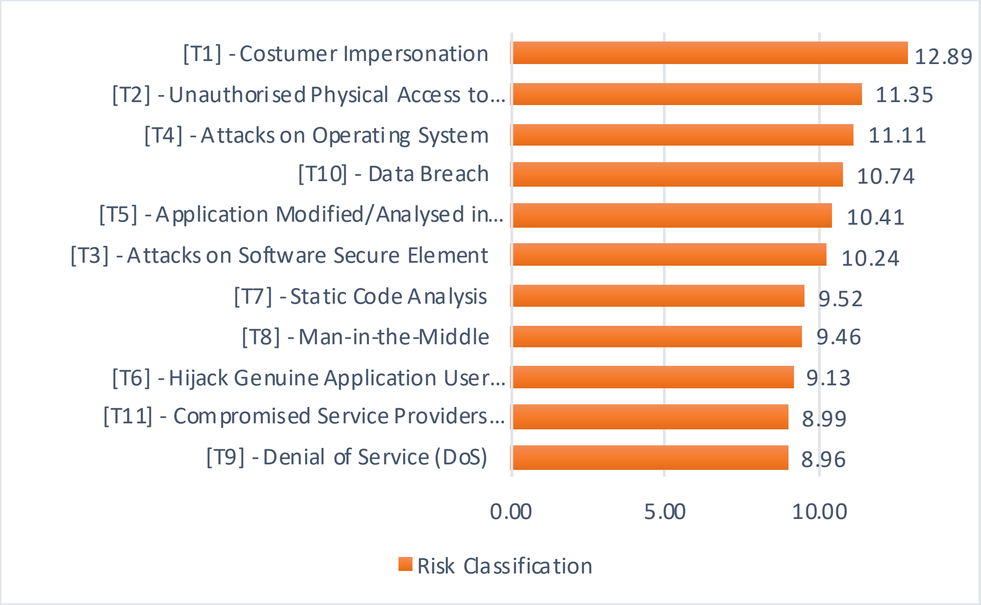


Figure 6.3: Consolidated Risk Evaluation by Threat (from the highest to the lowest)

Taking into account the average value of the risk, 10.25, it is possible to name the risks that are above the average of the classification as Top risks. Denial of Service ([T9]) is considered the threat with the lowest risk, although it was considered the threat with the 2nd highest probability, as can be seen in Figure 6.3. It is also by far the threat with the lowest impact attributed, which allows to conclude that the unavailability of the service is not as significant a risk as the rest.

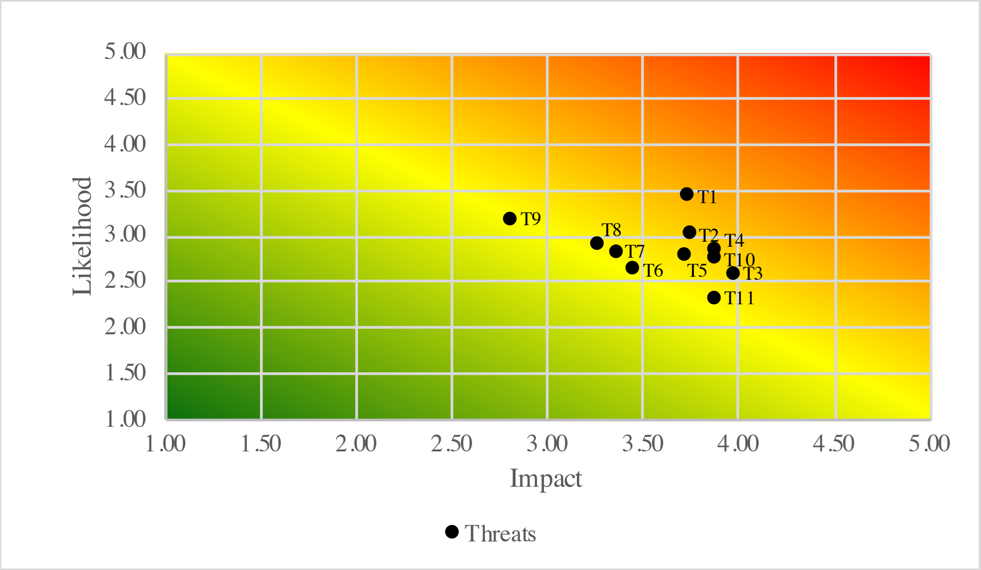


Figure 6.4: Risk Evaluation Distribution

Analysing the Risk Evaluation Distribution in Figure 6.4, it is possible to obtain the perception of the risk severity positioning of each threat, within the previously defined in Section (4.2.3) matrix values for risk estimation. Although the values obtained are close to each other, it is easily verifiable that the most conspicuous risks are T1 and T9, which correspond to the threats of higher and lower risk level, respectively. T9 (DoS) is by far the threat with the lowest impact in case of exploitation and is also considered by the respondents as the second most likely to occur, only surpassed by Customer Impersonation (T1), which is the threat with the highest level of estimated risk. By transposing these facts into practical reality, respondents determined the higher risk of social engineering compared to more sophisticated attacks with respect to severity. In other words, exploiting the knowledge and awareness gap for information security is easier to exploit than for example executing a DoS attack or a Data Breach, which are typically attacks that require high technical level, unlike social engineering attacks, or even improper access to the device, as is the case of T2 that is the second threat with the highest level of risk.

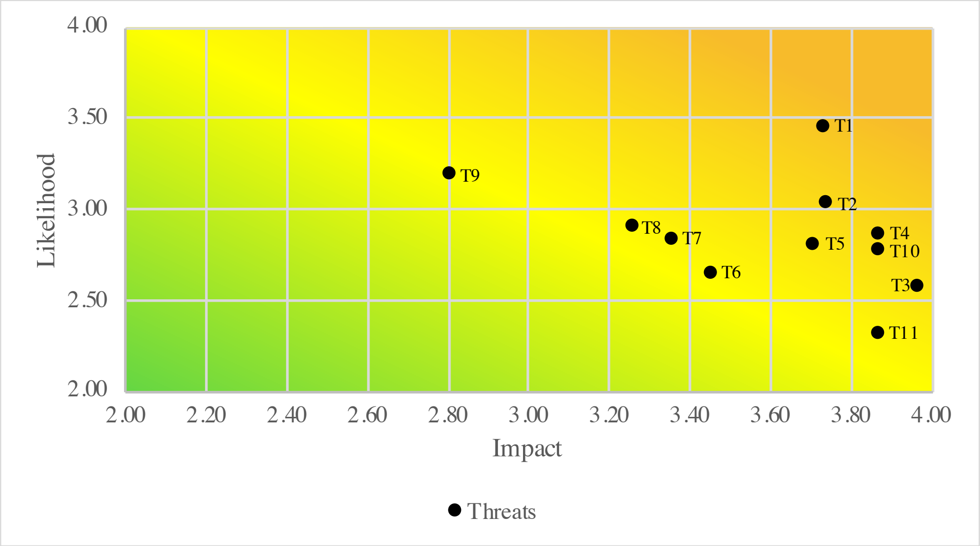


Figure 6.5: Risk Evaluation Distribution with Reduced Scale

Reducing the scale of the distribution of risk classification for HCEt (in Figure 6.5) allows a more detailed view of the results in order to perform a more detailed analysis in an attempt to find patterns that with the original scale are more difficult to visualise. For both variables, the scores can be divided into three groups of values: rankings from 2.5 to 3.0, 3.0 to 3.5, and 3.5 to 4.0. For Impact, T9 is the threat with the lowest classification (as previously mentioned), with T6, T7 and T8 in the intermediate group and all the remaining ones in the group with the highest classification. On the other hand, for likelihood, T11 stands out as the threat with the lowest probability of occurrence and T1, T2 and T9, the most likely ones, being that the most of the threats of this latter group represent social engineering attacks, requiring less effort and technical knowledge while giving superior gains, in the opinion of the respondents.

Table 6.6 presents the consolidated risk evaluation presenting all risks for the HCEt model ordered from the highest to the lowest. This should be the order of importance of the risks to be taken into account for this architecture.

Table 6.6: Consolidated Risk Evaluation

ID	**Title**	**Likelihood (L)**	**Impact (I)**	**Risk Level (L x I)**
[T1]	Customer Impersonation	3.45	3.73	12.89
[T2]	Unauthorised Physical Access to Mobile Device	3.03	3.74	11.35
[T4]	Attacks on Operating System	2.87	3.87	11.11
[T10]	Data Breach	2.77	2.87	10.74
[T5]	Application Modified/Analysed in Runtime by Malware	2.81	3.71	10.41
[T3]	Attacks on Software Secure Element	2.58	3.97	10.24
[T7]	Static Code Analysis	2.84	3.35	9.52
[T8]	Man-in-the-Middle	2.90	3.26	9.46
[T6]	Hijack Genuine Application User Interface	2.65	3.45	9.13
[T11]	Compromised Servers	2.32	3.87	8.99
[T9]	Denial of Service (DoS)	3.19	2.81	8.96

Next Chapter concludes this dissertation by presenting the resume of the achievements and conclusions from the study, as well as the recommendations for future research.

Chapter 7

Summary and Conclusions

This final Chapter analyses the achievements on the study performed as well as proposes suggestions for future work.

7.1 Summary of Contributions

In this dissertation, although having as main objective the Risk Assessment on the HCEt model, it required the investigation on essential related subjects, which are summarised in the following Sections.

7.1.1 Characteristics of EMV Chip Cards

The EMV history and the main features of EMV Chip Cards were analysed. The EMV Chip Cards, which are the most used cards in the world with more than 7 billion active cards by the end of 2017, have Contact and Contactless operation modes and usually both are supported. The Contactless mode does not require physical contact with the payment terminal and it is faster than the Contact mode due to the capability of performing transaction steps after the card has left the proximity of the terminal.

The EMV Chip Cards were created to establish interoperability and a higher level of security for card payments resulting in a reduction of counterfeit cards and subsequent fraud losses. They have security distinguishing features has, for example, the ability to perform cryptographic processing and store confidential information securely, risk management and authorisation controls, digitally signed payment data for authentication and integrity of transactions, and the ability to authenticate the card in offline transactions securely using asymmetric cryptography.

7.1.2 Types of Chip Card Emulation on NFC-enabled Mobile Devices

Host Card Emulation architecture provides emulation of contactless cards mainly by software, enabling transactional communication for mobile devices with NFC. Prior to the

HCE technology, there were different types of NFC payments in different implementations based on SE tamper-resistant hardware, such as the one presented in Section 3.1:

- Universal Integrated Circuit Card (UICC) - Making use of the traditional SIM card to embed the SE;
- Embedded SE - Secure Element based on a hardware chip assembled on the device, independent of the SIM card;
- SD-card - Using an application inside the SD card as an SE.

These SE-based types had disadvantages, for example, related to the provisioning of card's critical keys from Issuers to SD-card or TELCO Manufacturers and the incompatibility of having more than one card being emulated in an SD-card. These aspects led to the creation of a more flexible and interoperable alternative, and consequently the creation of HCE.

In the HCE architecture, a card can be emulated in two ways: through a remote system that communicates with the NFC-enabled mobile device during the transaction process (Cloud-Based HCE), or directly on the NFC-enabled mobile device through an app that emulates the card and exchanges APDU commands with the terminal and has payment tokens stored within for payment transaction (HCEt).

7.1.3 Architecture of Host Card Emulation with Tokenisation

In HCEt, the card emulation is performed by the mobile application in its entirety. It has stored all the keys needed to perform payment transactions. These keys are cryptographic keys and tokens with which the transactions can be generated as if it was a physical card and so the terminal will recognise it as one. The architecture of HCEt is composed by the following entities:

- Issuer – Transfers card credentials and token parameters for the TSP, and, performs transaction authorisations;
- Token Service Provider (TSP) – Generates and transfers tokens for application provisioning;
- Authentication Server – Transfers the generated tokens to the mobile application and perform token management;
- Mobile Device and POS terminal – The mobile device performs the transaction with the POS terminal via APDU commands through its NFC antenna;
- Payment Processor – Processes the transactions in order to verify which need to be sent to the TSP to be detokenised.

7.1.4 Risks Inherent to Host Card Emulation with Tokenisation Model and their Severity

Despite its advantages over solutions using SE hardware, there are several threats to this type of card emulation solutions. The risks inherent to the HCEt model were identified and evaluated, through a risk assessment. Due to the lack of documentation available to analyse and carry out a duly supported risk analysis, together with the fact that the subject matter was very specific and relatively recent, it was decided to classify the risk in the opinion of IT specialists and Information Security specialists.

Through an online survey (described in Chapter 5) the risk levels to the threats of HCEt model were evaluated (Figure 7.1) based on a recent risk assessment on mobile financial services that identifies the various threats inherent to this type of mobile applications, which also apply to the HCEt model, being a very specific form of a mobile financial service.

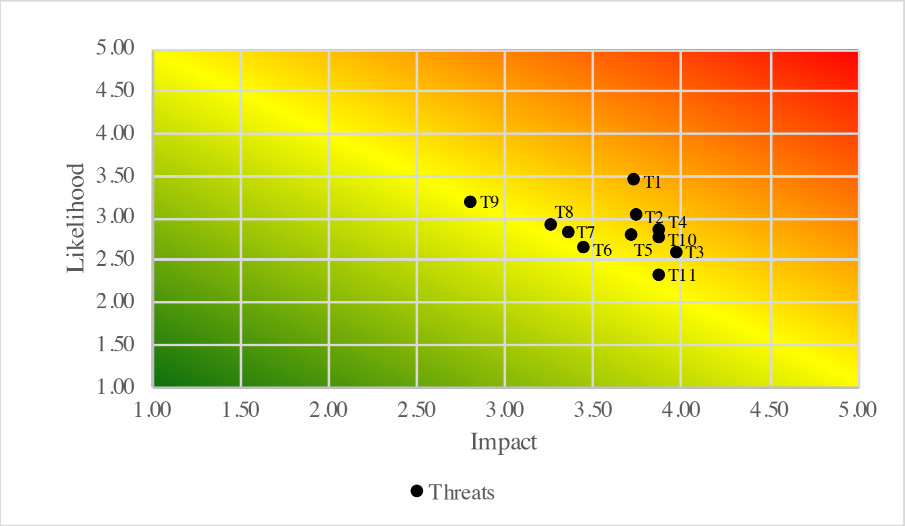


Figure 7.1: Risk Evaluation Distribution (from Section 6.7)

All threats were classified as having a “Medium” risk level, which represents a strong indicator. Threats classified with the higher score (”T1 - Costumer Impersonation” and ”T2 - Unauthorized Access to Mobile Device”) aim to exploit Social Engineering and attempt to take advantage of human weaknesses such as the lack of awareness of the threats related to information security.

7.2 Directions for Future Work

The research can be continued in various directions in the future, such as the following:

Extend the Performed Risk Assessment to a Larger Number of Respondents and Professional Areas

Based on the risk assessment carried out within the scope of this dissertation, a new risk assessment could be carried out to HCE in general, in which it could be surveyed to a larger number of people. In addition to IT and Information Security professionals, the survey could be extended to risk analysts, smartphone insurance specialists, professionals from various police units and criminal investigation with direct links to banking card and smartphone crimes, and fraud analysts from financial organisations.

By reformulating the survey and thus covering a larger and more diversified sample, it would allow measuring the risk of card emulation solutions in general, not just the tokenisation-based model, but, will also require a greater effort at the level of the necessary resources. In addition to the diversity of opinions that is desirable in such an inquiry, questioning law enforcement agencies and fraud analysis would add concrete knowledge of real situations that helps to get insight on cases that have already occurred.

Identify and Propose Mitigation Measures for Risk Treatment

As an important component of a risk assessment after identifying and assessing risks, the identification of mitigation measures is the process to be undertaken in order to be able to address those risks. Based on the risks assessed for the HCEt model, an important future work would be to analyse the best mitigation measures to be implemented (Risk Treatment) in a generic way, with the goal of reducing risk to acceptable values, with the lowest cost and implementation effort.

Having both risk assessment and risk treatment for the HCEt model, it would be an important support in evaluating a business solution to be implemented. It would make it simpler to assess the risks inherent in the model and cost of mitigation from a general point of view, providing a more assertive decision making.

Compare Alternative Solutions to HCEt and Compare Their Risks

In future work it would be interesting to be able to compare to HCEt existing card emulation solutions not using SE hardware. Cloud-based HCE model (described in Section 3.3.1) is one of solutions that could be compared regarding its advantages, disadvantages and its risks, aiming the assessment of which one would be the safest solution from a general point of view.

It would also be of value to compare HCE solutions with other alternative solutions that authenticate (or authorise) payments, such as SQRL, a solution proposed by one of the respondents that relies on an alternative method for authenticating login forms on websites without the need to enter credentials directly into the forms, based on QR code readings, and that could be applied to the authentication of an NFC-enabled smartphone in the presence of a POS terminal.

7.3 Conclusions

The capability of migrating a universal payment method such as the EMV chip card to a mobile device with the ability to emulate and behave like one (EMV chip card contactless) before a POS terminal without the need to change its hardware or software of the same and making it possible to have multiple cards in the same application, is undoubtedly a major breakthrough for the payment industry. Host Card Emulation has brought various new use cases based on portability and convenience, as well as new flavours of fraud and new threats to the financial industry.

In this dissertation, in which the model of HCEt has been analysed from the point of view of its inherent risks with the collaboration of IT and Information Security specialists, the results were clear about the overall severity of the risks identified, despite the short sample of results. None of the risks of HCEt have Low severity, which in brief, means that none of the risks should be disregarded as to their importance.

From all the risks identified and evaluated, the ones that standout from the overall evaluation are the most severe, ”T1 - Customer Impersonation” and ”T2 – Unauthorised Physical Access to Mobile Device” (described in Section 6.3), which are related to Social Engineering and taking leverage of the lack of awareness and training in information security. Despite the increasing complexity and specialisation of technical cyberattacks as well as the technical sophistication of both software and hardware, it has become very clear from this study that the human factor remains the easiest to exploit, with greater gains. This is relevant and tells much about the human side of Information Security that should be, desirably, seen as an essential necessity in the regular training of financial services' customers, but more importantly, in school education, as part of the foundation of the technological society of today.

Bibliography

[1] EMVCo, "Emvco reports over half of cards issued globally are emv-enabled," EMVCo, Tech. Rep., 2018. [*Online*]. Available: https://www.emvco.com/wp-content/uploads/2018/04/Global-Circulation-Figures_FINAL.pdf (cited on page 1)

[2] Statista. (2018) Number of smartphone users worldwide from 2014 to 2020 (in billions). [*Online*]. Available: https://www.statista.com/ (cited on page 1)

[3] K. S. a. S. R. Yong Wang, "Smartphone security challenges," *IEEE Computer Society*, 2012. (cited on page 1)

[4] S. S. N. J. H. Taherdoost, "Smart card security; technology and adoption," *IJS, vol.5, n^o.84*, 2011. (cited on pages 1 and 2)

[5] A. T. O. S. Khan, M. Nauman and S. Musa, "How secure is your smartphone: An analysis of smartphone security mechanisms," *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 2012. (cited on page 2)

[6] Symantec, "Symantec 2018 threat internet security threat report," Symantec, Tech. Rep., 2018. (cited on page 2)

[7] S. G. M. PASQUET, "Fraud on host card emulation architecture," *Second International Conference on Mobile and Secure Services (MobiSecServ)*, 2016. (cited on page 2)

[8] G. LLC, "Diverse protections for a diverse ecosystem: Android security 2016 year in review," Google LLC, Tech. Rep., 2016. (cited on page 2)

[9] M. Forum, "Guide to risk management in mobile financial services - part 1," Mobey Forum, Tech. Rep., 2016. (cited on pages 4, 43 and 48)

[10] EMVCo, *Book 1 - Application Independent ICC to Terminal Interface, vol. 4.3*, EMVCo Std., 2011. (cited on page 5)

[11] ——, *Book 2 - Security and Key Management, vol. 4.3*, EMVCo Std., 2011. (cited on page 5)

[12] ——, *Book 3 - Application Specification, vol. 4.3*, EMVCo Std., 2011. (cited on page 5)

[13] ——, *Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements, vol. 4.3*, EMVCo Std., 2011. (cited on page 5)

[14] (2018) Heropay. [*Online*]. Available: https://www.heropay.com (cited on page 6)

[15] *EMV Chip Deployment Status*, 2018. [*Online*]. Available: https://www.emvco.com/wp-content/uploads/2018/03/20180312_EMVCo_EMV_Chip_Deployment_Stats-20180327.pdf (cited on page 5)

[16] VISA. (2018) Visa chip card stats. [*Online*]. Available: https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats.html (cited on page 5)

[17] (2018) Emv deployment statistics. [*Online*]. Available: https://www.emvco.com/about/deployment-statistics (cited on page 7)

[18] D. J. van den Breekel, "Emv in a nutshell," *Radbound University Nijmegen*, 2016. (cited on pages 6 and 16)

[19] D. King, "Chip-and-pin: Success and challenges in reducing fraud," *Retail Payments Risk Forum*, 2012. (cited on pages 6 and 10)

[20] EMVCo, "A guide to emv," 2011. (cited on pages 6, 10, 14 and 15)

[21] ——. (2018) Emv contactless specifications. [*Online*]. Available: https://www.emvco.com/emv-technologies/contactless/ (cited on pages 8 and 16)

[22] (2018) Embedded security news. [*Online*]. Available: https://embeddedsecuritynews.com (cited on page 9)

[23] J. Poll, "Formal analysis of the emv protocol suite," *Therory of Security and Applications (TOSCA), Nijmengen, Springer*, 2011. (cited on page 8)

[24] A. C. Garvey, "Near field communication," *International Journal of Electrical and Computer Engineering (IJECE), vol. 2, no. 3*, 2012. (cited on page 19)

[25] ISO/IEC, *ISO/IEC 18092, Information Technology – Telecommunications and Information Exchange Between Systems – Near Field Communication – Interface and Protocol (NFCIP-1)*, ISO/IEC Std., 2013. (cited on page 19)

[26] ——, *ISO/IEC 21481 - Information technology – Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol -2 (NFCIP-2)*, ISO/IEC Std., 2012. (cited on page 19)

[27] ——, *ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards*, ISO/IEC Std., 2016. (cited on page 19)

[28] J. Roland, *Anwendungen und Techkik von Near Field Communication (NFC)*. Springer-Verlag Berlin Heidelberg, 2010. (cited on page 19)

[29] B. V. Coskun, "The survey on near field communication," *Sensors 15(6):13348-13405*, 2015. (cited on page 20)

[30] M. A. e. M. ACHEMLAL, "Host-based card emulation: Development, security, and ecosystem impact analysis," *IEEE HPCC, CSS and ICESS*, 2014. (cited on pages 20, 21 and 23)

[31] W. Jullien, "System-on-chip for real-time applications," *Kluwer International Series in Engineering and Computer Science, SECS 711*, 2004. (cited on page 20)

[32] UL, "Hce security implications, analysing the security aspects of hce," UL, Tech. Rep., 2016. (cited on pages 20 and 22)

[33] J. C. M. Blackberry. (2014) So, what's this hce thing anyway? [*Online*]. Available: http://devblog.blackberry.com/2014/09/so-whats-this-hce-thing-anyway (cited on page 21)

[34] Blackberry. (2013) Nfc api. [*Online*]. Available: https://developer.blackberry.com/native/documentation/device_comm/nfc/nfc_api.html (cited on page 21)

[35] (2018) Cyanogenmod. [*Online*]. Available: http://www.cyanogenmod.org (cited on page 22)

[36] (2018) Lineageos. [*Online*]. Available: https://www.lineageos.org (cited on page 22)

[37] (2018) Bankinter. [*Online*]. Available: https://www.bankinter.com (cited on page 22)

[38] M. Forum, "The host card emulation in payments: Options for financial institutions," Mobey Forum, Tech. Rep., 2014. (cited on pages 22, 24 and 25)

[39] Apple. (2018) Apple pay security and privacy overview. [*Online*]. Available: https://support.apple.com/en-us/HT203027 (cited on page 23)

[40] (2018) Apple pay. [*Online*]. Available: https://www.apple.com/apple-pay (cited on page 23)

[41] EMVCo, *EMV Tokenisation Payment Specification*, EMVCo Std., 2014. (cited on pages 25 and 47)

[42] P. SSC, *Tokenisation Product Security Guidelines - Irreversible and reversible*, PCI SSC Std., 2015. (cited on page 25)

[43] ——, *Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)*, PCI SSC Std., 2015. (cited on page 25)

[44] ISO/IEC, *ISO/IEC 27005 - International Standard ISO/IEC 27005 - Information technology — Security techniques — Information security risk management*, ISO/IEC Std., 2018. (cited on pages 27, 28 and 52)

[45] ENISA. (2017) Risk management glossary. [*Online*]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory (cited on page 29)

[46] E. T. J. Broder, *Risk Analysis and the Security Survey - 4th Edition.* Butterworth-Heinemann, 2012. (cited on page 31)

[47] L. Fonte. (2018) Master's dissertation survey. [*Online*]. Available: https://docs.google.com/forms/d/1FJZi7mI9Cv3NzTuq42pCEalHuhK0VcqW3pEXEoFdil0 (cited on page 31)

[48] H. University, "Program on survey research," 2013. (cited on page 31)

[49] CSO. (2017) Five new threats to your mobile security. [*Online*]. Available: https://www.csoonline.com/article/2157785/data-protection/five (cited on page 44)

[50] T. P. I. into Payments. (2016) Fbi warns on 'ceo fraud' with risk of usd 3 billion loss. [*Online*]. Available: https://www.thepaypers.com/digital-identity-security-online-fraud/fbi-warns-on-ceo-fraud-with-risk-of-usd-3-billion-loss/764878-26/abstract (cited on page 47)

[51] J. Vijayan. (2016) 'asacub' trojan converted to mobile banking weapon. [*Online*]. Available: https://www.darkreading.com/vulnerabilities---threats/asacub-trojan-converted-to-mobile-banking-weapon/d/d-id/1324001 (cited on page 48)

[52] (2015) Apple app store malware infected 4000 apps. [*Online*]. Available: http://www.bbc.com/news/technology-34338362 (cited on page 50)

[53] P. SSC, *PCI Data Security Standard (DSS): Requirements and Security Assessment Procedures*, PCI SSC Std., 2016. [*Online*]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1526317478310 (cited on page 53)

[54] OWASP. (2018) Security by design principles. [*Online*]. Available: https://www.owasp.org/index.php/Security_by_Design_Principles (cited on page 55)

[55] ——. (2017) Owasp secure coding practices. [*Online*]. Available: https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide (cited on page 55)

[56] R. Unuchek. (2017) Still stealing. [*Online*]. Available: https://securelist.com/still-stealing/83343/ (cited on page 58)

[57] T. Micro. (2018) Ghostteam adware can steal facebook credentials. [*Online*]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/ghostteam-adware-can-steal-facebook-credentials (cited on page 58)

Annexes

Annex I

Inquiry Request

Olá,

O meu nome é Luís Fonte e sou aluno finalista do Mestrado em Engenharia de Segurança Informática do Instituto Politécnico de Beja (IPBeja), de Beja, Portugal. Venho por este meio solicitar o seu contributo no âmbito dos trabalhos que estou a desenvolver conducentes à minha dissertação de mestrado. Como parte desses trabalhos, estou a realizar uma análise de risco sobre Emulação de Cartões em Dispositivos Móveis (chip cards / smart cards) executada por aplicações, uma arquitectura denominada de "Host Card Emulation (HCE)". No caso concreto da minha dissertação o foco é a arquitetura HCE baseada em "tokenisação", na qual chaves criptográficas derivadas (tokens) das chaves criptográficas dos cartões originais são armazenadas nas aplicações por forma a permitir a execução de transações.

Sendo este um tema relativamente recente e dada a carência de documentação científica que trate especificamente a temática do risco inerente ao mesmo, achei por bem e adequado, basear a classificação do risco na opinião de especialistas de TI e especialistas em Segurança da Informação. Para tal, tomei como base uma análise de risco recentemente realizada sobre aplicações móveis de serviços financeiros (estudo efetuado pela entidade Mobey Forum), que está diretamente relacionada com o tema em estudo na minha dissertação, e na qual são identificadas as diversas ameaças inerentes a este tipo de aplicações móveis.

O seu contributo consiste na resposta a um inquérito que criei especificamente sobre o tema em estudo na minha dissertação, e que pode ser acedido aqui.

"HCE with Tokenisation" é apresentada de forma resumida neste link que poderá querer consultar antes de responder ao inquérito.

Peço ainda que, se possível, partilhe este email com os contactos que considerar convenientes, por forma a poder contar com a opinião do maior número de especialistas nesta área, enriquecendo assim os resultados do inquérito.

O seu contributo será de grande valor para o sucesso do meu estudo.

Antecipadamente agradecido,
Luís Fonte
luispereiradafonte@gmail.com

Hello,

My name is Luís Fonte and I am a final year student of the Master in Computer Science Security Engineering at the Polytechnic Institute of Beja (IPBeja), in Beja, Portugal. I would like to ask for your contribution, in the context of the work on my dissertation. As a part of that work, I am conducting a risk analysis on Card Emulation performed within Mobile Devices (emulation of chip cards in mobile devices, performed within applications), an architecture known as Host Card Emulation (HCE). In this specific study the focus is the HCE architecture based on tokenisation, where cryptographic keys derived (tokens) from the original cryptographic card keys are stored within the application for enabling transaction execution.

As this is a relatively recent topic and given the lack of scientific documentation specifically addressing the inherent risk, I decided to base the risk classification on the opinion of IT specialists and information security experts. To that end, I used as a basis a risk analysis recently carried out about mobile applications for financial services, (by the entity Mobey Forum), which is directly related to the topic under study in my dissertation, and where the various threats inherent to this type of mobile applications are identified.

As your contribution, please answer the survey that I created specifically on the subject under study in my dissertation, and which can be accessed here.

“HCE with Tokenisation” is briefly explained in this link, which you may want to consult before answering the survey.

If possible, please share this email with the contacts that you consider convenient, so that I can count with the opinion of the greatest number of experts in this area, thus enriching the results of the survey.

Your contribution will be of great value to the success of my study.

Thanks in advance!
Luís Fonte
luispereiradafonte@gmail.com

Annex II

Conducted Survey - Host Card Emulation with Tokenisation (HCEt)

The annex starts in the next page.

Master's Dissertation Survey

Mobile Card Emulation Applications

Masters in Computer Science - Security Engineering - ESTIG / IPBeja - Beja, Portugal
Luís Manuel Pereira da Fonte

* Required

Introduction

This survey is conducted within the scope of my Master's Dissertation in Computer Science - Security Engineering and seeks to assess the risk levels regarding Mobile Card Emulation Applications, in a specific model. In this model, card cryptographic keys derived from the physical Integrated Circuit Card (ICC) keys are stored within the application for performing transactions when in communication with payment terminals through Near-Field Communication (NFC). The exact term for this type of Card Emulation is "Host Card Emulation (HCE) with Tokenisation", which is explained in detail in the following link:
https://drive.google.com/file/d/1UgOYqCqtE75CEECw0vSBco9-0JSRChcy

Being a relatively recent technology and still in consolidation in the tech world, there are yet no relevant studies on the specific related risks. Given this, and in order to solve the lack of existent documentation, it is important to base the risk estimation on the opinion of Cybersecurity and Information Technology (IT) experts with qualifications and experience, to ensure that the risk estimation is executed as impartially and assertively as possible.

This survey is designed to gather informed opinions about a risk classification. This is based on the threats identified in the study "Risk Management in Mobile Financial Services - The Risk Review" conducted by the reputable entity Mobey Forum and relating to the mobile environment in a collaboration that included several experts in banking solutions and risk management of various renown financial entities.

The survey consists of this introduction, and the questionnaire. The document available through the hyperlink above may be a valuable resource of technical information about the HCE model with Tokenisation.

You should need approximate 20 minutes to complete this questionnaire.

This survey is anonymous.

Your collaboration will be extremely valuable and in fact fundamental for this study. Thanks in advance.

Personal Questions

These general questions are intended for the distribution of the results by profiles

1. **Where do you currently live?** *

Mark only one oval.

○ Portugal

○ Other: ____________________

2. **What is your gender?** *

Mark only one oval.

○ Female

○ Male

3. **What is your age span?** *
Mark only one oval per row.

	Under 20 years	21 - 30 years	31 - 40 years	41 - 50 years	51 - 60 years	Over 60 years
Please select:	○	○	○	○	○	○

4. **Please indicate your current Profession:** *

5. **How many years working in Information Technology (IT)?** *
Mark only one oval per row.

	Under 1 year	1 - 3 years	4 - 6 years	7 - 9 years	10 or more years
Please select:	○	○	○	○	○

6. **How many years of experience in Cybersecurity?**
(self-taught, academic or professional experience)
Mark only one oval per row.

	Under 1 year	1 - 3 years	4 - 6 years	7 - 9 years	10 or more years	Not Applicable
Please select:	○	○	○	○	○	○

User Background and Experience with Smartphones, Financial Applications and HCE

Assuming you own and use a smartphone, please answer about your user experience

Smartphones

7. **How many years of Smartphone usage?** *
(as a general user)
Mark only one oval per row.

	Under 1 year	1 - 3 years	4 - 6 years	7 - 9 years	10 or more years
Please select:	○	○	○	○	○

8. **Which Mobile Operating Systems have you experience with?** *
(specify all that apply)
Check all that apply.

□ Android
□ Blackberry OS
□ iOS
□ Windows Phone
□ Other:

9. **Please indicate your level of trust in smartphone security, by default:** *
(based on your sense of security, in general terms)
Mark only one oval per row.

	Very High	High	Medium	Low	Very Low	Not applicable
Please select:	○	○	○	○	○	○

Mobile Financial Applications (such as Mobile Banking applications)

10. **How many years have you been using Mobile Financial Applications?** *

(example: Mobile Banking applications)

Mark only one oval.

○ Under 1 year

○ 1 - 3 years

○ 4 - 6 years

○ 7 - 9 years

○ 10 or more years

○ Never used *Skip to question 21.*

Mobile Financial Applications (such as Mobile Banking applications)

11. **How many Mobile Financial Applications have you used already?**

(please indicate the number of Financial Mobile Applications that you have experience with)

Mark only one oval.

○ 1 application

○ 2 - 3 applications

○ More than 5 applications

12. **Please indicate your level of trust in Mobile Financial Applications:**

(in general terms)

Mark only one oval per row.

	Very High	High	Medium	Low	Very Low	Don't have an opinion
Please select:	○	○	○	○	○	○

13. **Have you ever experienced a security incident related to a Mobile Financial Application?**

Mark only one oval.

○ Yes

○ No *Skip to question 15.*

Mobile Financial Applications (such as Mobile Banking applications)

14. **How do you classify the security incident that you experienced, according to its impact?**

(answer to this question only if responded “Yes” in the previous one)

Mark only one oval per row.

	Critical	High	Medium	Low	Very Low	Not applicable
Please select:	○	○	○	○	○	○

Mobile Card Emulation Applications (apps that perform contactless payments)

15. **Are you a user of Mobile Card Emulation Applications?** *

Mark only one oval.

○ Yes

○ No *Skip to question 21.*

Mobile Card Emulation Applications (apps that perform contactless payments)

16. **How many years have you been using Mobile Card Emulation Applications?**

Mark only one oval per row.

	Under 1 year	1 -3 years	4 - 6 years	7 - 9 years	10 or more years
Please select:	○	○	○	○	○

17. **How do you compare Mobile Card Emulation Applications to Contactless Physical Cards, in terms security?**

(in general terms)

Mark only one oval.

○ Much more secure

○ More secure

○ Equivalent

○ Less secure

○ Much less secure

○ Don't have an opinion

18. **Please indicate your level of trust in Mobile Card Emulation Applications:**

(in general terms)

Mark only one oval per row.

	Very High	High	Medium	Low	Very Low	Don't have an opinion
Please select:	○	○	○	○	○	○

19. **Have you ever experienced a security incident related to a Mobile Card Emulation Application?**

Mark only one oval.

○ Yes

○ No *Skip to question 21.*

Mobile Card Emulation Applications (apps that perform contactless payments)

20. **How do you classify the security incident, according to its impact?**

(answer to this question only if responded “Yes” in the previous one)

Mark only one oval per row.

	Critical	High	Medium	Low	Not applicable
Please select:	○	○	○	○	○

Host Card Emulation (HCE) and related technologies

21. **Please specify your level of knowledge regarding HCE and related technologies:** *

Mark only one oval per row.

	Very High	High	Medium	Low	Very Low	None
Please select:	○	○	○	○	○	○

Threats to Mobile Card Emulation Applications

Please choose the Likelihood and Impact values for each of the threats

Scale of classification: 1-Very Low, 2-Low, 3-Medium, 4-High, 5-Very High
Risk Evaluation: Likelihood x Impact
Likelihood: Probability that a threat event will occur
Impact: The magnitude of harm expected to result from the consequences of threat occurring.

Customer

22. **Customer Impersonation / Social Engineering**

(..."is a non-technical method that normally relies on user interaction and often tricks people to break normal security procedures in order to disclose confidential information or create a channel that an attacker can get access to." ... ”Impersonation of the costumer may happen during the registration for, or installation of, the Mobile Financial Service (MFS) or during the MFS transaction.”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

Mobile Device

23. **Unauthorised Physical Access to Mobile Device**

(”...According to LATimes in 2013, more than 12,000 mobile phones were lost or stolen every day in the US. The protection configured on each mobile device is crucial in these situations. As an example, an attacker can easily read a mobile device with confidential information without encryption. An attacker having access to a mobile device, even if only for a limited amount of time, can change the settings of the mobile device (e.g., the user preferences) or request applications to dump data, load any data or load any malicious application on...”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

24. **Attacks on Software Secure Element (SSE)**

(“... The SSE can be used to store a dedicated MFS application, sensitive information (e.g., credentials) for the MFS service or for the identification of the customer. ...”) - The compromise of SSE, mainly through Reverse Engineering, may reveal confidential information that can be used by the attacker.

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

25. **Attacks on Operating System**

(“...the operating system (OS) is vulnerable to certain types of attacks. If infected, the system can force the application to perform unwanted actions or even control the whole mobile device. The risk or this type of attacks is clearly higher with jailbroken/rooted devices.”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

Application

26. **Application Modification/Analysis in Runtime by Malware**

(“...If a mobile device is already infected with malware (e.g. by another malicious installed application or an infected operation system component/module), depending on the user’s privileges, even if the customer’s mobile device has the genuine financial application, it can be susceptible to attacks. As an example, the malware could be injected into the genuine application that might, for instance, result into retrieving sensitive data such as customer keys or credentials or even change the content that the genuine application presents to the customer. Rather than deploying malware to modify an application, an attacker could also directly install the application onto a mobile phone or emulator they control, and then manually modify the execution of the application. This allows the attacker to understand an application. The learnings of which could be exploited as a mass attack deployed through means such as malware...”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

27. **Hijack Genuine App User Interface**

(“...malware on a mobile device can for example hijack the user interface. This attack may require few privileges since it does not need to access the genuine application process information, but can, for example, when a victim opens the genuine application, present a cloned interface, where it could fool the victim into introducing their credentials.“)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

28. **Static Code Analysis**

(“...an attacker can retrieve information about the application or steal data (e.g. cryptographic keys) from the application. This information could be critical given that vulnerabilities may be found. Without access to the original source code, code analysis has to be performed by reverse engineering the application. Applications are often built from “library” components ... If one of those library components was lifted out of the application, it could be used outside the originally intended context. This could allow an attacker to have access to data and services they were not meant to have access to.”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

Communication

29. **Man-in-the-middle**

(“Man-in-the-middle are attacks where, as the name implies, an attacker is in the middle of the communication between the parties independently of the communications type, such as remote or proximity interaction (e.g., in an NFC communication, an attacker can perform such an attack by using a proxy channel between the proximity communications).With these attacks, a customer assumes that he/she is interacting directly with the intended component/service, but the attacker “in the middle” is eavesdropping or changing the information to their benefit...”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

Service Infrastructure

30. **Denial of Service (DoS)**

(“A Denial-of-Service (DoS) attack is an attempt to make a service unavailable to its users for its intended purposes. This can be realised in a number of different ways such as resetting or exhausting its resources, the bandwidth, the processing capacity or the memory. A successful DoS attack directly affects the availability of a network system. From the various forms of attacks, the Distributed Denial-of-Service (DDoS) is the most dangerous, where multiple systems are used to carry out a co-ordinated attack.”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

31. **Data Breach**

(“Data breaches are the intentional or unintentional release of critical information to an untrusted environment. The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data. However, if an unauthorised person views or misuses confidential information, that should also be considered as a form of data breach. Such breaches typically happen due to hacktivism, dissatisfied employees or careless behaviour with confidential data.”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

32. **Compromised Service Provider Servers**

(“A compromised server at a service provider can be very dangerous because it can infect the company itself or their customers through data breaches or malfunctioning operations. If the service provider is the intended target, the attackers can leak sensitive information, impersonate the company or even mess with the lifecycle process of the operations (e.g. change authorisation parameter settings)...”)

Mark only one oval per row.

	1	2	3	4	5
Likelihood	○	○	○	○	○
Impact	○	○	○	○	○

Other threats regarding Mobile Card Emulation Applications

Please indicate your perspective about other possible threats

Other threats - your opinion

33. **If you think there are other threats regarding Mobile Card Emulation Applications that were not presented, please describe them and indicate their Likelihood and Impact values:**

____

____

____

____

____

Additional Information

34. **If you have additional information or suggestions that you think may be relevant for this study please present them in the following text field:**

____

____

____

____

____