Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

MASTER THESIS

TITLE: Analysis and Evaluation of Security Developments in Electronic Payment Methods

MASTERS DEGREE: Master's degree in Applied Telecommunications and Engineering Management (MASTEAM)

AUTHOR: Joshua Iván Mendieta Zurita

ADVISORS: Tomás Perlines, Juan Hernández

DATE: August, 24th 2019

Title: Analysis and Evaluation of Security Developments in Electronic Payment Methods

Author: Joshua Iván Mendieta Zurita

Advisors: Tomás Perlines, Juan Hernández

Date: August 24th, 2019

Abstract

Often it is difficult to understand the level of security inherent in payment card transactions because the amount of information available about the various involved standards and technologies is vast. These technologies and standards were designed, developed and issued by different organizations to protect data used in card payment transactions to counteract the increasing threat that criminals represent with their constant attacks. This thesis assembles a compendium of the technologies and standards used by parties involved in card payments, keeping the focus on the merchant side. The work also creates metrics and uses them to evaluate these technologies and standards. Building on technical documents and standards, the thesis addresses these quesitons: To what extent do these involved technologies provide security for the data used in card payment transactions for the different payment channels? How much effort is required of merchants using self-assessment questionnaires (SAQs) to ensure their compliance with the payment card industry data security standard (PCI DSS)? In this context, SAQs are tools used to determine compliance with PCI DSS.

To achieve these goals it was required to first gather and organize information from the many organizations, elements, processes, technologies and standards involved in the card payment transaction. The separate technologies and SAQs identified were then assigned to their respective payment channels. Quantifiable metrics were developed and then applied to evaluating the features of individual technologies and SAQs. The evaluation results demonstrated that some technologies provide little to no added value to the security of card payments. The results also indicated that the level of effort required of a merchant to comply with PCI DSS is greater when using certaing SAQs. Based on these results, it is recommended to stop supporting magnetic stripes and card verification value version 2 technologies and to replace them with the EMV chip and the three domain secure version 2.0 authentication protocol, respectively. Also, merchants should aim to be eligible for SAQ A and SAQ P2PE versions when seeking to comply with PCI DSS in the different payment channels. Further study is required in the innovation and creation of technologies and rules to strengthen card payments against the constant evolution of criminal activities.

Acknowledgments

First of all, I would like to express my sincere gratitude to the Universitat Politècnica de Catalunya (UPC), for allowing me the privilege of studying, enrolling, and finishing my master's studies with them.

To my advisors, Juan Hernández and Tomás Perlines, and also to my tutor Francesc Tarrés. Without them, I would not have been able to start and finish my master thesis. They helped me enormously on this final journey, and I am grateful to them.

I am also grateful to my teachers, for all the help and knowledge that enriched me during my studies.

On a more personal note, I would like to express my gratitude to my family, especially to my aunt, Grace Mendieta, and my grandmother, Zoila Cáceres, for the help provided during my studies.

Finally, I would like to thank my deceased mother Mónica Zurita and my father Eduardo Mendieta for all the help provided during this time in my life. Without their financial aid, inspiration, and courage, I would not have finished my master's studies. They are the main reason I was able to complete this thesis.

Thank you all from the bottom of my heart.

Joshua Iván Mendieta Zurita

Deo Gratias

CONTENTS

ACRONYMS

3DS	Three-Domain Secure
ACS	Access Control Server
AReq	Authentication Request
ARes	Authentication Response
ASV	Approved Scanning Vendor
ATM	Automated Teller Machine
CA	Certification Authority
CD	Consumer Device
CDA	Combined Dynamic Data Authentication
CD-CVM	Consumer Device Cardholder Verification Method
CNP	Card-not-present
COTS	Commercial Off-the-Shelf
CP	Card-present
CReq	Challenge Requests
CRes	Challenge Response
CSR	Certification Signing Request
CVM	Cardholder Verification Method
CVV	Card Verification Value
DDA	Dynamic Data Authentication
DS	Directory Server
DSS	Data Security Standard
EMV	Europay Mastercard and Visa
EMVCo	Europay Mastercard and Visa Consortium
ENVS	External Network Vulnerability Scan
HCE	Host Card Emulation
HSM	Hardware Security Module
ICC	Integrated Circuit Card
ID&V	Identification and Verification
IIN	Issuer Identification Number
ISO	International Organization for Standardization
LRC	Longitudinal Redundancy Check
LUK	Limited-use Key
MAC	Message Authentication Code
MITM	Man-in-the-middle
MOTO	Mail Order and Telephone Order
MS	Magnetic Stripe
NFC	Near Field Communication
nSCD	Non-Secure Cryptographic Device
P2PE	Point-to-point Encryption
PA-DSS	Payment Application Data Security Standard
PAN	Primary Account Number
PCI	Payment Card Industry
PCI SSC	Payment Card Industry Security Standards Council
PIN	Personal Identification Number
POI	Point of Interaction or card payment terminal
POS	Point of Sale
PSP	Payment Solution Provider

PTS	PIN Transaction Security
RReq	Results Request
RRes	Results Response
SAQ	Self-Assessment Questionnaire
SDA	Static Data Authentication
SDAD	Signed Dynamic Application Data
SDK	Software Development Kit
SSAD	Signed Static Application Data
SUK	Single-Use Key
TLS	Transport Layer Security
TSP	Token Service Provider

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Even to day, obsolete and out-of-date technologies are still used in payment card transactions. To address this situation, it is important to analyze and evaluate of security developments in electronic payment methods to understand how the security of the data used in payment transactions has been improved with advent of newer technologies.

First of all, it is important to provide a brief introduction of the payment card industry, starting with the concept of payment cards. Payment cards are plastic or metal cards that allow the cardholder to make payments at a merchant's premises. This form of payment is known as electronic payment, and such cards are now widely used around the globe and compete with cash-based payments. Due to their broad, global acceptance, criminals have been continually attacking card-based payments.

These attacks, if successful, affect the various entities involved in card payments including, for example, the cardholder, the merchant and the issuer bank. For the cardholder, the criminal using the sensitive account data gathered, as a result of an attack, can perform a type of fraud called identity theft, which repercussions for the cardholder are, for example, the reduction of the total account balance to zero, a great amount of debt and an affected credit score. For the merchant, the criminal buying a good or service using stolen payment card information leads to chargeback initiated by the cardholder, which is the reposition of money to the cardholder leaving the merchant with the loss of the good or service sold to the fraudster. For the issuer bank, the criminal can withdraw money from an automated teller machine using a stolen or cloned payment card, which leads to the bank reimbursing the amount of money withdrawn to the cardholder. As a consequence, organizations and individuals involved in the payment card industry have suffered substantial losses. To counteract fraud, two important organizations were created by the major brands in the payment card industry to set standards and technical specifications. These organizations are the Payment Card Industry Security Standards Council and the Europay Mastercard Visa Consortium. These standards and technologies play a crucial role because they provide security and security rules for all participants in the payment transaction process.

Currently there are many sources of information, technical documents and standards that explain the different elements, procedures and requirements to secure the data used in card payment transactions. Because, this data comes from so many sources, it can be challenging to understand how the technologies and standards involved in the payment card industry provide security during the card payment transaction life cycle. It can be also challenging to find quantifiable metrics to evaluate the various technologies and tools that a merchant can use to comply with the payment card industry data security standard.

After gaining a picture of the current payment landscape, it is important to understand the different roles that each organization involved in this industry has to play to assure the security of transactions. These institutions define concepts, standards and technologies that, when used together, undoubtedly affect the security of the overall process. These organizations can also collaborate to develop new technologies and standards as the need arises in the market.

Another critical point is to understand the payment cards' structure. This is essential because it brings clarity on the number of elements that the payment card possesses, along with the objectives that these elements fulfill. While not all of these elements have a positive impact on the overall card payment transaction life cycle, those elements whose impact is negative are still present, and it is imperative to understand the reasons behind this.

To further understand the card payment transaction process, it is essential to comprehend its life cycle and the different institutions involved. Knowing the participants and their duties helps provide more detailed insight into the process. Additionally, a better comprehension of the channels used for card payments and their processes brings a clearer understanding of the card payment flow.

As mentioned above, there are different technologies and standards commonly used for card payments. It is important to understand the technologies involved in the payment process and the procedures, security mechanisms, and requirements these technologies use to secure payment channels. The standards present an additional security measure apart from the technologies used. It is critical to learn from whom the various types of standards require compliance, the objectives of these standards, and the different tools used to comply with them. In this way, the scope and responsibilities of the different institutions in providing security in the card payment transaction become clearer.

Finally, after gathering and analyzing all the previous information, it is essential to evaluate the involved technologies in the payment process and the involved self-assessment questionnaires used for the compliance of the payment card industry data security standard. This evaluation provides an understanding of the strengths and weaknesses of the card payment security, and answers to two specify questions. The first question being, To what extend do these involved technologies provide security for the data used in card payment transactions for the different payment channels?. And the second question being, How much effort is required of merchants using self-assessment questionnaires to ensure their compliance with the payment card industry data security standard? Different metrics will be defined to objectively evaluate the security of card payments. The evaluation results will be the basis for the recommendations to the involved parties.

To address the above objectives, this thesis has been divided into five chapters:

- Chapter 1 addresses the various organizations that directly or indirectly play a role in the card payment transaction procedures.
- Chapter 2 focuses on the different elements that comprise a payment card and explains the security mechanisms they provide.
- Chapter 3 explains the overall life cycle of the card payment transactions along with the payment channels used.
- Chapter 4 describes the technologies and standards used by the payment card industry to secure the data used in card payments.
- Chapter 5 defines metrics used to evaluate the technologies and standard compliance tools. These metrics are designed to assess the features the technologies offer and the amount of effort required of a merchant using the various payment card industry data security standard compliance tools.

CHAPTER 1. ORGANIZATIONS

This chapter explains the involvement and contribution of the different organizations involved in the card payment transaction process.

In the late 1990s each financial service organization had its own procedures for providing security to transactions carried out with payment card [1]. The absence of a common standard for security procedures for card payment transactions resulted in the growth of fraud losses between the late 1990s and early 2000s [1], which resulted in the creation of the first standards organization in 2006 [2].

In 1999 American Express, Discover, Japan Credit Bureau, MasterCard, UnionPay and Visa formed the Europay Mastercard Visa Consortium (EMVCo), which is an organization in charge of technical specifications for card pyment transactions [3]. Later in 2006 American Express, Discover, Japan Credit Bureau, MasterCard and Visa formed the Payment Card Industry Security Standards Council (PCI SSC), which is an organization in charge of issuing standards for card payment transactions [4]. Both of these organizations play an important role in the security of card payments (see Figure 1.1).

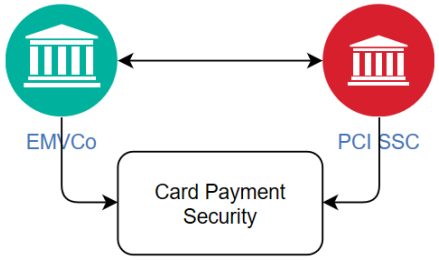

Fig. 1.1 EMVCo and PCI SSC

1.1 International Organization for Standardization (ISO)

Before mentioning the organizations in charge of electronic payments, it is essential to recognize the International Organization for Standardization.

ISO defines various sets of standards; two are of particular interest: ISO 24760 for information technology security and privacy [5], and ISO 27000 for information security management systems [6]. These standards define the following concepts that are important for the understanding of this document.

- Identification: Process of recognizing an entity in a particular domain as distinct from other individuals.
- Authentication: Provision of assurance that a claimed characteristic of an individual is correct.
- Authorization: Process of granting privileges with an understood level of confidence established by a claimed identity.

The requirements and procedures for the technologies and standards studied in this thesis, are developed around the above mentioned core concepts.

1.2 Europay Mastercard Visa Consortium (EMVCo)

EMVCo is a professional body that incorporates globally accepted standards to promote the development of an infrastructure to obtain a consistent, interoperable, and secure payment process. Also, EMVCo communicates with Near Field Communication Forum, GlobalPlatform, Global Systems for Mobile Communications Association, PCI SSC, French Association for Contactless Mobile Services, Asia Pacific Smart Card Association, Advance Card Technology Canada, European Telecommunications Standards Institute, the European Payment Council, Fast Identity Online Alliance, Secure Technology Alliance, the United States Payments Forum, and the World Wide Web Consortium to receive and share perspectives on areas of mutual interest [7].

EMVCo has categorized countries by regions to obtain Europay Mastercard Visa (EMV) chips deployment and adoption statistics. These statistics can be seen in Table 1.1.

Table 1.1 Global deployment and adoption of EMV chip card [8]

	2016		2017		2018	
Region	**EMV Cards**	**Adoption Rate**	**EMV Cards**	**Adoption Rate**	**EMV Cards**	**Adoption Rate**
Africa & the Middle East	184M	68.7%	219M	74.8%	272M	87.8%
Asia Pacific	3,331M	38.8%	4,147M	45.7%	5,001M	51.1%
Canada, Latin America, and the Caribbean	717M	75.7%	820M	85.7%	848M	86.9%
Europe Zone 1	921M	84.9%	939M	84.4%	966M	85.5%
Europe Zone 2	243M	63.7%	276M	71.4%	301M	80.4%
United States	675M	52.2%	785M	58.5%	842M	60.7%

EMVCo's specifications are shown as follows [7]:

- Contact EMV Specification
- Contactless EMV Specification
- Mobile EMV Specification
- EMV Payment Tokenization Specification

- EMV QR Code Specification
- EMV Secure Remote Commerce Specifications
- EMV 2nd Generation Specification
- EMV Three Domain Secure (3DS) Specification

The EMV chip is introduced in section 2.2, and a more detailed view of the EMV chip along with other EMV specifications is given in section 4.1. The information within these sections provides a better understanding of the payment transaction procedure.

1.3 Payment Card Industry Security Standards Council (PCI SSC)

PCI SSC is a global forum that leads a global effort between entities that stores, processes, or transmits sensitive cardholder data, to assure data security.

To correctly implement PCI SSC standards, the Council provides tools such as assessment and scanning qualifications, training and education, product certification programs and self-assessment questionnaires (SAQs) [9]. To learn more about SAQs refer to section 4.2.1.3.

PCI SSC defines the following set of standards [10]:

- Payment Card Industry (PCI) Data Security Standard (DSS)
- PCI Secure Software Standard
- PCI Secure Software Life Cycle Standard
- PCI Payment Application Data Security Standard (PA-DSS)
- PCI Point-to-Point Encryption Standard (P2PE)
- PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Standard
- PCI PTS Point of Interaction (POI) Standard
- PCI Card Production and Provisioning Logical Security Standard
- PCI Card Production and Provisioning Physical Security Standard
- PCI 3DS Core Security Standard
- PCI 3DS Software Development Kit (SDK) Standard
- PCI Personal Identification Number (PIN) Security Standard
- PCI Software-Based PIN Entry on Commercial Off-the-Shelf (COTS) Security Standard
- PCI Software-Based PIN Entry on COTS Test Standard
- PCI Token Service Provicers (TSP) Security Standard

See section 4.2 for a better understanding of the different PCI standards addressed in this document.

1.4 EMVCo and PCI SSC Interaction

EMVCo and PCI SSC collaborate to increase data security and reduce fraud. To achieve these goals, EMVCo, with its EMV chip, maintains the cardholder's sensitive data in encrypted form, while PCI standards specify procedures to keep the data secure through the entire transaction process, as detailed in [11].

In 2017, EMVCo and PCI SSC started a direct collaboration to support the launch of 3DS version 2.0. EMVCo's role was to deliver the EMV 3DS 2.0 specification, while PCI SSC's purpose was to provide security requirements, testing procedures, assessor training, and reporting templates to address the 3DS 2.0 specification [12].

Refer to section 4.1.2 and section 4.2.5 for a more in-depth view of 3DS 2.0.

CHAPTER 2. PAYMENT CARD STRUCTURE

This chapter's objective is to explain the different elements that comprise a payment card.

Payment cards have embedded in their plastic or metal various elements. Each of these elements plays a role in the payment transaction process and can be seen in Figure 2.1 [13]:

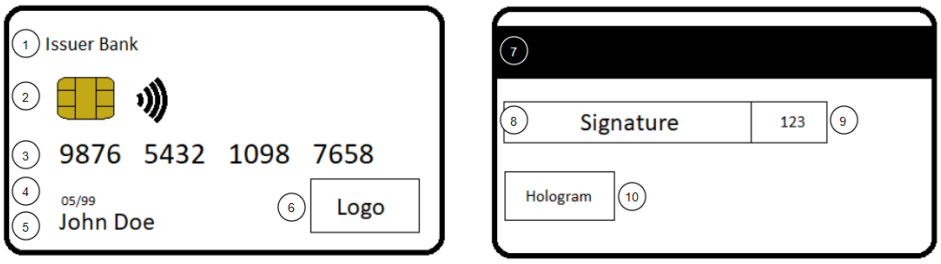

Fig. 2.1 Payment card structure

1. Issuer bank's name
2. EMV chip
3. Primary account number (PAN)
4. Expiration date
5. Cardholder's name
6. Card network logo
7. Magnetic stripe (MS)
8. Cardholder's signature
9. Card verification value (CVV)
10. Security hologram

2.1. Issuer Bank

Issuer banks are financial institutions that offer payment cards, extend credit limits to qualified consumers [14] and provide financial back-up to merchants for transactions made with issued payment cards.

For credit cards, the issuer bank assumes the ability of cardholders to pay their debt when using credit cards. For debit cards, the issuer bank uses the cardholder's balance to pay purchases made with debit cards.

2.2. EMV Chip

EMV Contact and Contactless specifications refer to the form of communication between the integrated circuit card (ICC) and the POI device performs. For EMV Contact, the ICC and the POI need to come into physical contact [15], while in EMV Contactless, the ICC and the POI use near field communication

(NFC) technology and are required to be within sufficient proximity [16] (see Figure 2.2).

The EMV chip improves security in card-present (CP) scenarios with the following features that reduce fraud from counterfeit, loss, and stolen cards [17]:

- Authentication of the chip card: Performed by the POI to distinguish genuine cards from fake or stolen cards.
- Risk management parameters: The issuer defines the conditions under which to conduct offline or online transactions.
- Transaction integrity: This is the result of digitally signing payment data.
- Robust cardholder verification methods: These help to protect against fraud from lost and stolen cards.

The chip uses various cryptographic functions to store the cardholder's sensitive data [18].

Fig. 2.2 Contact and contactless communication between ICC and POI

According to the EMVCo's report from 2018, half of the payment cards issued worldwide are EMV-chip based payment cards [19].

Refer to section 4.1.1 for a more in-depth view of the EMV chip, and refer to section 3.2 and section 3.3 for an explanation of CP and card-not-present (CNP) channels.

2.3. Primary Account Number (PAN)

The PAN identifies the payment card and is used by an issuing bank to determine the origin or destination of a transaction. The PAN's structure is as follows [20]:

- The first six digits identify the card network. These digits are known as the issuer identification number (IIN) or the bank identification number, and contain as its first digit the major industry identifier. The MII identifies the industry that the payment card issuer belongs to.
- The last digit is a check digit used to verify the correct transmission of the PAN during a card payment transaction.

- The digits between the IIN and the check digit identify the cardholder's account.

The Luhn algorithm is used to determine the check digit [21]. Figure 2.3 shows its procedure, followed by an explanation.

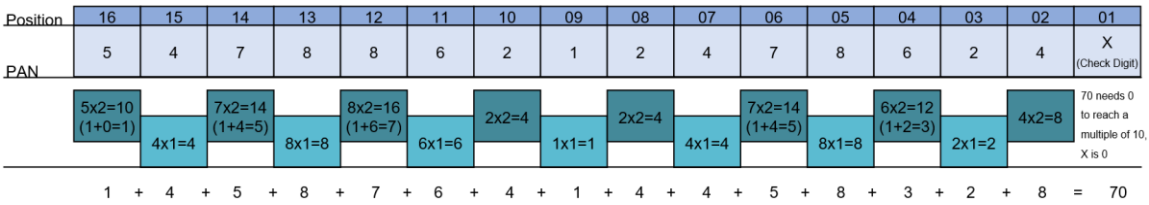

Fig. 2.3 Luhn algorithm process

1. Number each digit from right to left.
2. For even positions multiply by 2 and for odd positions multiply by 1.
    i. If the result of the multiplication is a two-digit number, add the digits together.
3. Add all the results obtained from step 2 together.
4. The check digit is difference between the result from step 3 and the nearest multiple of 10.

The PAN is sensitive data stored within the payment card. To protect it, PCI DSS has defined a maximum number of digits that can be shown on a display so as not to compromise the cardholder. Refer to section 4.2.1.1.

2.4. Expiration Date, Cardholder Name and Card Network

The expiration date allows issuers to replace cards on a timely basis and update the technology of their EMV chips. It is also used to prevent fraud in the CNP payment channel because, without the expiration date, a PAN cannot be used [22].

The cardholder name is the person authorized by the issuer bank to use the payment card. Only authorized individuals can make use of the payment card, and on the CP payment channel, the merchant is required to ask for an identification document before starting the payment card transaction process [23] when using the MS of the payment card.

The card network logo is used to identify the payment card's network. These card networks serve as a backer for institutions such as acquirers and issuers with their respective customers. These institutions are recognizable brands that are in charge of ensuring that transactions are processed correctly, of setting guidelines and qualifications for their member institutions, and of serving as mediators of disputes between parties involved in the transaction process [24].

2.5. Magnetic Stripe (MS)

An MS contains the cardholder's sensitive information stored in the magnetic fields of the band as cleartext. This band is a passive element that is still used to provide compatibility with out-of-date POI models, and is activated by swiping it through a POI [25]. See Figure 2.4.

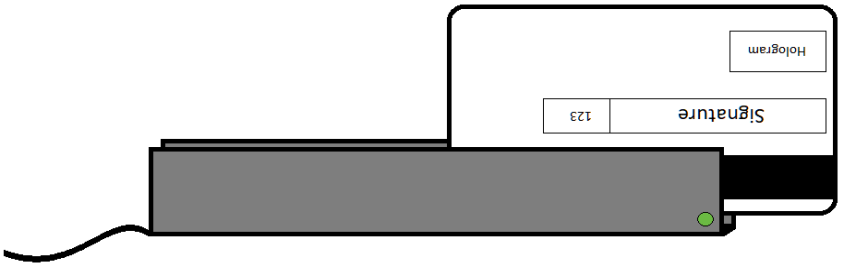

Fig. 2.4 MS card and reading device

This band contains three tracks of information. The first and second track contain the cardholder's PAN and name, the card's expiration date and the country code, and the third track stores additional information. Each track also incorporates a longitudinal redundancy check (LRC) used for error control during the transmission of data from that track [26].

Malicious individuals can target and clone magnetic bands because they hold static information and are easy to manufacture and encode [27]. Cloning requires a third-party electronic device to scan the card before the insertion into a POI. Such a device records the stored information from an MS, then transfers the data to a new card or rewrites it to a stolen card [28].

The European Central Bank in its executive summary of 2018 cites a reduction of fraud from point-of-sale (POS) systems and automated teller machines (ATMs) due to the high adoption rate of EMV chips in POIs, the use of geo-blocking, and the increase of security measures (see Table 2.1).

Table 2.1 European percentages of total fraud attributable to POS, CNP and ATM transactions [29]

Fraud Statistics for different scenarios					
Fraud Scenarios	**2012**	**2013**	**2014**	**2015**	**2016**
POS	23%	19%	19%	20%	19%
CNP	60%	67%	69%	71%	73%
ATM	17%	14%	12%	9%	8%

Refer to section 5.1.1 for an analysis of other technologies compared to the EMV chip.

2.6. Cardholder Signature

This feature is not currently being used by merchants. The idea behind it was to verify the signature of the payment card against the cardholder's ID or driver's license to corroborate the cardholder's identity [30]. With the advent of more robust verification mechanisms, the cardholder's signature has become an outdated security measure for payment cards [31]. As a result, cardholder signature is no longer required or used by American Express, Discover, Mastercard, or Visa since April of 2018 [32].

2.7. Card Verification Value (CVV)

The CVV is a three-digit or four-digit security code used by the issuing bank to verify the payment card. The CVV has evolved and improved over time. Its first version, the CVV1, was encoded in the card's MS. The second version, the CVV2, is used in CNP scenarios. To generate the CVV2, an issuer bank uses secret encryption keys to encrypt the PAN and expiry date [33].

As mentioned in section 1.4, EMVCo and PCI SSC worked together to bring out the 3DS 2.0 specification, which will replace CVV2 with a robust solution as seen in section 4.1.2 and section 4.2.5. An analysis in section 5.2.1 compares CVV2 with 3DS 2.0.

2.8. Security Hologram

Holograms on payment cards are another security mechanism that enables a more secure payment processing at a POS. The attendant at a POS checks the presence of the security hologram. If it is present, it confirms that the presented card is a valid payment card. If it is absent, it is an indication that the presented card might be a fake [34].

The main purpose for security holograms is to prevent forgery, or at least make it difficult. Holograms cannot be scanned or copied on a photocopier and have hidden images or text placed in them to provide immediate authentication and validation [35]. Security holograms many features including covert laser readable images, kinetic images, microtexts, nanotexts, concealed images, guilloche patterns (see Figure 2.5).

- Covert Laser Readable Images: Generated by dot matrix printers, and verified by a laser.
- Kinetic Images: A change in the angle of observation gives the illusion of movement.
- Microtexts: Text embedded in holograms with sizes from 50 to 150 micrometers.
- Nanotexts: Text embedded in holograms, verified by the use of a microscope, and with a size of less than 50 micrometers.

- Concealed Images: Thin lines and contours appear when viewed from a specific angle.
- Guilloche Patterns: A set of complicated geometric patterns that are drawn in high resolution and vary in color at each line.

Fig. 2.5 Security hologram example

CHAPTER 3. PAYMENT CHANNELS

This chapter explains the different payment channels that are used in the payment transaction process.

Payment channels are the forms in which a merchant accepts payments from a customer. There are two types of payment channels: CP and CNP.

3.1. Payment Life Cycle

To gain a fuller understanding of the topic covered in this thesis, it is essential to address the life cycle of a payment process and the involved entities (see Figure 3.1).

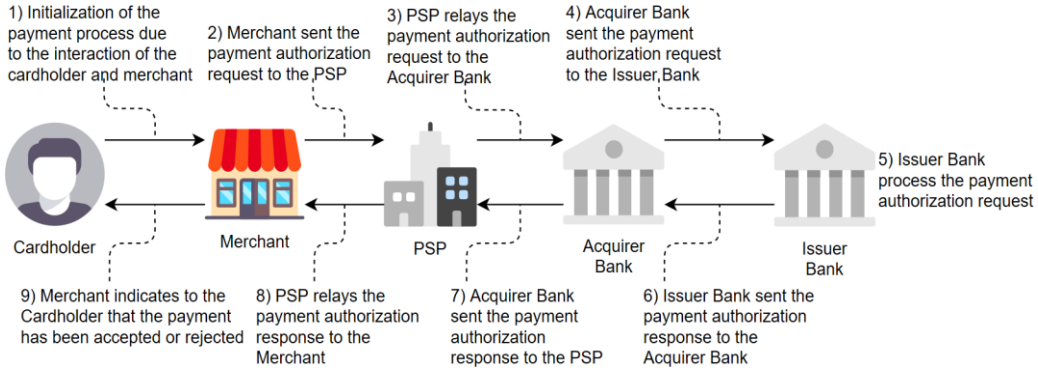

Fig. 3.1 Payment process life cycle

The different entities involved are defined [36] below:

- Cardholder: The cardholder is the person to whom the issuer bank issues the payment card; in other words, this is the owner of the payment card.
- Merchant: A merchant is any entity that has accepted a payment card as a form of payment for its goods or services.
- Payment Solution Provider (PSP): Also known as the payment network, the PSP is the entity in charge of connecting the merchant with various acquirer banks and card networks.
- Issuer Bank: An issuer bank is a financial institution that issues payment cards and offers other services to its consumers (see section 2.1).
- Acquirer Bank: An acquirer bank is a financial entity that in support of the merchant handles payments done with payment cards.

It is essential to define the elements used to process payment transactions:

- ICC: A plastic card with an embedded circuit used to control access to a resource or service [37].
- POI: Hardware component that permits purchases with payment cards [38].

- POS: The location a customer initialize a card payment [39].

Another term used often in this document is the PIN, which is an identifying number assigned by the issuer to the cardholder and which is used to authenticate the cardholder before a transaction [40] in the CP channel.

3.2. Card-Present (CP)

A CP transaction occurs when the cardholder is physically present at the merchant's facilities [41]. This type of payment channel uses the MS (see section 2.5) or the EMV chip (see section 2.2) technologies to start the payment process. In the CP channel, EMV uses different cardholder verification methods, mentioned in section 4.1.1.2.

In Figure 3.2, an overall view of the CP channel is presented.

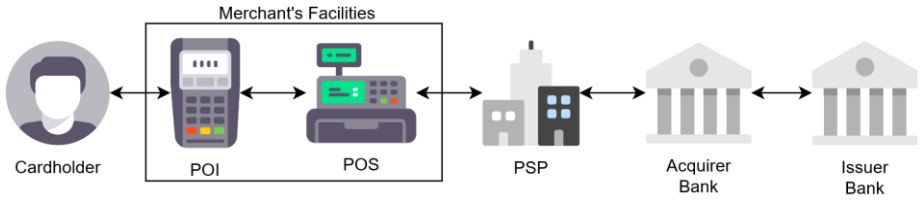

Fig. 3.2 Card-present channel

3.3. Card-Not-Present (CNP)

A CNP transaction occurs when the cardholder is not physically present at the merchant's facilities [42]. A CNP transaction can be performed through the merchant's application or website or by mail order and telephone order (MOTO). A scheme for this channel is presented in Figure 3.3.

These types of payment channels are more susceptible to fraud due to the physical absence of the cardholder during the transaction [43] and the challenge to clearly authenticate the legitimate cardholder. To address these problems, as mentioned in section 1.4, EMVCo and PCI SSC delivered the 3DS 2.0 specification. For more information, refer to section 4.1.2 and section 4.2.5.

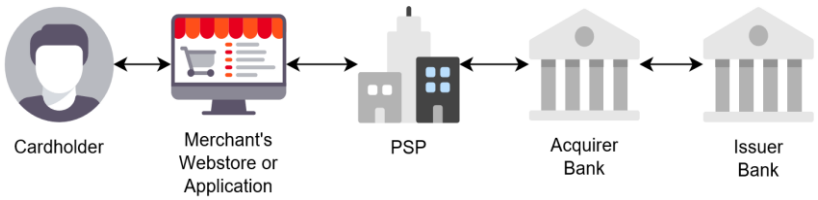

Fig. 3.3 Card-not-present channel

CHAPTER 4: INVOLVED STANDARDS

This chapter provides a description of some specifications and standards involved in the card payment transaction.

As illustrated in Figure 4.1, EMVCo and PCI SSC have defined various specifications and standards to secure the payment transaction process.

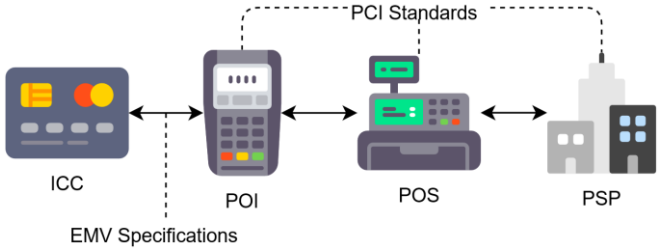

Fig. 4.1 Standards' scope in the transaction process

4.1. EMV Specifications

As mentioned in section 1.2, EMVCo specifications, seek to achieve interoperability by defining requirements and enabling secure payments. To this end, this section addresses the following EMV specifications:

- Contact and contactless EMV specifications
- EMV 3DS version 2.0 specification
- EMV payment tokenization specification

4.1.1. EMV Contact and Contactless Specification

The main objective is to secure payment transactions in the CP channel initialized by contact or contactless interaction between the ICC and the POI. In the contactless specification, the payment brands define their procedure, while in the contact specification, EMV has defined the process shown in Figure 4.2. To learn more about the transaction procedure of the EMV contact specifications, refer to [44] and [45].

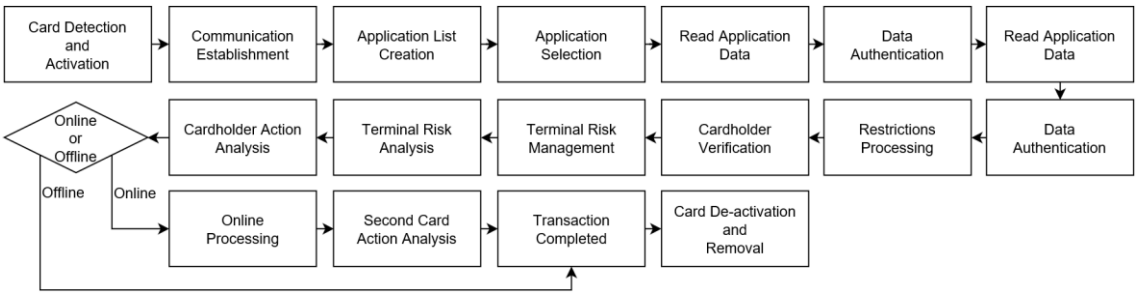

Fig. 4.2 EMV contact transaction process

Additionally, the EMV chip introduces a message authentication code (MAC) so that issuer banks can verify the integrity and authenticity of the transmitted messages [46].

4.1.1.1. Authentication Methods

The EMV chip performs data authentication [47], as seen in Figure 4.2, to ensure the authenticity of the payment card, which is achieved by one of the following means:

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

4.1.1.1.1. Static Data Authentication

SDA is independent of the actual transaction, making it susceptible to replay attacks [48], which occur when the transmitted data is maliciously delayed or retransmitted. The SDA procedure is shown in Figure 4.3, followed by an explanation.

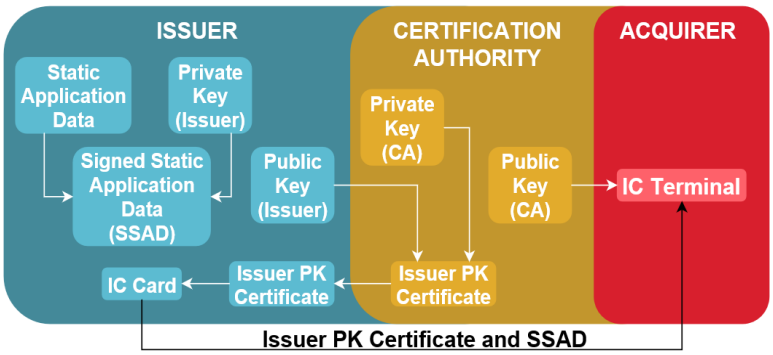

Fig. 4.3 Static data authentication procedure

ICC Issuance:

1. Issuer generates a key pair, then stores the private key in the ICC and sends the public key inside a certificate signing request (CSR) to a certification authority (CA).
2. The CA signs and sends back the received CSR, producing a certificate for the issuer. The issuer then stores the certificate in the ICC.

Payment Process:

1. The ICC signs the stored static application data with the issuer's private key. This produces signed static application data (SSAD), which the ICC transmits along with the issuer certificate to the POI.
2. The POI verifies the CA signature of the issuer certificate using the CA public key.

3. Finally, the POI verifies the received SSAD using the issuer's public key extracted from the issuer certificate.

4.1.1.1.2. Dynamic Data Authentication

Unlike SDA, DDA prevents replay attacks, although it is susceptible to man-in-the-middle (MITM) attacks directed at the communication between the ICC and the POI [49]. Its procedure is shown in Figure 4.4, followed by an explanation.

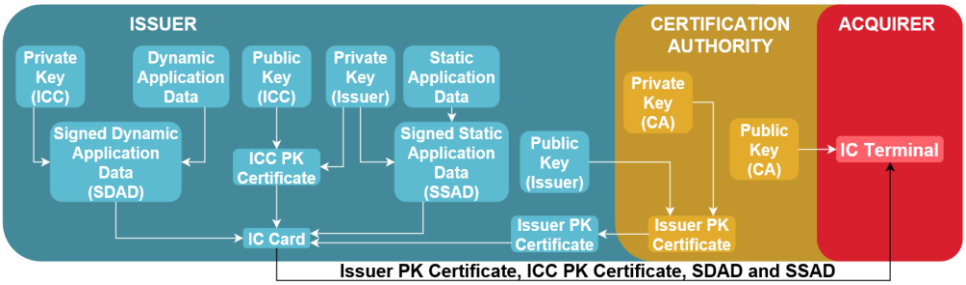

Fig. 4.4 Dynamic data authentication procedure

ICC Issuance:

1. Issuer generates a key pair, then stores the private key in the ICC and sends the public key inside a CSR to a CA.
2. The CA signs and sends back the received CSR producing a certificate for the issuer. The issuer then stores the certificate in the ICC.
3. Issuer generates a key pair for the ICC, then stores the private key in the ICC and produces a CSR with the public key.
4. The issuer signs the CSR producing a certificate then stores the certificate in the ICC.

Payment Process:

1. The ICC generates an SSAD file.
2. The ICC signs the dynamic application data (SDAD) using its private key. This dynamic application data is a random number generated by the terminal for each new EMV transaction.
3. The ICC sends the issuer's and ICC's certificates, the SSAD and the SDAD during the communication with the POI.
4. The POI verifies the issuer's certificate using the CA's public key.
5. The POI verifies the SSAD with the issuer's public key extracted from the issuer's certificate.
6. The POI verifies the ICC's certificate with the issuer's pubic key extracted from the issuer's certificate.
7. Finally, the POI verifies the SDAD with the ICC's public key extracted from the ICC's certificate.

The dynamic data is comprised by data generated or stored in the ICC, and a dynamic number. This dynamic number is an ICC-generated time-variant parameter.

4.1.1.1.3. Combined Dynamic Data Authentication

In addition to the DDA steps, the ICC uses a second dynamic signature, which contains the ICC decision of the current transaction that the POI must verify, thus preventing MITM attacks.

Furthermore, CDA has a PIN encipherment option that uses an additional key-pair associated exclusively with PIN encipherment. The POI uses the public key to encipher the PIN while the ICC uses the private key to verify the PIN [47].

4.1.1.2. Cardholder Verification Methods (CVMs)

The EMV chip uses several CVMs [47], as seen in Figure 4.2 of section 4.1.1, to verify the identity of the cardholder:

- Offline PIN Processing
- Online PIN Processing
- Signature Processing
- Combination CVMs
- Consumer Device Cardholder Verification Method (CD-CVM)

4.1.1.2.1. Offline PIN Processing

The offline PIN is used only if the online PIN processing is not working. The procedure is explained below and shown in Figure 4.5 [50]:

1. The cardholder enters the PIN into the POI.
2. The POI transmits the PIN to the ICC in plaintext or enciphered.
3. The ICC compares the received PIN to its stored PIN.
4. The ICC sends to the POI a yes or no answer depending on the comparison.
5. The POI shows to the cardholder the results of the PIN validation.

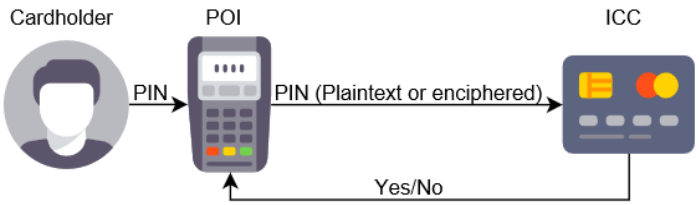

Fig. 4.5 Offline PIN procedure

4.1.1.2.2. Online PIN Processing

The online PIN procedure is explained below and shown in Figure 4.6 [51]:

1. The cardholder enters the PIN into the POI.

2. The POI sends to the PSP the PIN along with the PAN and other sensitive data.
3. The PSP relays the received information to the acquirer bank.
4. The acquirer bank checks the IIN to transmit the received information to the corresponding issuer bank.
5. The issuer receives the transmitted information and validates the PIN.
6. The issuer sends back to the POI a “yes” or “no” response depending on the validation. This PIN validation results passes through the acquirer bank and the PSP.
7. The POI shows to the cardholder the results of the PIN validation.

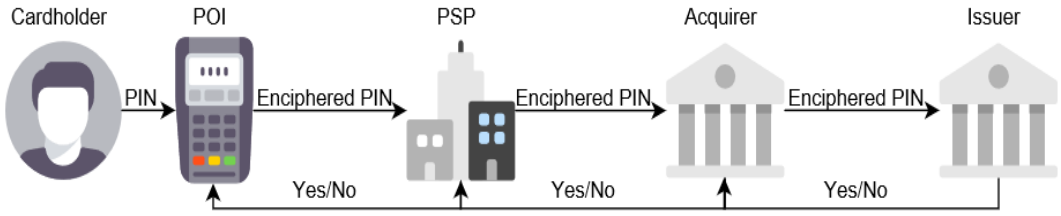

Fig. 4.6 Online PIN procedure

4.1.1.2.3. Signature Processing and Combination CVMs

The POI performs the signature processing, which completes the cardholder verification process [47]. In the combination CVMs, multiple CVMs must be successfully completed.

4.1.1.2.4. Consumer Device CVM

This type of CVM is used for mobile payments, and its main focus is to verify the identity of the person presenting a consumer device (CD). For that, this method uses platform authenticators and relying applications [52].

- Platform Authenticators: Mechanisms provided by an underlying device that used by a consumer to unlock the device using, for example, passcodes, passwords, facial recognition, or fingerprints.
- Relying Applications: Device applications that require information about the authentication of the consumer.

There are three evaluation levels used in CD-CVM solutions [52]:

- Device-level: Captures authentication data with platform authenticators and sends this data to the relying application.
- Operating system level: Implements authentication mechanisms using application programming interfaces.
- Application-level: Relies on the security functionalities provided by the device and mobile application.

4.1.2. EMV Three Domain Secure 2.0 (3DS 2.0)

EMVCo designed, developed, and standardized 3DS (see section 1.4) for the CNP channel [53] to replace CVV2, which was deemed an unsecured authentication method (see section 2.7).

4.1.2.1. Overview

Version 2.0 of the EMV 3DS has been developed to address problems with EMV 3DS 1.0, which included its lack of support for applications other than web browsers, its complicated payment process, and its vulnerability to phishing and MITM attacks [54].

This specification includes three domains: the acquirer, the interoperability, and the issuer domains. The acquirer domain gathers the cardholders' information. Then the interoperability domain transfers information between the acquirer domain and the issuer domain. Finally, the issuer domain performs the verification and authentication of the cardholder.

EMV 3DS 2.0 defines three cases for authentication initialization:

- App-based: A CD uses a 3DS requestor application integrated with a 3DS SDK to initiate a transaction.
- Browser-based: A CD using a browser accesses a website for transaction initialization.
- 3DS requestor: The 3DS requestor initializes the confirmation of account information and the authentication of the cardholder.

4.1.2.2. Security Requirements

The following requirements are in place to ensure payment security [55].

For links between the 3DS elements, the requirements are mutual authentication methods and transport layer security protocol communications.

For app-based authentication channel security functions, the requirements are authentication of the 3DS requestor application, encryption of the 3DS SDK data and Diffie-Hellman, which is a method to securely exchange cryptographic keys over an unreliable channel [56].

4.1.2.3. Authentication Flows

There are two types of authentication flows used by 3DS 2.0–the frictionless and the challenge, as seen in Figures 4.7 and 4.8 [55]. The different types of messages used by these two authentication flows are detailed within Annex A.

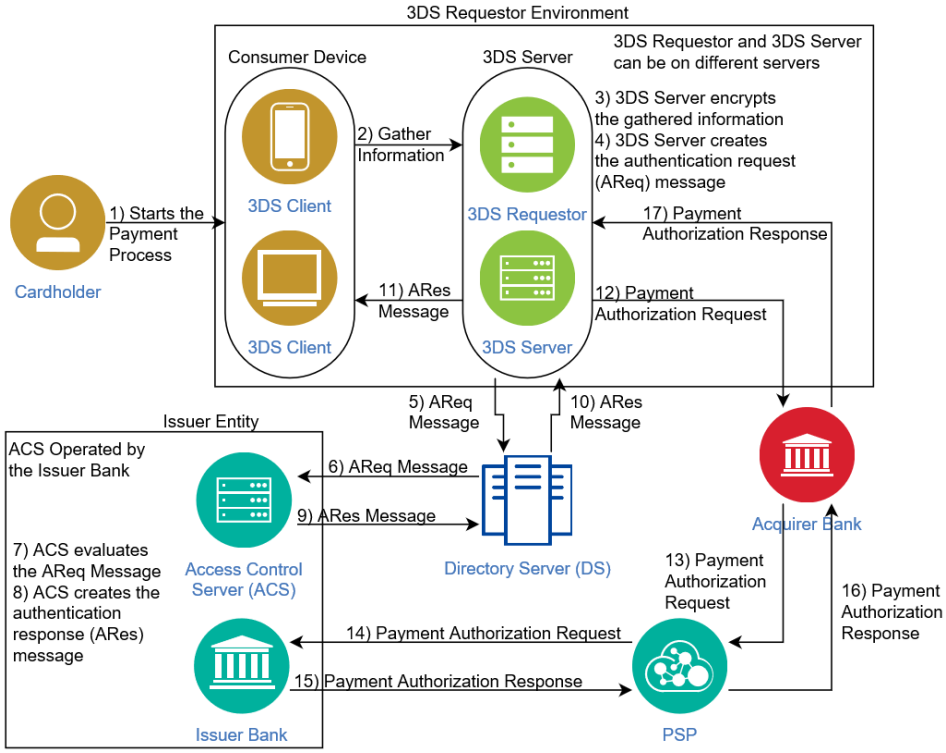

Fig. 4.7 Frictionless authentication flow

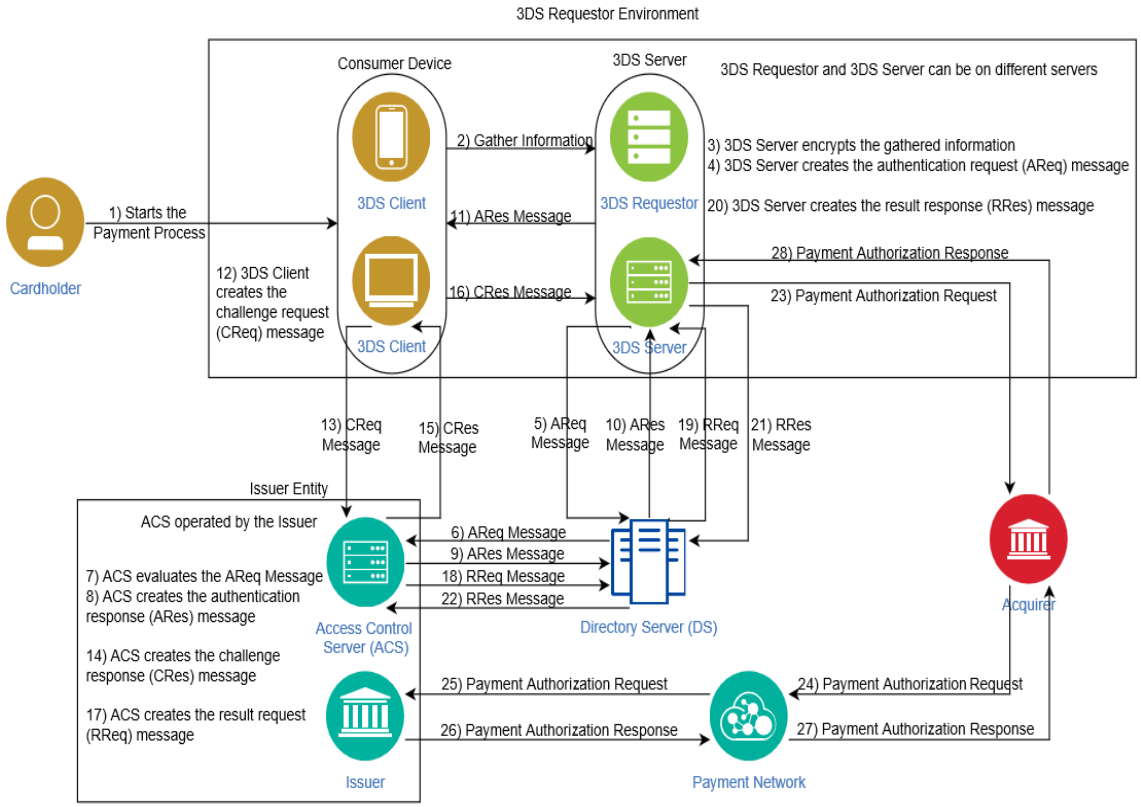

Fig. 4.8 Challenge authentication flow

4.1.3. EMV Payment Tokenization

The EMV payment tokenization specification is used in CP and CNP channels. This specification seeks to reduce risk and fraud. Its procedure can be seen in Figure 4.9 [57]. Each token generated is specific to the combination of a cardholder's PAN, the token requestor and the initially determined environment. Thus, a cardholder's PAN can have multiple tokens associated with it. To comply with regulatory requirements and to allow for a risk analysis, each token can be linked with a PAN using a payment account reference.

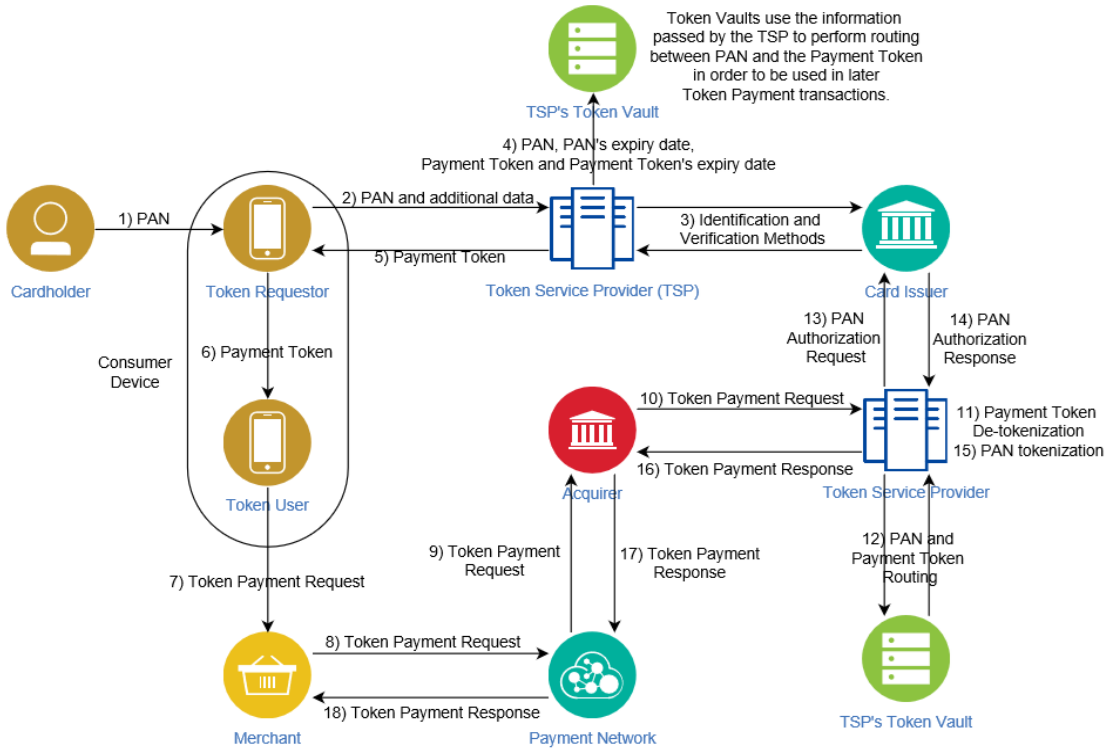

Fig. 4.9 Tokenization procedure

4.1.3.1. Identification and Verification (ID&V) Methods

ID&V methods are used to authenticate the cardholder before issuing a payment token.

To better understand the cardholder verification methods of the EMV payment tokenization specification, it is important to define the term authentication factor. An authentication factor is a procedure or piece of information used to authenticate the identity of a person. These authentications factors are something-you-know, something-you-are or something-you-have [58].

- Something-you-are: This authentication factor aims to authenticate the inherent traits of a person, which can be achieved by using, for example, biometrics, an iris pattern or a fingerprint.

- Something-you-know: This authentication factor aims to authenticate the information a person knows, which can be, for example, a password, or a user name.
- Something-you-have: This authentication factor aims to authenticate a possession of a person, which can be, for example, a smart card or a security token.

Tokenization uses various cardholder verification methods [57]. This specification also uses 3DS 2.0 (see section 4.1.2).

- Risk-oriented non-interactive cardholder authentication: Performs a risk-oriented assessment with data maintained and provided by a token requestor.
- Card-issuer asserted authentication: The card issuer assures that an issuer's approved authentication method is sufficient
- Card-issuer account verification: The issuer performs account verification.
- One-factor authentication: This uses only a something-you-know or something-you-have authentication factor.
- Two-factor authentication: Uses two out of the three authentication types, which are something-you-know, something-you-are, or something-you-have.

4.1.3.2. Use Cases

Google Pay service and Apple Pay service are using tokenization to transact payments more securely.

In the case of Google Pay, the cardholder's CD has a token assigned to it and stores an encryption key. This encryption key decrypts limited-use keys (LUKs) and single-use keys (SUKs) [59]. Finally, the TSP uses the LUKs and SUKs to link the token with the cardholder's PAN and to validate the token [60].

Along with tokenization, for Google Pay also uses host card emulation (HCE). HCE is a technology used to emulate a payment card that can communicate with a POI via an NFC chip. Since the host device is not secure, HCE uses different payment data for each transaction and transaction cryptograms [61].

For Apple Pay, the cardholder's CD has a token assigned to it, and its CD secure element stores this token near the NFC chip [62]. Then the token, token key, transaction amount, and other required information are used to generate a dynamic cryptogram after each transaction. Finally, the TSP uses the token to validate the token inside the dynamic cryptogram [63].

4.2. PCI Standards

As mentioned in section 1.3, PCI's standards provide requirements for securing data in the card payment transaction process. Figure 4.10 shows the PCI SSC standards this document addresses and their scope.

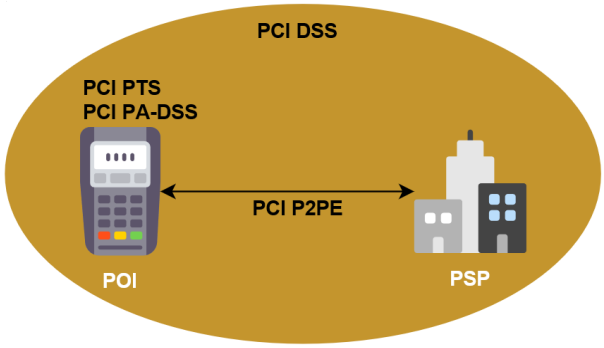

Fig. 4.10 PCI standards' scope

4.2.1. PCI Data Security Standard (PCI DSS)

PCI DSS defines requirements for all entities processing, transmitting, or storing cardholder data, including merchants. These requirements were designed to protect account data and to facilitate global adoption of data security measures [64].

4.2.1.1. Overview

For merchants, the payment brands have defined four compliance levels (see Table 4.1). These levels depend on the number of transactions per year that a business processes with payment cards. These compliance levels specify the validation methods an enterprise needs to meet to remain compliant [65].

- Level 1 entities: Undergo a yearly internal audit by an accredited PCI auditor. Additionally, once a quarter, they must have an external network vulnerability scan (ENVS) performed by an approved scanning vendor (ASV).
- Level 2, level 3, and level 4 entities: Yearly completion of a relevant SAQ. Additionally, a business may be required to have an ENVS performed by an ASV.

Table 4.1 PCI DSS enterprise compliance levels

PCI DSS Compliance Levels	
Level 1	More than 6M transactions per year
Level 2	Between 1M and 6M transactions per year
Level 3	Between 20K and 1M transactions per year
Level 4	Fewer than 20K transactions per year

PCI DSS divides account data into cardholder data and sensitive authentication data [64] (see Table 4.2). Cardholder data can be stored in devices, except for the PAN, which needs to be stored as unreadable, while sensitive account data cannot be stored in devices.

Table 4.2 PCI DSS account data categorization

		Data Element	Storage Permitted
Account Data	**Cardholder Data**	PAN	Yes (unreadable)
		Cardholder Name	Yes
		Service Code	Yes
		Expiration Date	Yes
	Sensitive Authentication Data	Full Track Data	No
		CVV2	No
		PIN	No

This standard specifies that if the PAN is to be displayed, then it needs to be masked unless a merchant has a specific need to show the full PAN. Masking refers to hiding a portion of the PAN's digits when it is displayed or printed. As mentioned in section 2.3, PCI DSS defines the first six and last four digits as the maximum PAN digits that need not to be masked [66].

In the case of PAN storage, the standard specifies that the merchant should perform one of the following procedures [64]:

- One-way hashing: Uses a one-way mathematical function that uses the PAN as input and produces a fixed-length output called a message digest. This message digest is non-reversible.
- Truncation: Removes a portion of the PAN permanently.
- Index tokenization: Replacement of the PAN with an unpredictable value using an index as an input.
- Encryption: Transforms the PAN into an unintelligible form that requires a specific key to be reverted to the PAN again. This method requires the association of key-management processes and procedures.

4.2.1.2. Main Goals

In general, PCI DSS defines six goals that are achieved by the fulfillment of the standard's requirements.

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

To learn more about the rationales behind these goals, refer to Annex B.

4.2.1.3. Self-Assessment Questionnaires (SAQ)

SAQs are self-evaluation tools merchants use to confirm they are compliant with PCI DSS. PCI SSC defines multiple SAQs [67], which are listed in Table 4.3. For more information, refer to Annex C. Refer to section 5.1.2 and section 5.2.2 for an evaluation of SAQs for CP and CNP channels.

Table 4.3 Types of SAQs per payment channel

SAQs for PCI DSS compliance	
CP	**CNP**
P2PE	A
	A-EP (e-commerce)
D	D (e-commerce)
B	B (MOTO)
B-IP	B-IP (MOTO)
C-VT	C-VT (MOTO)
C	C (MOTO)

4.2.2. PCI Point-to-Point Encryption (PCI P2PE)

PCI P2PE is a set of security requirements for encryption solution providers to validate their work and ensure the protection of sensitive authentication data and the cardholder's data by encrypting them before transmission [69] in the CP channel.

4.2.2.1. Environment and Decryption Types

PCI P2PE defines different environments [70]: the encryption environment, the decryption environment, key-injection facilities, and the cardholder data environment. These environments are defined as follows.

- Encryption environment: This environment is located on the merchant's side and contains PCI-approved POI devices used for the acceptance and encryption of account data.
- Decryption environment: This environment is at the P2PE solutions provider. It contains the HSM used to decrypt the encrypted account data sent by the encryption environment.
- Key-injection facilities: This environment is located either at the component provider or at the P2PE solutions provider. These key-injection facilities inject keys both at the PCI-approved POI devices to perform encryption and at the P2PE solutions provider's HSM to perform decryption.
- Cardholder data environment: This environment includes the people, processes, and technologies, that handle cardholder data and sensitive data authentication.

Furthermore, PCI P2PE performs two types of decryption: hardware decryption and hybrid decryption [69].

- Hardware decryption: The HSMs perform the decryption of account data.
- Hybrid decryption: The decryption of account data is performed by the HSM and by a non-secure cryptographic device (nSCD) host system.

4.2.2.2. Domain Types

PCI P2PE applies to several domains, as shown in Table 4.4. These domains constitute regions where security needs to be applied and validated [69].

Table 4.4 PCI P2PE domains and responsibilities

PCI P2PE Domains	
Domain Name	**Summary**
Encryption Device and Application Management	Covers the usage of secure PCI-approved POI devices, P2PE applications, and P2PE non-payment software. This domain's requirements include the review, installation, and configuration of P2PE applications and P2PE non-payment software.
Application Security	This domain includes the secure payment applications with access to clear-text account data that are installed only on PCI-approved POI devices.
P2PE Solution Management	This domains includes providers of the various devices, products, and environments that consist of a P2PE solution, and the provisioning of a P2PE instruction manual.
Merchant–Managed Solutions	The merchants manage the P2PE solution, in which the encryption and decryption environment duties and functions are separated.
Decryption Environment	This environment covers the secure management of HSMs and nSCD host systems involved in the decryption of encrypted account data.
P2PE Cryptographic Key Operations and Device Management	Responsible for the requirements for strong-cryptographic keys and secure-management functions for all PCI-approved POI devices, HSMs, and nSCD host systems.

4.2.2.3. Procedure

Figure 4.11 summarizes the procedure that PCI P2PE follows. It is important to note that whether the merchant is perfoming the P2PE internally or having a third-party provider perform the service the procedure remains the same [69].

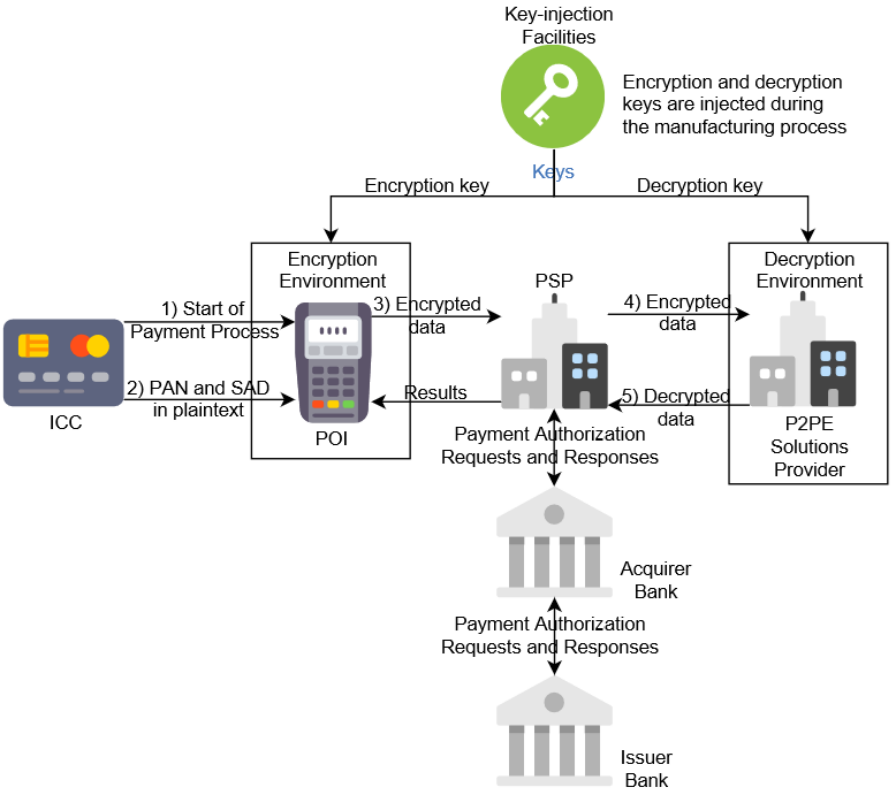

Fig. 4.11 PCI P2PE procedure

4.2.3. PCI Payment Application Data Security Standard (PCI PA-DSS)

PCI PA-DSS is a set of security requirements intended for off-the-shelf applications. This standard is imposed on payment application software vendors to minimize sensitive data leaks from the payment application during the transaction process [71]. Although this standard originated from PCI DSS, the fact that an entity uses a PCI PA-DSS application does not imply full PCI DSS compliance.

PCI PA-DSS states six main goals to protect cardholder data used in the payment application. Some of these goals are shared with PCI DSS [71].

- Manufacture and maintain a secure payment application
- Implement strong access control and monitoring
- Provide easy and secure integration and remote access
- Protect cardholder data
- Secure network connectivity before transmission of data
- Ensure easy implementation, governance and maintenance of PA-DSS

4.2.4. PCI PIN Transaction Security (PCI PTS)

PCI PTS covers the PCI PTS HSM and the PCI PTS POI. These standards are a set of security requirements, guidelines and testing procedures manufacturers and vendors must meet to satisfy the needs of the financial payment industry by assuring the security of the HSMs and POIs from manufacturing to the initial deployment location. The aligned goals of these standards are these:

- To ensure the security of devices at a physical and logical level to protect and guarantee the safety of sensitive data and cryptographic keys.
- To ensure the secure manufacturing and deployment of devices.

Each of these standards targets different objectives. For example, PCI PTS HSM targets the secure handling of cryptographic keys to securely perform remote administration. PCI PTS POI targets the integration of the POI into the POS terminal, the configuration and maintenance of the device and the requirements needed to secure reading and exchange of data.

When a merchant is pursuing the fulfillment of PCI DSS compliance, one of the requirements is that the POIs used by the merchant must be PCI PTS POI compliant. In contrast, the HSMs may be validated with either the PCI PTS HSM or the federal information processing standard 140-2. See [72] and [73] for more information.

4.2.5. PCI Three Domain Secure (PCI 3DS)

PCI 3DS 1.0 defines the requirements, controls, and security measures needed to protect 3DS environments. This standard acts as a security guideline, and the decision to require it is made by the card payment brands.

As seen in section 1.4, PCI SSC collaborated on the publication of the PCI 3DS Core Security and PCI 3DS SDK Security Standards. These standards address the different components that are involved in the EMV 3DS 2.0 specification, as seen in section 4.1.2.

The PCI 3DS Core Security Standard addresses all the security requirements, methods and processes that an entity needs to ensure protection and security of the 3DS server, 3DS Directory Server (DS) and 3DS Access Control Server (ACS).

The PCI 3DS SDK Security Standard covers specific 3DS data elements that play a role in the 3DS 2.0 transaction process and specifies the type of protection that each of these elements requires, which can be to ensure confidentiality, integrity or both. For more information, refer to [74] and [75].

CHAPTER 5. EVALUATION

This chapter presents the concepts used for the creation of the evaluation metrics, the reasoning behind the metric value assignments, and the evaluation results, which are used to provide recommendations for each payment channel.

Building on the presentation of various technologies and standards in previous chapters, this chapter evaluates two main topics. The first topic is about those technologies with the greatest impact on the security of payment transactions today. The second topic is about the amount of effort required of merchants to comply with PCI DSS. For these two topics, each payment channel (see chapter 3) has its corresponding assigned technologies and SAQs.

The metrics presented in this chapter have been created by the author based on the characteristics of each technology and standard compliance tool. The goal is to assign quantifiable values to each of these characteristics and to use these values for evaluation purposes.

5.1. Card-Present Scenario

In the CP channel (see section 3.2) there are two technologies involved in the payment transaction process in today's payment card structure: the MS (see section 2.5) and the EMV chip (see section 2.2 and section 4.1.1). This section also focuses on the SAQ B-IP and the SAQ P2PE (see section 4.2.1.3), each with different requirements that merchants need to meet to comply with PCI DSS.

5.1.1. Technology

This section's objective is to evaluate the overall security of the EMV chip and MS technologies. First, it is important to define metrics to indicate quantifiable value for evaluation purposes. With that in mind, five metrics have been selected: confidentiality, integrity, authentication, data type, and attack resistance.

- Confidentiality: This is the assurance that data is accessed only by authorized entities.
- Integrity: This is the assurance that data has not been altered in transmission, from its creation to its delivery, and the assurance that only authorized entities can modify that data.
- Authentication: This is the assurance that a claimed characteristic of an individual is correct (see section 1.1).
- Data type: This defines the character of the data used by a technology, which can be static or dynamic.

- Attack resistance: This defines the ability of the technology to withstand attacks from criminals.

For the metric “confidentiality,” the assessment is done with one of two values.

- Value -1: If the technology lacks the metric.
- Value 0: If the technology possesses the metric.

The metric “integrity” is assessed on a scale of three values.

- Value -1: If the technology lacks the metric.
- Value 0: If the technology possesses the metric with the attribute “weak.”
- Value +1: If the technology possesses the metric with the attribute “strong.”

The metric “authentication” is assessed with two values.

- Value -1: If the technology lacks the metric.
- Value 0: If the technology possesses the metric.

The metric “data type” is assessed with two values.

- Value 0: If the technology uses static data.
- Value +1: If the technology uses dynamic data.

The metric “attack resistance” is assessed on a scale of three values.

- Value -1: If the technology lacks the metric.
- Value 0: If the technology possesses the metric with the attribute “low.”
- Value +1: If the technology possesses the metric with the attribute “high.”

Below is the evaluation of these technologies against each of these five metrics.

For the EMV chip:

- Confidentiality is achieved due to the encrypted data stored inside the ICC, which can only be decrypted by the POI using the appropriate decryption-key.
- Strong integrity is achieved by the issuer, with MACs to assure the validity and authenticity of the message, as discussed in section 4.1.1.
- Authentication is achieved due to the various authentication methods, as discussed in section 4.1.1.1.
- The data type is dynamic, as the chip uses dynamic data for authentication and transaction procedures.
- High attack resistance is intrinsic to the EMV chip due to the many authentication, verification, and security mechanisms that this technology possesses. These make it extremely hard to attack by, for example, cloning.

For the MS:

- Absence of confidentiality is due to the use of plain text data stored within the tracks of the MS.
- Integrity is weak because the LRC only checks transmission errors.
- Authentication is absent due to the lack of authentication mechanisms.
- The data type is static as a result of the limitations of the technology.
- The MS has low attack resistance given its lack of confidentiality and authentication mechanisms, along with weak integrity and the type of data it uses. Given its technical limitations, the MS is easily attacked by, for example, cloning.

Table 5.1 shows the assigned metric values for the technologies evaluated above.

Table 5.1 CP technology evaluation scores

Technology			
EMV Chip	**Value**	**MS**	**Value**
Confidentiality	0	No confidentiality	-1
Strong integrity	+1	Weak integrity	0
Authentication	0	No authentication	-1
Data type is dynamic	+1	Data type is static	0
High attack resistance	+1	Low attack resistance	0
Overall Score	+3	**Overall Score**	-2

5.1.2. PCI DSS Compliance

The objective of this section is to evaluate the level of overall effort required of merchants for compliance with PCI DSS using either SAQ P2PE or SAQ B-IP. Three metrics have been selected: number of applicable PCI DSS requirements, number of questions to be assessed, and applicable scope of systems.

- Number of applicable PCI DSS requirements: This metric provides the number of requirements a merchant must meet to be in compliance when using a specific SAQ.
- Number of questions to be assessed: This metric provides, for a specific, SAQ the number of questions that a merchant needs to assess.
- Applicable scope of systems: This metric provides a clear and defined scope for what an SAQ evaluates.

For the metric “number of applicable PCI DSS requirements,” since PCI DSS includes 12 requirements, four possible values have been defined.

- Value 1: If the number of requirements is less than or equal to 3.
- Value 2: If the number of requirements is 4–6.
- Value 3: If the number of requirements is 7–9.

- Value 4: If the number of requirements is 10–12.

The metric “number of questions to be assessed” is assessed on a scale of four values, since the maximum number of questions an SAQ can have is unknown.

- Value 1: If the number of questions assessed is less than or equal to 50.
- Value 2: If the number of questions assessed is 51–100.
- Value 3: If the number of questions assessed is 101–150.
- Value 4: If the number of questions assessed is greater than 150.

The metric “applicable scope of systems” is assessed with one of two values.

- Value 1: If the SAQ clearly specifies which network devices the merchant must configure for PCI DSS compliance and if the number of network devices a merchant needs to configure is low.
- Value 2: If the SAQ does not specify which network devices the merchant must configure for PCI DSS compliance and if the number of network devices a merchants needs to configure is high.

Table 5.2 lists the assigned metric values for the two evaluated SAQs.

Table 5.2 CP SAQ evaluation scores

SAQ Metrics			
SAQ P2PE	**Value**	**SAQ B-IP**	**Value**
3 applicable PCI DSS requirements	1	10 applicable PCI DSS requirements	4
33 questions to be assessed	1	82 questions to be assessed	2
Reduced and clear scope of systems	1	Extensive and unclear scope of systems	2
Overall Score	3	**Overall Score**	8

5.1.3. Results

Based on the results from section 5.1.1 and section 5.1.2, the final results for security and effort in CP scenarios can be seen in Figure 5.1. These results suggest the preferred scenario for a CP channel for electronic payments is to use the EMV chip and SAQ P2PE for their high level of security and low level of required effort.

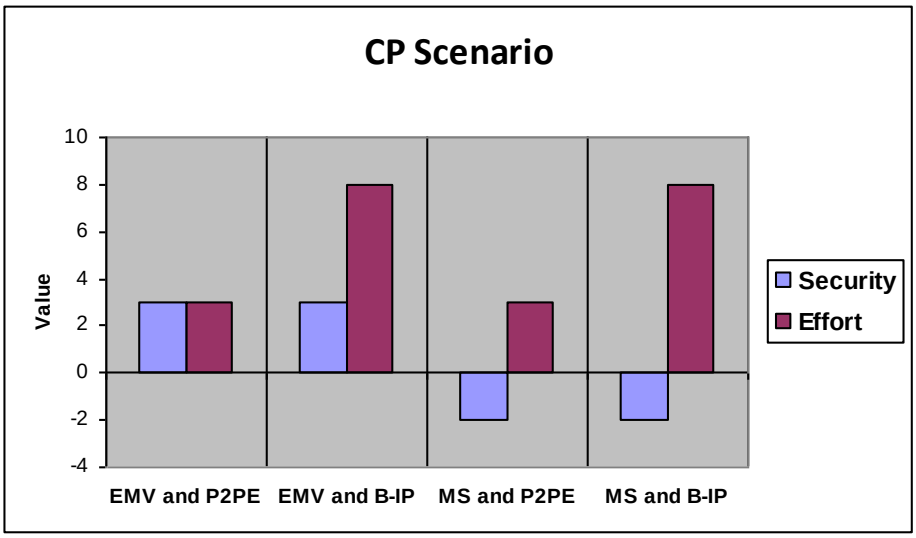

Fig. 5.1 CP scenario results

Having this in mind, the following recommendations are presented.

- Manufacturers of terminals should stop supporting MS technology.
- Manufacturers of payment cards should stop embedding MS into the payment cards.
- Merchants should stop supporting MS payments.
- Merchants should aim to meet the eligibility criteria of SAQ P2PE to reduce the amount of effort needed for PCI DSS compliance.

5.2. Card-Not-Present Scenario

In the CNP channel (see section 3.3) there are two main technologies involved in the payment process, CVV2, which is present in today's payment card structure (see section 2.7), and 3DS 2.0 (see section 1.4, section 4.1.2 and section 4.2.5), which is a state-of-the-art technology. This section also focuses on the SAQ A and the SAQ A-EP (see section 4.2.1.3), each with different requirements that merchants need to meet to comply with PCI DSS.

5.2.1. Technology

The objective of this section is to evaluate the overall security of the 3DS 2.0 and CVV2 technologies. First, it is important to define quantifiable metrics for this evaluation. Four metrics have been selected: non-repudiated purchase, authentication, validity and technology characteristic.

- Non-repudiated purchase: This is ability to guarantee that a purchase has been made by a cardholder.
- Authentication: This is the provision of assurance that a claimed characteristic of an individual is correct (see section 1.1).

- Validity: This states the length of time for which a given set of parameters is valid for the technology. Two cases are present in this metric.
    - Validity per transaction: The technology with a given set of parameters is valid for a given transaction. New parameters are presented for each new transaction.
    - Validity during card lifetime: The technology with a given set of parameters is valid during the lifetime of the payment card. Once the payment card expires, the technology parameters are changed.
- Technology characteristic: This identifies the essential nature of the technology. Two cases are presented in this metric.
    - Dynamic: This term identifies the technology as a procedure used to reach a defined goal.
    - Static: This term identifies the technology as a static value used to reach a defined goal.

For the metric “non-repudiated purchase,” the assessment is done with one of two values.

- Value -1: If the technology lacks the metric.
- Value 0: If the technology possesses the metric.

The metric “authentication” is assessed with two values.

- Value -1: If the technology lacks the metric.
- Value 0: If the technology possesses the metric.

The metric “validity” is assessed with two values.

- Value 0: If the attribute of the metric is “during card lifetime.”
- Value +1: If the attribute of the metric is “per transaction.”

The metric “technology characteristic” is assessed with two values.

- Value 0: If the technology possesses a static nature.
- Value +1: If the technology possesses a dynamic nature.

Below is the evaluation of these technologies against each of the above metrics.

For 3DS 2.0:

- Non-repudiated purchase is present, as the cardholder must authenticate itself before making a purchase of a good or service from a merchant.
- Authentication is present, as this technology can perform authentication in either a frictionless or a challenged flow.
- Validity is per transaction because the parameters that the technology uses to authenticate a cardholder vary with each transaction.

- The characteristic of the technology is dynamic in nature, as the technology is a procedure used to authenticate a cardholder.

For CVV2:

- Non-repudiated purchase is absent because the cardholder does not authenticate itself before making a purchase of a good or service from a merchant.
- Authentication is absent because the technology verifies only the possession of the payment card or that the consumer knows the CVV2 value but does not authenticate the cardholder.
- Validity extends for the card lifetime because the issuer bank uses certain parameters to obtain a CVV2 value, which is printed on the payment card and is changed only when a new payment card is issued.
- The characteristic of the technology is static in nature, as the technology is a static value used to verify the possession of the payment card.

The values assigned to these technologies for each metric are listed in Table 5.3.

Table 5.3 CNP technology evaluation scores

Technology			
3DS 2.0	**Value**	**CVV2**	**Value**
Non-repudiated purchase	0	No non-repudiated purchase	-1
Authentication	0	No authentication	-1
Validity per transaction	+1	Validity during card lifetime	0
Dynamic nature	+1	Static nature	0
Overall Score	+2	**Overall Score**	-2

5.2.2. PCI DSS Compliance

The objective of this section is to evaluate the level of overall effort required of merchants for compliance with PCI DSS by using SAQ A or SAQ A-EP. Three metrics have been selected: number of applicable PCI DSS requirements, number of questions to be assessed and applicable scope of systems.

- Number of applicable PCI DSS requirements: This metric provides the number of requirements a merchant must meet to be in compliance when using a specific SAQ.
- Number of questions to be assessed: This metric provides for a specific SAQ, the number of questions that a merchant needs to assess.
- Applicable scope of systems: This metric provides a clear and defined scope for what an SAQ evaluates.

For the metric “number of applicable PCI DSS requirements,” since PCI DSS includes 12 requirements, four possible values have been defined.

- Value 1: If the number of requirements is less than or equal to 3.
- Value 2: If the number of requirements is 4–6.
- Value 3: If the number of requirements is 7–9.
- Value 4: If the number of requirements is 10–12.

The metric “number of questions to be assessed,” is assessed on a scale of four values since the maximum number of questions an SAQ can have is unknown.

- Value 1: If the number of questions assessed is less than or equal to 50.
- Value 2: If the number of questions assessed is 51–100.
- Value 3: If the number of questions assessed is 101–150.
- Value 4: If the number of questions assessed is greater than 150.

The metric “applicable scope of systems” is assessed with one of two values.

- Value 1: If the SAQ clearly specifies which network devices the merchant must configure for PCI DSS compliance and if the number of network devices needed to configure is low.
- Value 2: If the SAQ does not specify which network devices the merchant must configure for PCI DSS compliance and if the number of network devices needed to configure is high.

The assigned metric values for the evaluated SAQs are given in Table 5.4.

Table 5.4 CNP SAQ evaluation scores

SAQ Metrics			
SAQ A	**Value**	**SAQ A-EP**	**Value**
5 applicable PCI DSS requirements	2	12 applicable PCI DSS requirements	4
22 questions to be assessed	1	191 questions to be assessed	4
Reduced and clear scope of systems	1	Extensive and unclear scope of systems	2
Overall Score	4	**Overall Score**	10

5.2.3. Results

From the results in section 5.2.1 and section 5.2.2, the final results for security and effort in CNP scenarios are assembled in Figure 5.2. Based on these results, the preferred scenario for a CNP channel for electronic payments is to use 3DS 2.0 and SAQ A for their high level of security and low level of required effort.

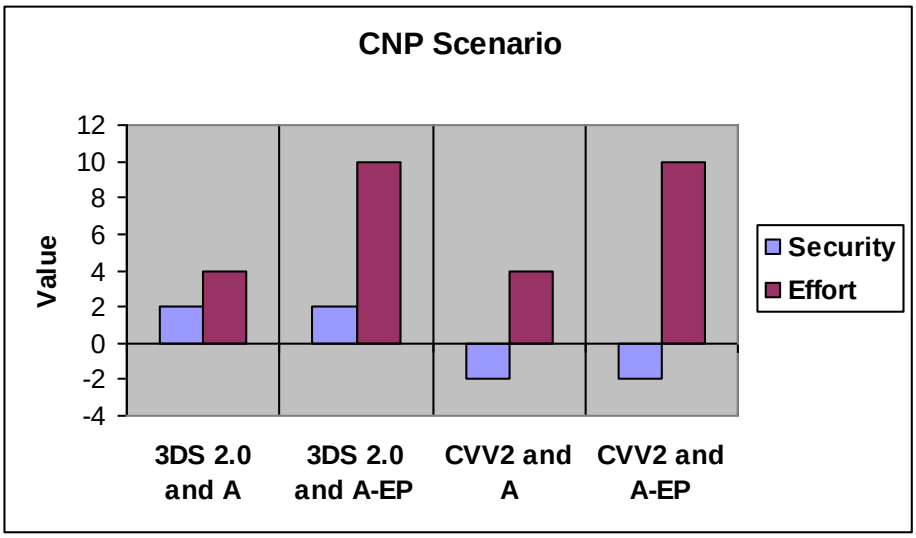

Fig. 5.2 CNP scenario results

With the results obtained previously, it is possible to provide the following recommendations:

- Merchants should aim to meet the eligibility criteria of SAQ A to reduce the amount of effort PCI DSS compliance requires.
- Merchants should start adopting 3DS 2.0 as an authentication protocol instead of using CVV2.
- Manufacturers of payment cards should stop printing CVV2 into the payment cards.

CONCLUSIONS

This thesis presents a compilation of information on payment card technologies and standards that was gathered and matched from various official documents. With this, it is possible to understand from a single source the security mechanisms the technologies and standards provide. This thesis also, defined and applied a number of metrics to evaluate and compare the technologies and standards compliance tools reviewed.

Organizations such as ISO, EMVCo, and PCI SSC play a critical role in the security of card payment transactions. ISO has an indirect role in the process; this organization defines many concepts used in information security and other areas that serve as a base for various technologies and standards. EMVCo plays a direct role in the security of card payments. This organization defines the technologies used by the parties involved during a card payment and is in charge of continually maintaining, developing, and updating technologies to secure card payments. PCI SSC also plays a direct role, defining various standards that involved parties need to comply with to assure card payment security. Moreover, as discussed earlier in this thesis, an active collaboration between EMVCo and PCI SSC resulted in the development of the 3DS 2.0 protocol.

The analysis of the structured elements of the payment card revealed ten elements. Each of these elements, except for two, implements a security feature for the payment card. The first exception is the magnetic stripe, which is an outdated and unsecured technology for the card-present channel that is still in place to make the payment card backwards compatible with out-of-date POIs. The second exception is the CVV2, which is a security mechanism for the card-not-present channel that only authenticates the possession of the payment card.

Studying the card payment life cycle revealed at least five entities with a role in the payment process. The two payment channels available for the card payment process are the card-present channel and the card-not-present channel. These channels indicate the presence or absence of the cardholder at the merchant's facilities when a card payment is initiated.

Three EMVCo technologies are reviewed in this document: the EMV chip, EMV 3DS 2.0, and the EMV payment tokenization. Each of these technologies implements several security features, including data authentication, cardholder verification methods, authentication flows, and verification and identification methods. These security features are essential because the presence, absence, or combination of them affects the overall security of the technology. The study addressed four standards from the PCI SSC: the PCI DSS, the PCI PTS, the PCI PA-DSS and the PCI P2PE. These standards have protecting the cardholder's sensitive data as their primary objective. For the PCI DSS specifically, there are eight self-assessment questionnaires that each merchant can use, depending on its eligibility criteria.

Having evaluated the SAQs and technologies for the CP scenario, this thesis recommends the EMV chip as providing better security features and use of SAQ P2PE, which reduces the effort merchants must invest for PCI DSS compliance. In the CNP scenario, the evaluation results indicate a clear recommendation for the better security of the channel the use of the 3DS 2.0 technology and for the SAQ A as requiring less effort from merchants for PCI DSS compliance.

During the evaluation presented in this research, it was possible to answer the two previously mentioned questions. For the first question, To what extent do these involved technologies provide security for the data used in card payment transactions for the different payment channels? For the CP channel, it was found that the MS technology does not provide security due to the characteristics this technology possesses. In contrast, the EMV chip technology with its intrinsic characteristics provides security to the CP channel. For the CNP channel, it was found that CVV2 does not provide security due to its characteristics. In contrast, 3DS 2.0 with its intrinsic characteristics provides security to the CNP channel. And for the second question, How much effort is required of merchants using SAQs to ensure the compliance with PCI DSS? It was found that for the CP channel, using the SAQ B-IP requires more effort than using the SAQ P2PE. As for the CNP channel, it was found that using the SAQ A-EP requires more effort than using the SAQ A.

After evaluating both payment channels, it was possible to present further recommendations. For the CP channel, manufacturers of terminals should stop supporting MS technology, manufacturers of payment cards should stop embedding the MS into cards, and merchants should stop supporting MS payments. For the CNP channel, card manufacturers should stop printing the CVV2 into cards, and merchants should move to 3DS 2.0 as an authentication protocol instead of using CVV2.

The greater security of the technologies recommended above will considerably reduce the amount of fraud that both payment channels suffer. This reduction of fraud implies a reduction of the incurred losses for the different involved entities in payment card transactions. Additionally, using the above recommended SAQs for PCI DSS compliance result in less required effort from merchants, which can lead to a reduction of involved costs and time spent.

There is an ethical obligation to protect the sensitive data within the payment card used during the payment transaction. This ethical obligation resides to prevent the financial and emotional consequences that victims of fraud suffer. With this in consideration, it is important to use the previous technologies recommended. These said technologies, are up-to-date and state-of-the-art technologies that strengthen the security of payment card transactions today.

It is important to mention some limitations that the present thesis presents. First, in evaluating technology in the CP channel, it was assumed that there is no mechanism to detect cloned payment cards MSs. In reality, such methods do exist but are not implemented, and it would be interesting in future research to include this in the evaluation process to learn how it affects the score of the

“attack resistance” metric. Second, in evaluating the effort required to completed SAQs, the costs implicit in using each SAQ were not considered. These might include costs per transaction, cost per service and cost of POIs. Considering these costs in future research would procude a more precise estimate of the effort merchants must invest in PCI DSS compliance.

For future steps, it is essential to continue with a detailed study of new security mechanisms being implemented for innovative and alternative methods of electronic payments. Also, continuing research and innovation in authentication mechanisms will improve the security of card payments for both payment channels while maintaining practicability and acceptance by the consumer. Finally, it should be noted that the constant evolution of criminal attacks on electronic payments for illegal gains must be followed and counteracted by the development of further security technologies and measures.

REFERENCES

[1] “The History of PCI Compliance,” *WEXInc*. [Online]. Available: https://bit.ly/33zObqu [Accessed Jun. 12, 2019]

[2] “PCI DSS history, everything you need to know,” *WorldPay from FIS*. [Online]. Available: https://bit.ly/2ZZpxx8 [Accessed Jun. 12, 2019]

[3] “ENVCo the Basics,” *EMVCo*. [Online]. Available: https://bit.ly/2MkFcUF [Accessed Jun. 12, 2019]

[4] “About Us,” *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2gaBJoR [Accessed Jun. 12, 2019]

[5] "ISO/IEC 24760-1:2019: IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts," *ISO*. [Online]. Available: https://bit.ly/2XSUW2y [Accessed Jun. 12, 2019]

[6] "ISO/IEC 27000:2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary," *ISO*. [Online]. Available: https://bit.ly/2XSenZb [Accessed Jun. 12, 2019]

[7] “EMVCo: Operating Principles,” *EMVCo*. [Online]. https://bit.ly/2WI9CWx [Accessed Jun. 12, 2019]

[8] “Worldwide EMV Chip Card Deployment and Adoption,” *EMVCo*. [Online]. Available: https://bit.ly/2Xili1L [Accessed Jun. 12, 2019]

[9] "PCI Security," *PCI Security Standards Council*. [Online]. Available: https://bit.ly/1Wgodxc [Accessed Jun. 13, 2019]

[10] “PCI Security Standards Overview,” *PCI Security Standards Council*. [Online]. Available: https://bit.ly/2XbkCuS [Accessed Jun. 13, 2019]

[11] “Increasing Security and Reducing Fraud with EMV Chip and PCI Standards,” *PCI Security Standards Council*. [Online]. Available: https://bit.ly/1hjFA2i [Accessed Jun. 13, 2019]

[12] “EMVCo and PCI SSC Combine Expertise on 3-D Secure 2.0,” *PCI Security Standards Council*. [Online]. Available: https://bit.ly/2ReiVHs [Accessed Jun. 13, 2019]

[13] “First Data: Credit Card Fraud Protection – User Guide,” *First Data*. [Online]. Available: https://bit.ly/31gX5XJ [Accessed Jun. 14, 2019]

[14] “What is a Credit Card Issuer?,” *The Balance*. [Online]. Available: https://bit.ly/2wX6NBm [Accessed Jun. 14, 2019]

[15] “Contact EMV,” *EMVCo*. [Online]. Available: https://bit.ly/2ZsFuuX [Accessed Jun. 17, 2019]

[16] "Contactless EMV," *EMVCo*. [Online]. Available: https://bit.ly/2Y8YJNa [Accessed Jun. 17, 2019]

[17] “A Guide to EMV Chip Technology,” *EMVCo*. [Online]. Available: https://bit.ly/2tJLnGI [Accessed Jun. 17, 2019]

[18] Henk C. A. van Tilborg (2005), “Encyclopedia of Cryptography and Security,” Springer, New York

[19] “EMVCo Reports Over Half of Cards Issued Globally are EMV-enabled,” *EMVCo*. [Online]. Available: https://bit.ly/2vuxsI2 [Accessed Jun. 17, 2019]

[20] “What Is A Credit Card Number? The Meaning of Each Digit,” *WalletHub*. [Online]. Available: https://bit.ly/2ZuUoBy [Accessed Jun. 19, 2019]

[21] “Credit Cards,” *DataGenetics*. [Online]. Available: https://bit.ly/2WGJnzD [Accessed Jun. 19, 2019]

[22] “Why Do Credit Cards Expire?,” *CreditCardsCanada*. [Online]. Available: https://bit.ly/2WZQlQA [Accessed Jun. 20, 2019]

[23] “Get to Know the Parts of a Debit or Credit Card,” *The Balance*. [Online]. Available: https://bit.ly/2BGbQpH [Accessed Jun. 20, 2019]

[24] “How Credit Card Payment Processing Systems & Networks Really Work,” *Money Crashers*. [Online]. Available: https://bit.ly/2Y0bK8H [Accessed Jun. 20, 2019]

[25] “Credit Card Glossary: Magnetic Stripe,” *Creditcards.com*. [Online]. Available: https://bit.ly/2IuD4GJ [Accessed Jun. 20, 2019]

[26] “ISO Magnetic Stripe Card Standards,” *QCard The Lab Authority*. [Online]. Available: https://bit.ly/2MFVF5g [Accessed Jun. 20, 2019]

[27] “Introduction to Magnetic Stripe & Other Card Technologies,” *High Tech Aid*. [Online]. Available: https://bit.ly/2L2Oqn1 [Accessed Jun. 20, 2019]

[28] “Cloning,” *Investopedia*. [Online]. Available: https://bit.ly/2ItQToT [Accessed Jun. 20, 2019]

[29] “Executive summary,” *European Central Bank*. [Online]. Available: https://bit.ly/2YFqWI1 [Accessed Jun. 20, 2019]

[30] “Anatomy of a Credit Card,” *Credit Card Insider*. [Online]. https://bit.ly/31NqRUW [Accessed Jun. 20, 2019]

[31] “Mastercard, Discover, AmEx and Visa ditching signatures,” *Creditcards.com*. [Online]. Available: https://bit.ly/2qurDok [Accessed Jun. 20, 2019]

[32] “Credit card signatures are almost a thing of the past,” *CNN Money*. [Online]. Available: https://cnn.it/2M2hr3D [Accessed Jun. 20, 2019]

[33] “CVV Generate (CSNBCSG),” *IBM Knowledge Center*. [Online]. Available: https://ibm.co/2yUzUqh [Accessed Jun. 20, 2019]

[34] “Why Holograms are Used on Credit and Debit Cards,” *CreditCardProcessing.com*. [Online]. Available: https://bit.ly/2FmbJo9 [Accessed Jun. 20, 2019]

[35] “Learn More About Security Holograms,” *NovaVision*. [Online]. Available: https://bit.ly/2YMUinK [Accessed Jun. 20, 2019]

[36] "Card Acceptance Guidelines for Visa Merchants," *Visa*. [Online]. Available: https://vi.sa/2qxh7Mp [Accessed Jul. 17, 2019]

[37] "Integrated Circuit Card," *Investopedia*. [Online]. Available: https://bit.ly/2Sm8GS1 [Accessed Jul. 17, 2019]

[38] "Payment Card Industry Glossary," *PCI Ramblings*. [Online]. Available: https://bit.ly/2yG2DPs [Accessed Jul. 17, 2019]

[39] "What is POS? The Definitive Definition," *HarborTouch*. [Online]. Available: https://bit.ly/2T4SwwK [Accessed Jul. 17, 2019]

[40] "Personal Identification Number (PIN) Security Tips," *The Balance*. [Online]. Available: https://bit.ly/2EHTXco [Accessed Jul. 17, 2019]

[41] "Card-present (CP) transactions," *Creditcards.com*. [Online]. Available: https://bit.ly/2NZ4Bow [Accessed Jul. 17, 2019]

[42] "What is Card Not Present?," *Ecommerce Platforms*. [Online]. Available: https://bit.ly/2NUyshB [Accessed Jul. 17, 2019]

[43] "Card-Not-Present Fraud," *Investopedia*. [Online]. Available: https://bit.ly/2XMzxfZ [Accessed Jul. 17, 2019]

[44] “Book 1: Application Independent ICC to Terminal Interface Requirements,” *EMVCo*. [Online]. Available: https://bit.ly/2IMjGDX [Accessed Jun. 25, 2019]

[45] “Book 3: Application Specification,” *EMVCo*. [Online]. Available: https://bit.ly/2WIdUbu [Accessed Jun. 25, 2019]

[46] "Message Authentication Code Processing," *IBM Knowledge Center*. [Online]. Available: https://ibm.co/2JTHWEC [Accessed Jun. 25, 2019]

[47] “Book 2: Security and Key Management,” *EMVCo*. [Online]. Available: https://bit.ly/2NggJRx [Accessed Jun. 25, 2019]

[48] “EMV Key Management – Explained,” *Cryptomathic*. [Online]. Available: https://bit.ly/2NbIFG6 [Accessed Jun. 25, 2019]

[49] “Strengthening Card Authentication: a migration to DDA,” *Smart Payment* Association. [Online]. Available: https://bit.ly/2X3Y0Is [Accessed Jun. 25, 2019]

[50] “EMV CVM: Offline PIN,” *Host Merchant Services*. [Online]. Available: https://bit.ly/2Np3cHg [Accessed Jun. 25, 2019]

[51] “Online PIN,” *American Express*. [Online]. Available: https://amex.co/32NqJ8I [Accessed Jun. 25, 2019]

[52] “EMV Mobile Payment – Consumer Device Cardholder Verification Method Security Requirements,” *EMVCo*. [Online]. Available: https://bit.ly/327x7aj [Accessed Jun. 27, 2019]

[53] “EMV 3-D Secure,” *EMVCo*. [Online]. Available: https://bit.ly/2iBNmXp [Accessed Jun. 27, 2019]

[54] “EMV 3-D Secure 2.0,” *Identity Management & Security*. [Online]. Available: https://bit.ly/2YXpzW1 [Accessed Jun. 27, 2019]

[55] “EMV 3-D Secure Protocol and Core Functions Specification,” *EMVCo*. [Online]. Available: https://bit.ly/2NaUHiW [Accessed Jun. 27, 2019]

[56] “Diffie-Hellman Protocol,” *WolframMathWorld*. [Online] Available: https://bit.ly/2nhuFJG [Accessed Jun. 27, 2019]

[57] “EMV Payment Tokenization Specification – Technical Framework,” *EMVCo*. [Online]. Available: https://bit.ly/2RP5KgD [Accessed Jul. 01, 2019]

[58] “Authentication Factor,” *TechTarget SearchSecurity*. [Online]. Available: https://bit.ly/2YLsjcW [Accessed Jun. 27, 2019]

[59] “Tokenization,” *Google Payment Merchant Help*. [Online]. Available: https://bit.ly/2L0YAoL [Accessed Jul. 04, 2019]

[60] “How payments work,” *Google Payment Merchant Help*. [Online]. Available: https://bit.ly/2XPrSg4 [Accessed Jul. 04, 2019]

[61] “HCE and Tokenization for Payment Services – discussion paper,” *GSMA*. [Online]. Available: https://bit.ly/2JbHVN6 [Accessed Jul. 04, 2019]

[62] “How Apple Pay Works Under the Hood,” *FreeCodeCamp*. [Online]. Available: https://bit.ly/30dJKPr [Accessed Jul. 04, 2019]

[63] “Apple Pay – An attempt to demystify – Take 2,” *Ganeshi*. [Online]. Available: https://bit.ly/2CIz426 [Accessed Jul. 04, 2019]

[64] “Payment Card Industry (PCI) – Data Security Standard,” *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2OHluV9 [Accessed Jul. 05, 2019]

[65] “PCI DSS Certification,” *Imperva*. [Online]. Available: https://bit.ly/2Lmegm8 [Accessed Jul. 05, 2019]

[66] “PCI DSS Data Storage Do’s and Don’ts,” *PCI Security Standards Council*. [Online]. Available: https://bit.ly/2FngMVt [Accessed Jun. 19, 2019]

[67] "Payment Card Industry (PCI) – Data Security Standard – Self-Assessment Questionnaire – Instructions and Guidelines," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2SvSpKl [Accessed Jul. 18, 2019]

[68] “Payment Card Industry (PCI) – DSS and PA-DSS – Glossary of Terms, Abbreviations, and Acronyms,” *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2ymM2jl [Accessed Jul. 30, 2019]

[69] “Payment Card Industry (PCI) – Point-to-Point Encryption,” *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2NUHKtZ [Accessed Jun. 26, 2019]

[70] "Payment Card Industry (PCI) – Point-to-Point Encryption – Glossary of Terms, Abbreviations, and Acronyms," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2NVfibw [Accessed Jun. 26, 2019]

[71] "Payment Card Industry (PCI) – Payment Application Data Security Standard," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2XJUSqo [Accessed Jun. 27, 2019]

[72] "Payment Card Industry (PCI) – PIN Transaction Security (PTS) Hardware Security Module (HSM) – Modular Security Requirements," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2xSKoG4 [Accessed Jun. 27, 2019]

[73] "Payment Card Industry (PCI) – PIN Transaction Security (PTS) Point of Interaction (POI) – Modular Security Requirements," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2LXDA1Y [Accessed Jun. 28, 2019]

[74] "Payment Card Industry 3-D Secure (PCI 3DS) – Security Requirements and Assessment Procedures for EMV 3-D Secure Core Components:

ACS, DS, and 3DS Server," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/32AiDAj [Accessed Jul. 09, 2019]

[75] "Payment Card Industry 3-D Secure (PIC 3DS) – Security Requirements and Assessment Procedures for EMV 3-D Secure SDK," *PCI Security Standard Council*. [Online]. Available: https://bit.ly/2xPLm5R [Accessed Jul. 10, 2019]

ANNEXES

Annex A: EMV 3DS 2.0 messages types

The 3DS authentication protocol uses many messages to carry out the process of authenticating an individual. These messages have different functions, and they are listed as follows.

3DS Messages Types	
Name	**Description**
Authentication Request Message (AReq)	The first message of the 3DS authentication protocol, this message contains the cardholder, payment and device information. The formation of this message occurs after the 3DS server has requested cardholder authentication. Also, there is only one AReq message per transaction.
Authentication Response Message (ARes)	This message acknowledges the receipt of the AReq message from part of the ACS to the 3DS server. It returns the results of the authentication request. There can be only one ARes message per transaction.
Challenge Request Message (CReq)	This message initiates the interaction of the cardholder in the challenge flow. It carries the cardholder's authentication data. For app-based channels, there can be multiple CReq messages per challenge, while in browser-based channels, there can be only one CReq message per challenge.
Challenge Response Message (CRes)	This is the response of the ACS to the CReq message. For browser-based channels, it transmits the cardholder's authentication outcome. For app-based channels, it can indicate the results or further requirements to complete authentication.
Results Request Message (RReq)	This message is sent by the 3DS server to the ACS and includes the authentication or verification results. There can be only one RReq message per transaction.
Results Response Message (RRes)	This message is sent by the ACS to the 3DS server acknowledging receipt of the RReq message. There can be only one RRes message per transaction.
Error Message	This message contains information about errors that occurred in message processing among the 3DS server, the DS, the ACS, and the 3DS SDK.

Annex B: PCI DSS goals and requirements

An explanation for each of the requirements in the PCI DSS is given below.

PCI Data Security Standard		
Goals	**Requirements**	**Reason**
Build and maintain secure networks and systems	Install and maintain a firewall configuration to protect cardholder data.	To perform network monitoring and to block transmissions that are outside security criteria.
	Do not use defaults provided by vendors for system passwords and other security parameters.	Default passwords and settings are easily determined.
Protect cardholder data	Protect stored cardholder data.	Methods such as encryption, truncation, masking, and hashing protect critical account data from malicious users.
	Encrypt transmission of cardholder data across open, public networks.	Malicious users can exploit the vulnerabilities of wireless networks.
Maintain a vulnerability management program	Protect all systems from malware and frequently update anti-virus software or programs.	Anti-virus software protects systems from malicious software aiming to exploit vulnerabilities and needs to be updated regularly.
	Develop and maintain secure systems and applications.	The main goal is to regularly patch systems to prevent exploitation and compromise.
Implement strong access control measures	Restrict access to cardholder information by the need to know from the business.	Ensure the access of only authorized personnel to critical data.
	Identify and authenticate access to system components.	To provide accountability and tracing of actions performed on critical data and systems.
	Restrict physical access to cardholder data.	Keep unauthorized individuals from accessing or removing data.
Regularly monitor and test networks	Track and monitor all access to network resources and cardholder data.	To prevent, to detect or to minimize the impact of a data compromise.
	Regularly test security systems and processes.	The main goal is to look for and patch new vulnerabilities.
Maintain an information security policy	Maintain for all personnel an information security policy.	To protect data by assigning specific responsibilities to specific personnel.

Annex C: Types of SAQs

This annex shows the different SAQs that a merchant can use, if they meet the eligibility criteria, to comply with PCI DSS.

Types of SAQs			
SAQ	**Channel**	**Questions**	**Description**
A	CNP	22	Directed to merchants that have all cardholder data processing outsourced to a PCI-compliant third-party service provider. Additionally, the merchant's systems or premises must not transmit or electronically store cardholder data.
A-EP	CNP (e-commerce)	191	For merchants that have outsourced cardholder data processing to a PCI-compliant third-party service provider and have a website(s) that could impact the security of the payment transaction. The merchant's systems or premises must not transmit or electronically store cardholder data.
B	CP and CNP (MOTO)	41	This SAQ is for merchants that use imprint machines or standalone dial-out terminals that do not electronically store cardholder data.
B-IP		82	An SAQ for merchants that use only standalone PTS-approved payment terminals that do not electronically store cardholder data.
C-VT		79	This SAQ is for merchants that, via a keyboard, enter a single transaction into an internet-based virtual payment terminal solution provided by a PCI-DSS validated third-party service provider. There is no electronic storage of cardholder data.
C		160	This SAQ is for merchants, that do not store cardholder data and that use payment application systems connected to the Internet.
P2PE	CP	33	Directed to merchants that use only hardware payment terminals included and managed by a validated PCI P2PE solution. There is no electronic storage of cardholder data.
D	CP and CNP (e-commerce)	329	For merchants not included in any of the SAQs previously mention.