Master Thesis
Towards an Improved EMV Credit Card Certification

Version of June 26, 2007

Etienne Gerts

Master Thesis
Towards an Improved EMV Credit Card Certification

THESIS

submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

in

SOFTWARE ENGINEERING

by

Etienne Gerts
born in Gouda, the Netherlands

Software Engineering Research Group
Department of Software Technology
Faculty EEMCS, Delft University of Technology
Delft, the Netherlands
www.ewi.tudelft.nl

Master Thesis
Towards an Improved EMV Credit Card Certification

Author: Etienne Gerts
Student id: 1092928
Email: e.c.a.gerts@student.tudelft.nl

Abstract

Credit card fraud has been a major issue for financial institutions, since the very moment credit cards were introduced. To reduce this fraud, a new worldwide standard has been introduced by some of the main players in this market: Europay, MasterCard and Visa (EMV). The EMV standard exploits smart card technology for both credit card and card holder authentication, rather than magnetic strip technology that provides virtually no authentication at all.

The certification process around this new standard however is a very time consuming and costly task that causes major problems for payment service providers, whose core activity is to process credit card payments. The main reason for the cumbersome certification process is that the whole chain of components must be certified for each implementation, where in the past certification of the comprising components was considered sufficient. The goals of the research are to investigate in depth the EMV certification process in general and the testing of individual components compared to the certification of the chain of these components in particular. This Master Thesis describes the research of the EMV certification process, provides an analysis of the results and presents recommendations on how the certification process can be optimised.

The current EMV certification process will be proven to have a very low path coverage and therefore has a poor quality. From the performed research and subsequent analysis, recommendations will be derived to improve the test suite coverage by adapting the existing certification test suites, by extended unit testing and by increased integration coverage. The proposed improvements will decrease the elapsed time, reduce costs, increase the quality of the product and shorten the time to market.

Thesis Committee:

Chair:	Prof. Dr. A. van Deursen, Faculty EEMCS, TU Delft
University supervisor:	Dr. H.G. Gross, Faculty EEMCS, TU Delft
Company supervisor:	W.M. Lobbezoo Msc., Empty Quarter Consultancy b.v.
Committee Member:	Ir. B.R. Sodoyer, LS Software Engineering, TU Delft

Preface

"Oh, what a tangled web we weave, When first we practise to deceive!"
Sir Walter Scott, Marmion: A Tale of Flodden Field
Canto VI, Stanza XVII

This Master's Thesis describes my graduation project, which concludes my study of Computer Science at Delft University of Technology. The graduation project was performed at Empty Quarter Consultancy BV (EQC).

When I used to make a credit card payment before my encounters with the wonders of the financial world, I had to provide my credit card number and the expiry date. So when the suggestion came to graduate on (a specific type of) credit card payments, I thought people were kidding: "How difficult can it be?". I know by now that in order to process a credit card payment, the financial industry has built a tangled web, both in a hardware sense and in a software sense, hence the quote. This is a rather popular quote, a clich for sure, but the culture agnostics often leave out the second part of the strophe. How applicable however is it here! Where the EMV prophets preach the world full coverage of their certification tests, I will have to prove them wrong.

I would like to thank several people that were involved during my graduation project. First of all, I would like to thank dr. Hans-Gerhard Gross, my supervisor of Delft University of Technology. He helped me during the whole graduation project, reviewed my Thesis, and gave a lot of helpful comments and feedback. Secondly, I would like to thank Willem Lobbezoo, my supervisor at EQC. Willem started the research about EMV in October 2003, put a lot of effort in the project, and assisted me during my Thesis. His effort made the whole project possible. I also would like to thank Gerardo de Geest, who made the initial contacts and prepared for the project. I would like to thank my friends in general and my girlfriend in particular, who where always there for me when I needed them, and last, but not least, I would like to thank my parents for their support and sponsoring during my entire education.

Etienne Gerts
Delft, the Netherlands
June 26, 2007

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Credit card fraud has become a major issue for financial institutions. In 2006 the credit card fraud was 428 million pounds for the UK only [20]. To reduce credit card fraud, a new worldwide standard has been introduced called EMV (**E**uropay **M**astercard **V**isa). These are the names of three of the main credit card companies in the world today. Until now, credit cards were equipped with easy to copy magnetic stripes and, therefore, provided no card authentication. This means that there was no way to determine that the card was original, or a copy.

Cardholder authentication was not forced by the credit card companies, and was rarely used (identifying oneself by showing a passport, for instance). The new core technology used by the new EMV standard is a smartcard containing a chip that is protected by cryptographic algorithms. This allows terminals to authenticate the card by ensuring that the card is genuine (1). By using a PIN code procedure, one can also authenticate the cardholder (2). Because of those two pillars on which the EMV standard rests, being card authentication and cardholder authentication, the project to introduce this new technology in the UK is referred to as **"Chip & Pin"**. Figure 1.1 displays the new chip and pin logo.

Figure 1.1: The Chip & Pin Logo

Chip & Pin was rolled out nationwide in 2004 with advertisements in the press and national television touting the *Safety in Numbers* slogan [33]. The UK was one of the first countries were Chip & Pin was rolled out. At the moment, almost all credit card payment facilities are Chip & Pin compatible, and all domestic credit card transactions are Chip &

Pin transactions. In the Netherlands the first EMV credit cards were rolled out in begin 2005.

The business process around credit card payments, in general, is the process by which a shopper buys goods or services from a merchant and pays for these by using a credit card.

The various stakeholders in the process are:

1. The ”Shopper” is the consumer who is buying goods or services from a ”Merchant”.
2. The ”Merchant” is the shop owner who is selling goods or services to the ”Shopper”.
3. The ”Issuer” is the (”Shopper”’s) bank that has issued a credit card to the ”Shopper” who is using this credit card to pay for the transaction. The ”Issuer” will bill the ”Shopper” and inform him by a periodic bank statement.
4. The ”Acquirer” is the (”Merchant”’s) bank that will collect the money for the ”Merchant”. The ”Acquirer” will remit the money to the bank account of the ”Merchant” and inform him by a periodic bank statement.
5. The ”Credit Card Company” is the credit card company that takes care of the processing between ”Issuers” and ”Acquirers”.
6. The ”PSP” is the **P**ayment **S**ervice **P**rovider that is providing the above services in one integrated package to the ”Merchant”. A ”PSP” is offering one single standardized interface to the ”Merchant” for processing payments. By doing so, the ”PSP” is taking away the burden for the ”Merchant” to interact with many different financial institutions. The ”PSP” furthermore is offering additional services to the ”Merchant” like currency conversions and reconciliation.

As an example: a Shopper may have a Visa (Credit Card Company) [28] card from ABN AMRO (Issuer) [1] that he uses to pay a Merchant, who, in turn, has a bank account with ING (Acquirer) [18]. The merchant has a contract with a PSP like Triple Deal [27] to handle this transaction. The transaction flow for such a simple payment is shown in Figure 1.2. The POS (**P**oint **O**f **S**ale) application runs at the merchant’s shop (cash register).

To guarantee that the payment of the Shopper is handled properly, the credit card companies demand to certify the full transaction flow from the terminal to the issuer (and back again). In the situation of using magnetic stripe transactions, the various systems were certified independently by the credit card companies. In the new situation using EMV the certification process is end-to-end. This means that certification is required for each combination of merchant, country, terminal, language, PSP, acquirer and issuer. This implies an enormous amount of extra effort for the various players when one component is replaced, since now the whole chain needs to be certified, instead of the individual components that make up the chain [17]. The certification process of the whole chain is done by a selected group of acquirers on behalf of the credit card companies. The preparation of such a certification and the certification itself takes a lot of time. In practice it turns out that each certification takes 3 to 6 months [2].

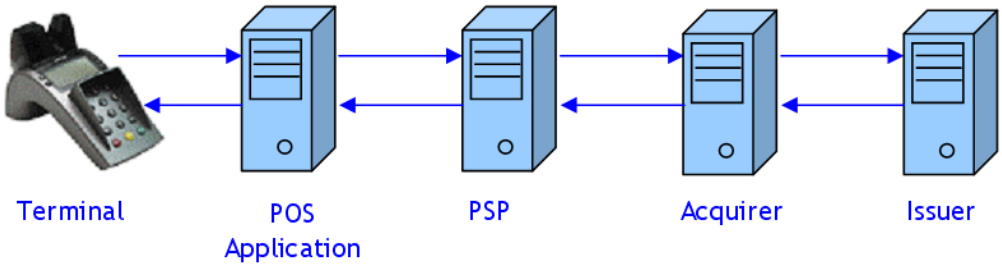


Figure 1.2: Transaction Flow

The granted certificate is only valid for the specific chain of components. This means that when one of the components in the chain changes: for example the POS Application gets a software update, or the payment is done with a different terminal, the certificate is invalid. The consequence is that the certification process has to be done all over again for the new combination of components. For a PSP that wants to support different terminals and POS applications this certification process brings a lot of extra work and effort, and is almost unfeasible.

This brings us to the key question of this Thesis, which is: 'If each of the components is certified and if all the protocols are certified between these components, would this not be sufficient to conclude that individually certified components could be exchanged, without the requirement to certify the whole chain again?' If the answer to this question would be 'yes', this would mean a tremendous reduction in certification efforts.

From this key question, other sub-questions can be derived to help in finding the right answer:

1. How do the provided test scripts of the card companies meet the requirements/ specification of the EMV standard? In other words, what's the quality of the current EMV certification process?

2. How can we specify and test individual components to verify that they satisfy the requirements/ specifications?

3. How can we specify and test the protocols used between the individual components in the chain (request-response) in such a way that we could safely replace individual components in the chain?

4. Can we make the (unconditional or conditional) statement that the whole chain is certified when all the individual components in the chain are certified?

5. If this statement cannot be made, can the current certification process be optimized so it will take less time than 3 to 6 months?

An approach proposed to answer the prime questions that are raised above is described in the literature study document [15]. In this Thesis the described approach is followed to really answer these questions.

EMV is still very new and unknown in The Netherlands. At the moment, there is also no other research known about the EMV certification process, that is performed by others. The performed research of this Thesis is done at a reference PSP from which the name will not be mentioned. Also a reference acquirer is used, which will also stay unnamed.

In the first chapter an overview of EMV is given. To fully understand the certification process, the business process of a payment transaction is studied and described in more detail. Furthermore, the EMV standard is described, followed by an explanation of the chain of different components that are involved during a transaction. Once the business process, including its components, and the EMV standard are clear, a more detailed description of the different EMV transaction is provided. To come to an improved EMV certification process, first the reason why a certification process is needed is explained in Chapter 3. The difference between the regular certification process and the new EMV certification process is given. To gain more experience, and to study the EMV certification process in more depth, a real certification process is carried out. After the description of this process, the individual components in the chain and the integration of the components are described. After the analysis an critical evaluation is done for the EMV certification process, the individual components, and the integration of the components, to help finding an answer for the research questions. With the critical evaluation some improvements for the EMV certification process are proposed in Chapter 4. After these proposals, the improvements are evaluated in Chapter 5. The Thesis ends with a summary, conclusions and future work in Chapter 6, and a personal reflection in Chapter 7.

Chapter 2

EMV Overview

In this chapter the business process around credit card transactions and EMV transactions, in particular, will be discussed. First the business process of a credit card transaction in general is explained. This section is followed by a short explanation of the EMV standard. After the EMV standard is more clear, the chain of components that are used for a EMV credit card transaction are described, followed by the different EMV transaction that can be performed.

2.1 The Business Process

As mentioned in the introduction, the business process is the process by which a shopper buys goods or services from a merchant and pays for these by using a credit card. First some different input channels for such a transaction are described in Section 2.1.1. In Section 2.1.2 the transaction process of a credit card transaction is explained in more detail.

2.1.1 Input Channels

The merchant is interested in one simple interface by which he can submit transactions and receive back the money in an easy way, irrespective of different payment methods that are offered to the shopper. On top of this, many merchants are interested in an automated reconciliation where outstanding receipts are automatically matched with the funds that have been remitted into the merchant's bank account. These services are typically provided by a PSP.

Another important aspect of the PSP's position is the following. PSP's started to process payments real-time typically over the Internet. Although originally designed for e-commerce purposes, their service offering has developed into a 'plug & play' solution for handling multiple sales channels as well, see Figure 2.1. Whatever sales channels are connected, all the clients' payments are processed over the same Internet infrastructure, in an identical way and are all together reconciliated. The five most common sales channels today are:

- Point Of Sales (POS), the cardholder is present at the merchant's counter

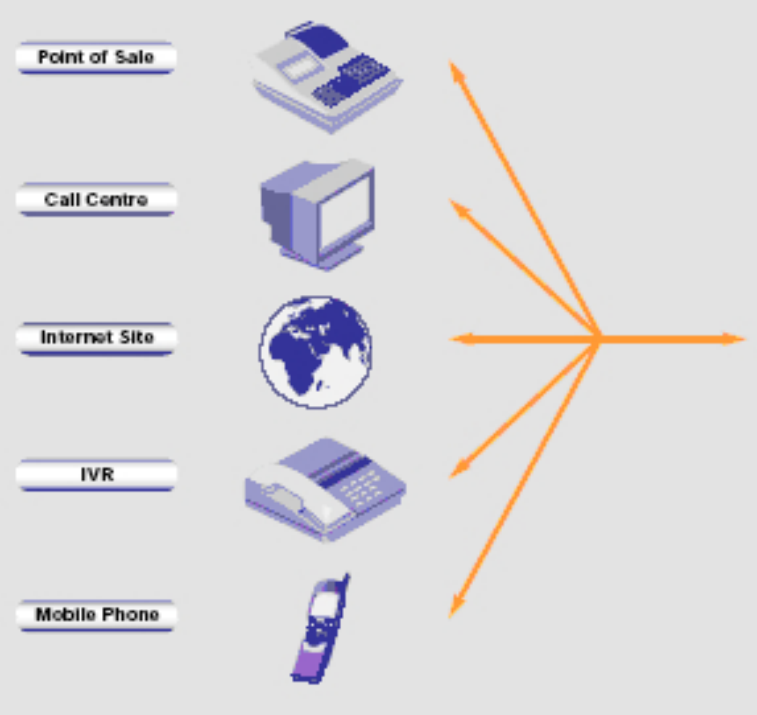


Figure 2.1: Multiple input channels

- Call Centre, the cardholder calls in to the call centre of the merchant to place an order
- Internet Site, mostly called e-commerce, the cardholder places an order online at the merchant's internet shop
- Interactive Voice Response (IVR), the cardholder places an order by calling the merchant's voice response system
- Mobile Phone orders, the cardholder uses his phone (WAP/iMode) to make a payment to the merchant

The most interesting one of these five channels, from an EMV perspective, is the POS application. The main difference between this channel and the other channels is that the cardholder is present at the POS (attended transaction). For the other channels this is not the case (unattended transaction). The EMV standard has obviously less significance for the other channels, since there is no card and cardholder present at the merchant desk when a transaction is initiated.

2.1.2 Transaction Process

The major stakeholders in an EMV transaction, and their roles, are described in the introduction. With this information we can walk again through the process of a sales transaction.

This is illustrated by Figure 2.2 that is used by EQC, and which was also used in my Bachelor Thesis [9]. A sequence diagram of the payment transaction process can also be found in Appendix A.

1. When a shopper comes at a merchant to pay for some goods or services with his credit card the first action in the process is for the merchant to authorise the (intended) transaction.
2. Authorisation refers to the procedure by which the merchant, at the time of sales, sends a request for authorisation to the PSP.
3. The PSP in its turn transmits the request to the acquirer of the Merchant
4. The acquirer in its turn sends it (through the card companies network) to the particular card issuer to get an approval for the transaction.
5. The issuer sends his response back to the acquirer.
6. The acquirer transmits, in its turn, the response to the PSP.
7. The PSP indicates to the merchant if the transaction is authorised correctly.
8. Once the authorisation is successfully obtained, the merchant can deliver the goods or services to the shopper.

After an authorisation the merchant has not yet received his money. This is subsequently done by a capture request. Capture refers to the procedure by which the PSP, on behalf of the merchant, stores and deposits the merchant's credit card transactions with the acquiring bank, and by doing so, requests for actual payment.

9. To start this process, the merchant sends the PSP a request to capture the transaction.
10. The PSP sends this capture request to the acquirer.
11. The acquirer, in its turn, transmits the capture message through the card companies to the issuer.
12. The result of the capture flows back from the issuer to the acquirer.
13. The acquirer emits the result to the PSP.
14. The PSP, in its turn, informs the merchant with the result.

Once the capture has been successfully performed, it is for the acquiring bank to settle the transaction by performing a pay-out. Settlement refers to the process by which acquiring banks process deposited transactions by merchants, inform their PSP of the processing results and remit the funds to the merchants bank account.

The acquiring bank collects the funds from the issuer and remits the funds related to the settled transactions either to the merchant directly or to the PSP. At that point in time the

merchant receives the money in his bank account. In case the money has been transferred to the PSP, the PSP will then remit the money to the bank account of the merchant. In this phase, the PSP can offer a range of consolidation and reconciliation services to the merchant.

2.2 The EMV Standard

The EMV standard is aimed at reducing credit card fraud by using smartcard technology. This technology is based upon two pillars: authentication of the card itself by using cryptographic technology (RSA and digital signatures) (1) and authentication of the cardholder by using PIN code processing functionality (2).

The EMV standard is designed by Europay, MasterCard and Visa. This standard is published in four manuals [11, 12, 13, 14]. The process at the highest level is shown in Figure 2.3.

Each of the partners has produced its own set of manuals that defines the specific implementation of this standard. The Visa implementation is covered in three manuals [19, 29, 30]. Each of the manuals describes the application from one of the following perspectives: the application (1), the card (2) and the terminal (3). The implementation of MasterCard is covered in one manual [21]. There is no specific specification of Europay, because Europay has recently merged with MasterCard.

The EMV standard describes 11 very distinct steps. To get a better understanding about the complex EMV standard, these 11 steps are briefly described below. Most of the steps are mandatory, but some steps are optional.

To fully understand the EMV protocol in all its depths, this protocol has been implemented as a ”proof of concept” as part of a Bachelors Thesis [9].

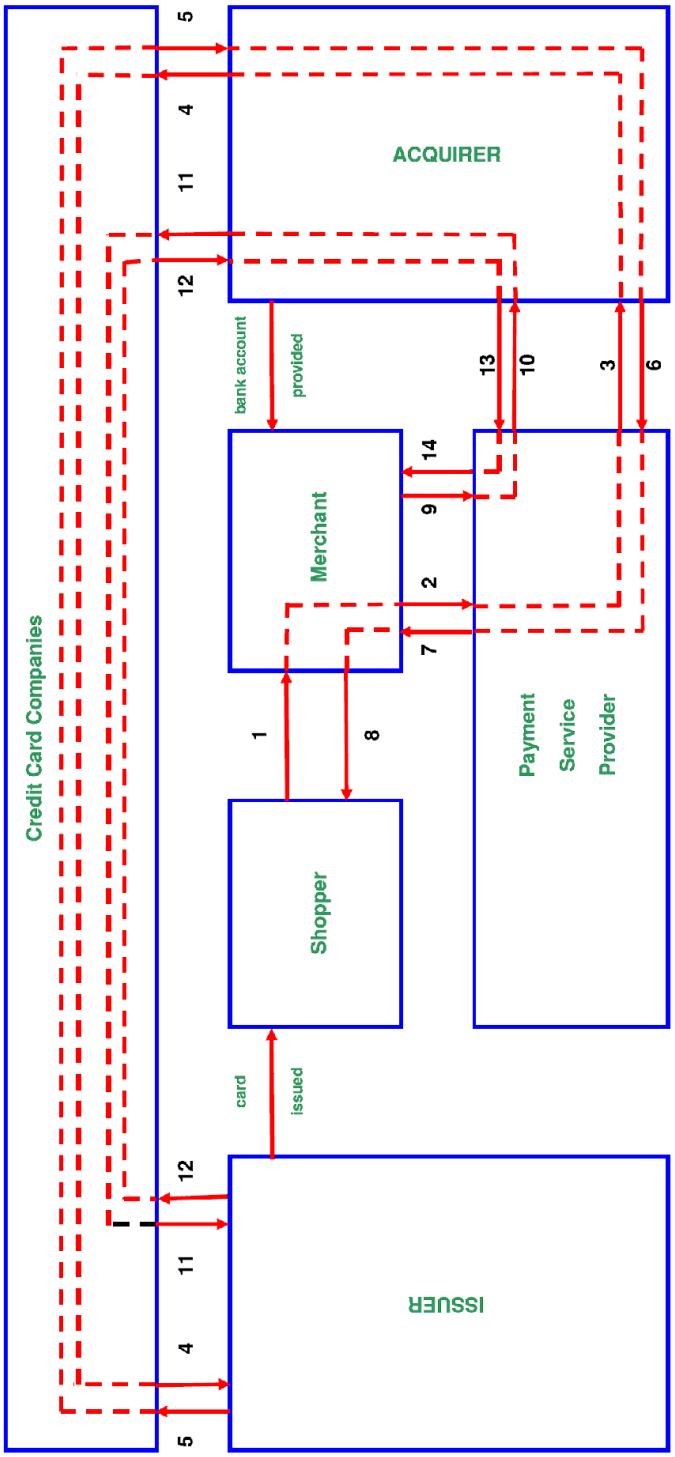
2.2.1 Application Selection (mandatory)

When an EMV card is presented to a terminal, the terminal determines which applications are supported by both the card and terminal. An application is for instance Visa Credit or Visa Debit. The standard allows for multiple ”logical” cards on one ”physical” card.

The terminal displays all mutually supported applications to the cardholder, and the cardholder selects from this list the application to be used for payment. If these applications cannot be displayed, the terminal selects the highest priority application as designated by the issuer during card personalization.

2.2.2 Initiate Application Processing/Read Application Data (mandatory)

When an EMV application is selected, the terminal requests that the card indicates the data and functions supported for that application. The card may indicate different data or different supported functions based upon characteristics of the transaction such as domestic or international. The terminal reads the data indicated by the card and uses the supported function list to determine the kind of processing to be perform.



1. Shopper presents credit card
2. Request for Authorization to PSP
3. Request for Authorization to Acquirer
4. Request for Authorization to Issuer
5. Authorization from Issuer
6. Authorization from Acquirer
7. Authorization from PSP
8. Merchant delivers goods / services
9. Capture from PSP (optional, otherwise automatic)
10. Capture from Acquirer
11. Capture from Issuer
12. Settlement by Issuer
13. Settlement by Acquirer
14. Settlement by PSP

Figure 2.2: The Payment Transaction Process

2.2.3 Offline Data Authentication

The terminal determines whether it should authenticate the card offline using either offline static or dynamic data authentication based upon the card and terminal support for these methods.

Offline Static Data Authentication (SDA)

SDA validates that important application data has not been fraudulently altered since card personalization. The terminal validates static (unchanging) data from the card using the card's issuer public key, which is stored on the card inside a public key certificate and a digital signature, which contains a hash of important application data encrypted with the issuer private key. A match of the recovered hash with a generated hash of the actual application data proves that the data has not been altered.

Offline Dynamic Data Authentication (DDA)

DDA, like SDA, validates that the card data has not been fraudulently altered and additionally validates that the card is genuine. DDA has two forms: Standard DDA and Combined DDA/AC Generation.

Standard DDA

With Standard DDA, the terminal requests that the card generates a cryptogram using dynamic (transaction unique) data from the card and terminal and an ICC Private Key. The terminal decrypts this dynamic signature using the ICC Public Key recovered from card data. A match of the recovered data to the original data verifies that the card is not a counterfeit card created with data skimmed (copied) from a legitimate card.

Combined DDA/AC Generation

With Combined DDA/AC Generation, the generation of the dynamic signature is combined with the generation of the card's Application Cryptogram during Card Action Analysis to assure that the Application Cryptogram came from the valid card.

2.2.4 Processing Restrictions (mandatory)

The terminal performs Processing Restrictions to see whether the transaction should be allowed. The terminal checks whether the effective date for the card has been reached, whether the card has expired, whether the application versions of the card and terminal match, and whether any Application Usage Control restrictions are in effect. An issuer may use Application Usage Controls to restrict a card's use for domestic or international, cash, goods, services, or cash back functions.

2.2.5 Cardholder Verification (mandatory)

Cardholder verification is used to ensure that the cardholder is legitimate and the card is not lost or stolen. The terminal uses a Card Verification Method (CVM) List from the card to determine the type of verification to be performed.

The CVM List establishes a priority of cardholder verification methods, which consider the capabilities of the terminal and characteristics of the transaction to prompt the cardholder for a specific method of cardholder verification.

If the first CVM in the CVM List that must be performed indicates offline PIN, the terminal prompts the cardholder for a PIN. The terminal transmits the cardholder-entered PIN to the card, which compares it to a Reference PIN stored secretly in the card. The CVM List may also specify other methods of cardholder verification, such as online PIN, signature, or no cardholder verification required. Under certain conditions, the terminal may use a default CVM as defined by the Credit Card Company.

2.2.6 Terminal Risk Management (mandatory)

Terminal Risk Management checks whether the transaction is over the merchant floor limit, the account number is on an optional terminal exception file, the limit for consecutive offline transactions has been exceeded, the card is a new card, or the merchant has forced the transaction online.

Some transactions are randomly selected for online processing. Terminal Risk Management also includes optional velocity checking by the terminal using data elements from the card. The card data elements used are those defined by Eurocard, MasterCard, and Visa (EMV) specifications.

Terminal velocity checking results are considered during Terminal Action Analysis. Visa recommends support for velocity checking by the card and the data elements used card velocity checks are defined by Visa. Card velocity checking results are considered during Card Action Analysis.

2.2.7 Terminal Action Analysis (mandatory)

Terminal Action Analysis uses the results of Offline Data Authentication, Processing Restrictions, Terminal Risk Management, Cardholder Verification and rules set in the card and terminal to determine whether the transaction should be approved offline, sent online for authorisation, or declined offline.

The card rules are set in fields called Issuer Action Codes (IACs) sent to the terminal by the card and the terminal rules are set in Terminal Action Codes (TACs). After determining the transaction disposition, the terminal requests an application cryptogram from the card.

The type of application cryptogram is based upon the transaction disposition with a Transaction Certificate (TC) for an approval, an Authorisation Request Cryptogram (ARQC) for an online request, and an Application Authentication Cryptogram (AAC) for a decline.

2.2.8 Card Action Analysis (mandatory)

Upon receiving the application cryptogram request from the terminal, the card performs Card Action Analysis where Card Risk Management checks may be performed to determine whether to change the transaction disposition set by the terminal. These may include checks for prior incomplete online transactions, failure of Issuer Authentication or offline data authentication failure on a previous transaction, and count or amount velocity checking limits having been reached.

The card may convert a terminal request for an offline approval to an online transaction or an offline decline, and the card may convert an online request to an offline decline. The card cannot override a terminal decision to decline a transaction. After completion of the checks, the card generates the application cryptogram using application data and a secret DES key stored on the card. It returns this cryptogram to the terminal.

For offline approved transactions, the TC and the data used to generate it are transmitted in the clearing message for future cardholder disputes or chargeback purposes, or both. The TC may be used as a 'proof' of transaction when a cardholder disputes a transaction and to verify that the transaction data has not been changed by the merchant or acquirer. For offline-declined transactions, the cryptogram type is an AAC.

2.2.9 Online Processing

If the card and terminal determine that the transaction requires an online authorisation, the terminal transmits an online authorisation message to the issuer if the terminal has online capability. This message includes the ARQC cryptogram, the data used to generate the ARQC, and indicators showing offline processing results.

During online processing, the issuer validates the ARQC to authenticate the card in a process called Online Card Authentication (CAM). The issuer may consider these CAM results and the offline processing results in its authorisation decision. The authorisation response message transmitted back to the terminal may include an issuer-generated Authorisation Response Cryptogram (ARPC) (generated from the ARQC, the Authorisation Response Code, and the card's secret DES key). The response may also include post-issuance updates to the card called Issuer Scripts.

If the authorisation response contains an ARPC and the card supports Issuer Authentication, the card performs Issuer Authentication by validating the ARPC to verify that the response came from the genuine issuer (or its agent).

Successful Issuer Authentication may be required for resetting certain security-related parameters in the card. This prevents criminals from circumventing the card's security features by simulating online processing and fraudulently approving a transaction to reset card counters and indicators.

If Issuer Authentication fails, subsequent transactions for the card will be sent online for authorisation until Issuer Authentication is successful. The issuer has the option to set up the card to decline the transaction if Issuer Authentication fails.

2.2.10 Issuer-to-Card Script Processing

If the issuer includes script updates in the authorisation response message, the terminal passes the script commands to the card. Prior to applying the updates, the card performs security checking to assure that the script came from the valid issuer and was not altered in transit. Supported script commands allow updating offline processing parameters, blocking and unblocking the application, blocking the card, resetting the Offline PIN Try Counter, and changing the Offline PIN value.

2.2.11 Completion (mandatory)

The card and terminal perform final processing to complete the transaction. An issuer-approved transaction may be converted to a decline based upon Issuer Authentication results and issuer-encoded parameters in the card.

The card uses the transaction disposition, Issuer Authentication results, and issuer-encoded rules to determine whether to reset card-based counters and indicators. The card generates a TC for approved transactions and an AAC for declined transactions.

If the terminal transmits a clearing message subsequent to an authorisation message, the TC is transmitted in the clearing message. With single message systems or systems involving acquirer host data capture of approved transactions, the terminal must generate a reversal for issuer-approved transactions which are subsequently declined by the card.

2.3 The Chain

This section describes the used components of the transaction chain, as mentioned in the introduction, in more detail.

2.3.1 Terminal

First of all, a terminal will read the chip on the credit card. For example the Trintech Smart 5000 terminal (see Figure 2.4). This is a terminal with a built-in EMV kernel. An EMV kernel handles the communication with the credit card through a flow of control (see Figure 2.6).

This Trintech terminal has a combined ICC/ Magnetic stripe reader. Each terminal must always have a magnetic stripe reader for backwards compatibility.

2.3.2 POS application

The POS application provides the merchant with a simple interface to enter the amount for the transaction and the currency. The POS application will then start communicating with the terminal to retrieve the required information from the card. It will send the information to the PSP, and handle the response of the PSP.

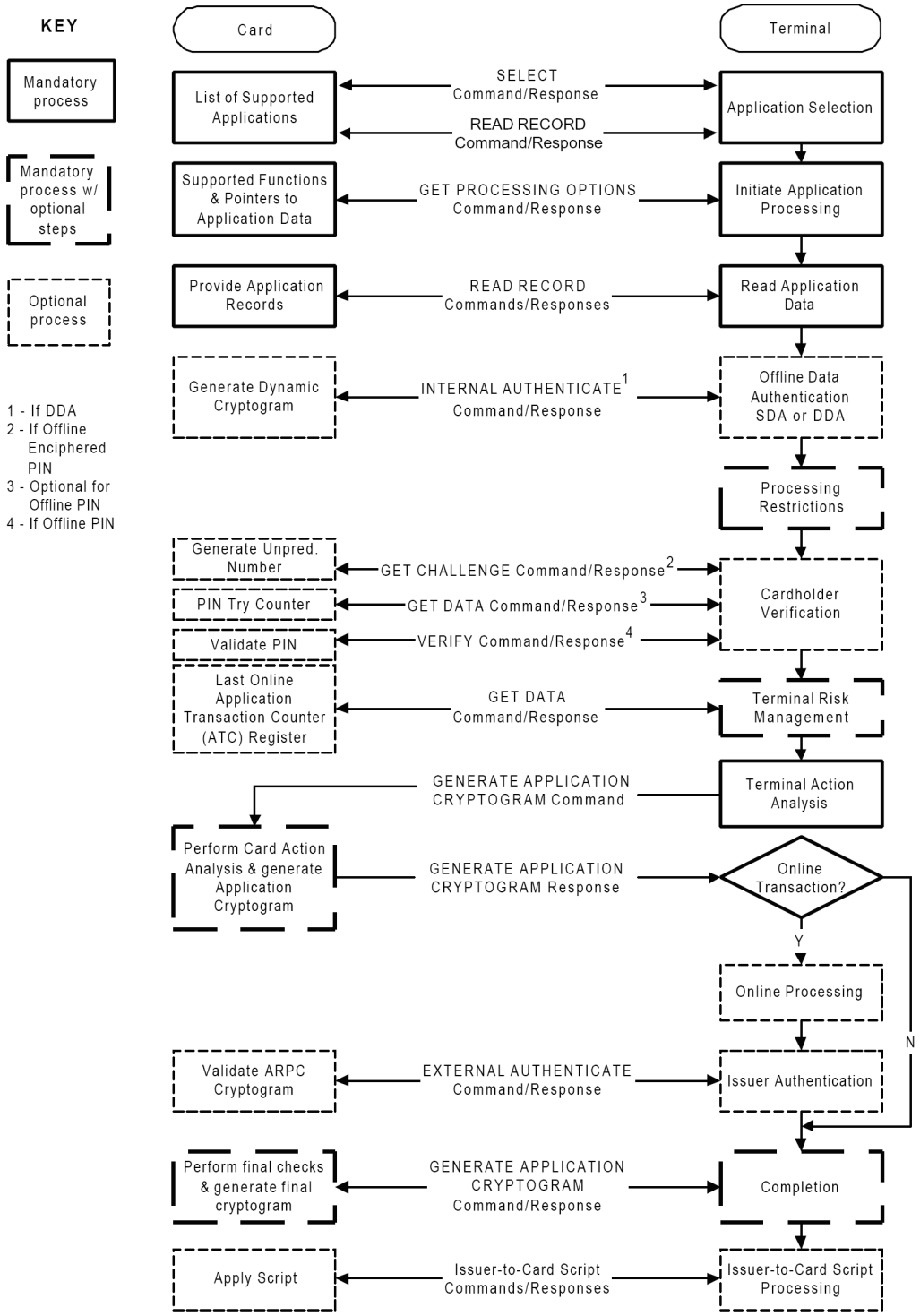


Figure 2.3: Sample Transaction Flow

Figure 2.4: Trintech Smart 5000

2.3.3 PSP

To the merchant, the PSP supplies one interface. The merchant will simply send a request to the system of the PSP and the PSP will figure out what kind of payment it is, perform the authorisation and do the capture and settlement. This request represents step 2 of Figure 2.2. To authorise the payment, the PSP system communicates to the different acquirers. The used reference PSP uses an XML interface.

This reference PSP system is not as simple as it looks like. At the moment it is performing up to 13 transactions every second. This number is increasing. Even the system is not using its maximum capacity, scalability is an important issue. The implementation of functionality in the PSP has, therefore, been split over various cells. Each cell represents a specific part of the PSP's functionality, and runs on a separate machine. For the most important cells the PSP has multiple active instances to balance the load. For every instance there is also at least one inactive instance for backup.

One of the measures taken to support lots of transactions is having multiple servers receiving transactions simultaneously. These servers are called shopper cells. A request from a merchant arrives at a shopper cell with the lowest load at that moment. This shopper cell will do the processing of that request. The next request from a merchant could arrive at a different shopper cell. Note that two different requests can be about the same transaction, so some special measures are taken to stay synchronised. Every shopper cell synchronises its transaction information to a central cell. The result is that this central cell contains all the information of all transactions. When a shopper cell receives a request that needs information of a previous request, and this previous request is not available locally, the request is forwarded to the central cell. More about the different requests, and requests that need information of a previous request is explained in Section 2.4.

Another measure to increase scalability is the acquirer cell. Every transaction has to be authorised by a certain acquirer. To perform an authorisation a connection to an acquirer has to be made for each transaction. Because there can be multiple transactions waiting for authorisation from an acquirer simultaneously, there are multiple acquirer cells, each with its own connection to the acquirer. This means that a transaction from a merchant can be authorised through acquirer cell one and another transaction through acquirer cell two.

Once every day the central cell creates a file containing all the authorised transactions that have to be captured (the merchant wants his money of course). This file is sent to the acquirer and the acquirer will send the money to the PSP. A simplified graphical view of the PSP system described above can be seen in Figure 2.5.

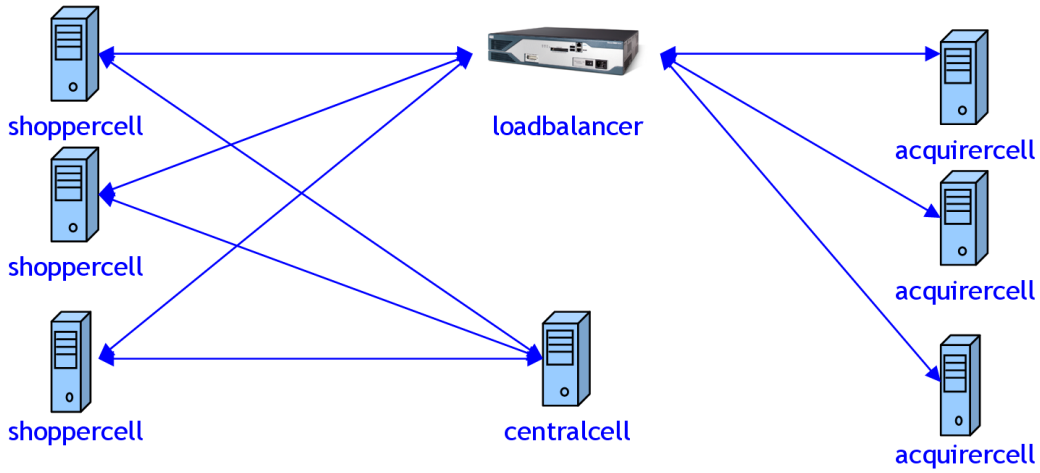


Figure 2.5: The PSP system

2.3.4 Acquirer

To authorise the payment, the PSP system communicates with the different acquirers. Communication with the reference acquirer is done through the APACS30 protocol [4, 5]. APACS30 defines the connection setup and the packages to be sent through this connection. The connection setup will be done using a X25 protocol. To implement this, the reference PSP uses Cisco X25 router. Packages to this router can be sent though a telnet connection. The acquirer is his place communicates with the different credit card companies if this is necessary.

2.3.5 Credit Card Company

The different credit card companies implemented the designed EMV standard in different ways. The consequence of this is that for every different credit card company there is a different test suite to test the implementation. The disadvantage of these different implementations is that for every credit card company these test suites must be performed during the certification process.

The communication with the credit card companies is done through the acquirer, so there is no direct communication with the credit card companies.

2.3.6 Issuer

The credit card companies handle the communication with the different issuers, a process of which we do not have visibility. This communication is not part of the EMV standard.

2.3.7 Overview

The focus of the Thesis lies on the first three components in the chain: terminal, POS application, and the PSP, including the communication between these components and the communication between the PSP and the acquirer. The other components are out of scope, because these are controlled by other companies who do not want to give inside information.

2.4 EMV Transaction

There are lots of ways for an EMV transaction to complete. The way chosen depends on the card and the terminal [11, 12, 13, 14].

A nice example of a choice to be made is whether the transaction can be authorised offline. The merchant can set the floor limit of the terminal. This floor limit indicates that the transaction must be authorised online when the transaction amount is above this limit. The card might want to authorise offline anyway, but the terminal will not allow this [11]. To achieve 100% online authorisation the floor limit must be set to 0. An overview of all the available EMV transaction can be seen in Figure 2.6. In the next section the different paths for this flow will be described in more detail. In this description our reference PSP is used as an example. When a payment request is sent the merchant will wait for the response of the PSP.

2.4.1 Payment requests

Offline authorisation

Offline authorisation is the process where the card will authorise the transaction. No authorisation request has to be sent to the acquirer to authorise the transaction. Offline authorisation can be useful in case of transactions with small amounts. The risk for such transactions will still be acceptable and the transaction will be authorised much faster.

For an offline authorisation transaction 1 or 2 requests are transmitted from the POS application to the PSP. The amount of requests depends on how the transaction will be captured. There are two types of flows possible:

1. Send an authorisation request to the PSP. The capturing of the payment will be done periodically by the PSP. For example every night.

2. First send an authorisation request to the PSP. When the authorisation is confirmed by the PSP, and by the merchant, a capture request is sent to the PSP. The capturing of the payment is done manually by the POS application.

Online authorisation

Online authorisation is the process with which the issuer will authorise the transaction. The card will generate an Application Request Cryptogram (ARQC), which will be sent to the issuer. The issuer will decrypt this ARQC and use this to generate an Application Response Cryptogram (ARPC). The ARPC will be sent back to the card and the card will validate this. If the ARPC is correctly validated, the card will authorise the transaction.

Online authorisation is mandatory in the United Kingdom above a certain floor limit. It is much more secure than offline authorisation, because the issuer will validate the card.

For an online authorisation transaction 2 or 3 requests are sent from the POS application to the PSP. The number of requests depends on how the transaction will be captured and if and how a Transaction Certificate is added to a payment. There are three types of flows possible:

1. First send an authorisation request to the PSP. When the authorisation is confirmed by the issuer, PSP and the merchant an Add Transaction Certificate request is sent to the PSP. The capturing of the payment will be done periodically by the PSP.

2. First send an authorisation request to the PSP. When the authorisation is confirmed by the issuer, by the PSP, and by the merchant an capture request is sent to the PSP. Within this capture request the Transaction Certificate is added. The capturing of the payment is done manually by the POS application.

3. First send an authorisation request to the PSP. When the authorisation is confirmed by the issuer, PSP and the merchant an add Transaction Certificate request is sent to the PSP. The third request that is sent is a capture request. The payment is captured manually.

Referral

When a merchant wants to authorise a payment, the response can be a referral. A referral response means that the payment is declined, but the transaction can be authorised with a special authorisation code. The merchant has to contact the issuer of the credit card to retrieve this authorisation code. After this code is committed to the PSP, the payment is authorised. When the merchant does not want to contact the issuer, or cannot contact the issuer, the payment stays declined.

The inserted authorisation code has to be sent to the PSP, this will cause an extra request. When an online authorisation payment is referred, the merchant sends 3 or 4 requests instead of 2 or 3 requests.

Fallback

When an EMV payment fails or can not be invoked, a fallback transaction is done. This means that a normal swipe payment is performed instead of the EMV payment. A fallback payment can only be done when, for example the credit card does not have a chip (an old credit card), or when the chip on the credit card is broken. When the terminal of the

merchant is EMV ready (it is able to handle EMV payments), and the credit card is EMV ready (and is not broken) there will never be a fallback transaction even if the customer/ merchant wants this.

Refund

A refund transaction is the opposite of a normal sale transaction: the merchant sends money from his bank account to the bank account of the customer. This is a simple transaction and only takes one request.

Cancel

When the merchant or the customer wants to cancel the payment during the payment process it could be possible that the payment is already authorised and even captured. When the payment has to be cancelled a cancel request is sent to the PSP to indicate that the payment is cancelled. When the transaction was already captured a refund is sent to return the money.

2.4.2 Synchronization

For one transaction there can be more than one request. For example, an online authorisation payment can have up to three requests. When a request is sent to the reference PSP it arrives at a shopper cell. There are different shopper cells. This implies that the shopper cell that receives the second request of a transaction can be different than the shopper cell that has received the first request. The consequence of more then one shopper cell is that there has to be some synchronisation with the central cell. For example, a capture request need some information from the first authorisation request. When this request arrives at different shopper cells then the authorisation request the payment of the capture is not know.

When a shopper cell receives an authorisation request this information is also emitted to the central cell (see Figure 2.5). The central cell saves this information into a database. When a shopper cell receives a request that is not an authorisation request, for example a capture request, it needs to know if the payment is authorised and even exists in the PSP. When the shopper cell of the authorisation request is different from the shopper cell of the capture request it will not have this information. If a shopper cell receives such a request, this request is passed on to the central cell. Every shopper cell synchronise its information with the central cell, therefore the central cell has all the information of every payment. The central cell handles the request and sends a response to the shopper cell. The shopper cell forwards its response to the merchant.

2.4.3 Message flow

In Figure 2.6 you can see a control flow of different requests and responses. From this flow can be seen that a payment can be authorised if the entered PIN is correct, but it is possible that also the signature has to be checked. When the signature is not correct, the merchant can decline the payment even when the payment is authorised by the issuer. When this is the case, a cancel request is send to the PSP and the payment is cancelled.

A refund can only be done after the transaction is captured. The maximum amount of this refund is the original transaction amount. When the merchant wants to do a refund for a transaction that is not yet been captured, the merchant must cancel the transaction.

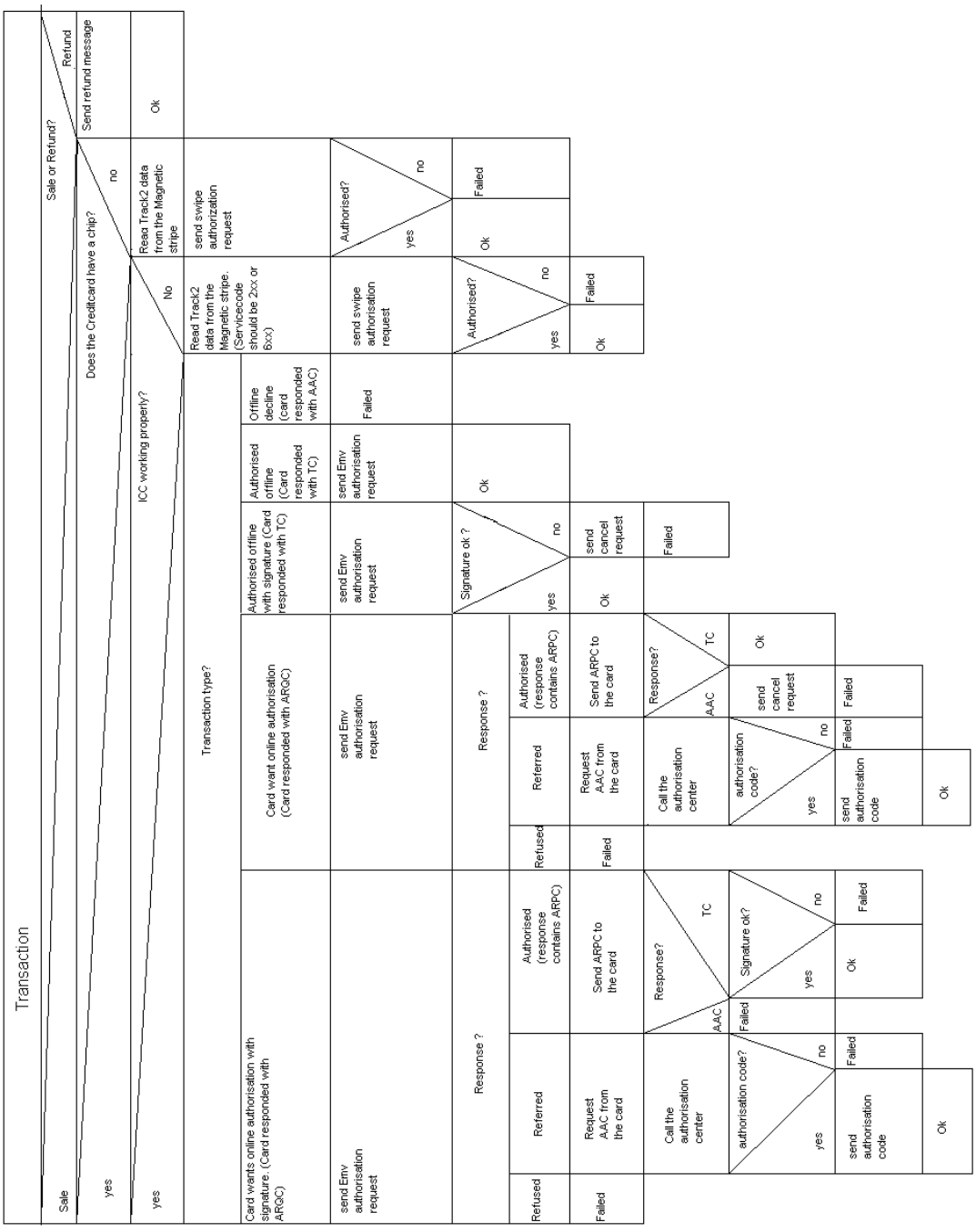


Figure 2.6: Control Flow

Chapter 3

Analysis and Critical Evaluation of the Certification Process

To be able to answer the first research question the certification process is described in more depth in this chapter. The reason why a certification process is needed is pointed out first. After this short introduction, a description is given of what includes the certification process. The next section describes the difference between the regular certification process, and the EMV certification process. A performed life certification is described, followed by analysis of the individual components, and the integration of the components, in the chain. The chapter ends with a critical evaluation, and a short summary and conclusions.

3.1 Why a Certification Process?

The main reason why a certification process is needed, is to prove that a component, or a chain of components is able to handle a transaction properly (request and response). When the certification process is carried out with a positive result, a certificate is provided. This certificate indicates, that the component, or the chain of components can handle credit card transactions properly, and is aloud to process credit card transactions.

3.2 What Includes the Certification Process?

In short: the certification process includes running different test transactions (of one or more brands) that should have an expected outcome. When all test transactions have this expected outcome, and all the results are checked by the Certification Authority, the certification process is succeeded. Which tests are applicable for the chain of components that needs to be certified is decided by the Certification Authority.

Because a PSP can decide which brands need to be supported, there is a separate part in the certification process for every credit card brand. Each brand has a different amount of test that needs to be performed with success. For larger brands, like MasterCard and Visa, there are more test transactions than for a small brand, like Maestro and JCB. In Table 3.1

Brand	Total amount of tests
Visa	51
MasterCard	45
Maestro	31
Interop	30
Laser	18
Maestro UK	9
JCB	6
MagStripe	6
Online	6
Solo	6
Total	202

Table 3.1: Amount of test transactions per brand

an overview is given of the total amount of test transactions for each brand. All the test transactions of a brand together are also called a test suite.

A test transaction consists of a specific test credit card and a test script. The test script describes which handling should be followed to perform the test transaction.

3.3 Certification Process in More Detail

There are two certification processes: a regular certification process for traditional swipe and keyed transactions, and an EMV certification process which is for traditional swipe and keyed transactions, but also for EMV transactions.

3.3.1 Regular Certification Process

For the regular certification process certifying the individual components is sufficient. When a certain chain of components is certified, and one of the components is changed, a re-certification of the whole chain is not necessary. It will be sufficient to only certify the component that is changed. For example, when there are two chains of different components (and the interfaces of the terminals are identical) the terminals in the two chains can be exchanged without re-certifying the chains.

The information fields that need to be processed with traditional swipe and keyed transactions are the card number, card holder name, and the Cardholder Verification Code (CVC).

The regular certification process is shown in Table 3.2. As first action the Solution Questionnaire must be filled in (step 1). This document indicates which credit cards will be supported, like MasterCard, VISA, Solo, Maestro, and/or JCB. After sending this document to the Certification Authority, it will send back which test eventually should run correctly to get a certificate (Step 2). The PSP should run all the tests and submit all the test results to the Certification Authority (Step 3). After the Certification Authority has collected all the information it will check the submitted results against the expected results. After these

	Action	Estimated Time
1.	Solution Questionnaire	1 day
2.	Technical schedule & Relevant test scripts from Certification Authority	5 days
3.	Run tests, Receipt processing, Fill in and submit test results	2 days
4.	Results back from Certification Authority	5 days
5.	Fix issues and redo number 4	? days

Table 3.2: Regular Certification Program

checks, the Certification Authority will inform the PSP on the results of its inspection (step 4).

When there are (small) issues, these issues must be resolved (step 5). After resolving these issues, the faulty tests (maybe all) must be rerun. Note that Step 3, step 4, and step 5 indicate a cycle. The amount of time that this cycle will take is not known, and depends on the amount of issues found during step 4. When all the issues are solved, and all the tests run properly a certificate is granted.

A certification process consists of multiple test transactions. Each test transaction has a test script which indicates how the test should be performed, what is tested, and what the result should be. Below an example from the Switch/Maestro brand test suite.

```
Test NO: ST1
Test Card Number: **** **** **** 5679
Type of transaction: Keyed
Transaction amount: 1,0000.01 GBP
Extra transaction data:
- Start date: 01/2006
- Expiration date: 02/2009
Expected result: Rejected
Reason: Amount is above ceiling limit
Check:
- If a transaction that is above ceiling limit is rejected.
- If the application can handle start date and expiration
   date
Flow: Enter the amount, the transaction should be keyed with
      the given extra transaction data
```

This specific test transaction tests if the application is able to handle transactions that are above the ceiling limit. Switch/Maestro credit cards sometimes have a start date (instead of only an expiration date). This is also tested in the same test. The ceiling limit for the certification process should be 1,000 GBP. All transactions above this limit should be declined. Because this transaction is above this limit it should end in a refusal for a successful test result.

3.3.2 EMV Certification Process

The new EMV standard also comes with a new certification process. The EMV standard has more data fields then only a card number, card holder name, and a CVC, like the most magnetic stripe and keyed transactions. Also the card itself is more complex: a micro chip instead of a traditional magnetic stripe. The disadvantage of this is that the certification process is also more complex. The request to and response from the issuer contains more data. So not only the value of the card number, card holder name, and CVC should be correct, also many other data fields should have a correct value. For every transaction, all these data fields must be sent through the chain of components, so they can be checked. Because of these extra data fields, the higher complexity of the process, the whole certification process takes more time than regular certification process. Also when one of the components in the chain is different, the whole chain must be certified again.

The EMV certification program [2] is shown in Table 3.3. The first action to be taken is completing in the Chip & Pin Solution Questionnaire (step 1) [3]. This is a document with the specification of the components in the chain. The document indicates, for example, whether the terminal is able to go online, is attended or unattended, combined ICC magnetic stripe, etc. The document also indicates which credit card brands must be supported, like MasterCard, VISA, Solo, Maestro, and/or JCB. The document must be completed by the PSP that wants to certify a specific combination of components.

After sending this document to the Certification Authority, they will request a MasterCard Terminal Integration Process (TIP) (step 2). This TIP indicates which test eventually should run correctly to get a certificate from MasterCard. This TIP depends on the capabilities of the terminal, stated in the Chip & Pin Solution Questionnaire.

When the Certification Authority receives the TIP from MasterCard, the relevant scripts from MasterCard and other relevant credit card brands are put together (step 3) [26].

The Certification Authority will send the relevant tests of all the test suites to the PSP, who can start the pre-certification (step 4). During the pre-certification the PSP performs all the required tests himself. When all tests run properly, the PSP must submit the results of all the tests to the Certification Authority.

After the Certification Authority has collected all the information, it will check the submitted results against the expected results. The Certification Authority will inform the PSP with the results of its inspection (step 5). When there are issues found (which is mostly the case the first time), these issues must be resolved (step 6). After resolving these issues, the faulty tests (maybe all) must be rerun. Note that Step 4, step 5, and step 6 indicate a cycle, and therefore the time that this cycle will take is not known. This depends on many factors, like how many issues came up during inspection, what is the complexity of the issues, etc.

When all the issues are solved, and all the tests run properly, an onsite testing is arranged (step 7). During this onsite testing the Certification Authority comes onsite at the PSP to redo all the entire test suites that the PSP has already done during pre-certification. The main reason for this is that the Certification Authority must know for sure that the submitted results during pre-certification are really the results from the stated configuration, and not manipulated in some way.

	Action	Estimated Time
1.	Chip & Pin Solution Questionnaire	1 day
2.	MasterCard TIP Request	5 days
3.	Technical schedule & Relevant test scripts from Certification Authority	10 days
4.	Run tests, Receipt processing, Fill in and submit test results	5 days
5.	Results back from Certification Authority	10 days
6.	Fix issues and redo number 4	? days
7.	Onsite testing	3 days
8.	Results back from onsite testing (also from MasterCard)	15 days

Table 3.3: Current Certification Program

After the onsite testing is performed these results will be checked again by the Certification Authority, but also by MasterCard (step 8). Because the Certification Authority has to pay MasterCard (and the PSP in his turn to the Certification Authority) for every attempt to get the results checked by MasterCard, the Certification Authority only sends in the result if they are sure that they will pass. When MasterCard does not find any issues a certificate for this specific chain of components is granted.

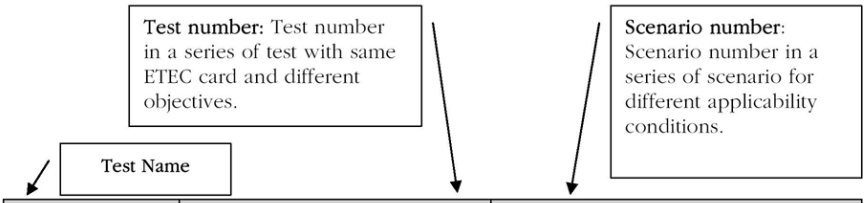
The whole certification process takes 3 to 6 months [2]. The possible delays in this process are step 4, step 5, and step 6, because it is unpredictable to indicate how long it will take to solve the issues that were revealed during pre-certification.

In Figure 3.1 can be seen how a test script for an EMV test transaction should be interpreted. In Figure 3.2 you can actually see how a script looks like for a MasterCard brand test transaction. This specific test transaction tests if the terminal behaviour is correctly when Card Authentication Method (CAM) is not supported by the card. Card Authentication Method (or Online Card Authentication) is a validation of the card by the issuer to protect against data manipulation and skimming [11]. When the result of this test transaction is an authorisation response, the test is successful.

3.4 Life Certification

To gain more practical information about the EMV certification process a life certification is performed at the reference PSP, with a specific chain of components. This practical information will be helpful for the evaluation of the EMV certification process and for proposing improvements. In this section an overview is given of the different steps that are performed through the whole certification process.

The introduction of EMV at the reference PSP started in October, 2003, by Willem Lobbezoo. He performed a lot of pre-research about EMV. Also the performed Bachelor Thesis [9] by me, and 3 fellow students, contributed to this pre-research.



REQ01 MASTERCARD	Test 01	Scenario 01
Objective	*Test Objective*	
Applicability Condition	*Terminal condition to fulfill to run the test scenarios.*	
Transaction Type	*Credit: Credit transaction* *Debit: Debit transaction* *Credit – Debit: depending on applicability conditions, transaction can be either credit or debit.*	**Online Test**: *- Yes: This scenario requires terminal to be connected to simulator for authorisation* *- No: This scenario does not require terminal to be connected to simulator*
Reference Documentation	*Specifications references for the test*	
Card configuration	*Card configuration to match test requirements*	
User Action	*Action to perform to run the test*	
Issuer simulator Configuration	*Issuer simulator Configuration requested to run the test scenario*	
Pass Criteria	*Conditions of test validation*	
Note	*Various information on test scenario, card or simulator*	

Figure 3.1: Test Scenario Description

3.4.1 Preparations

Before the certification process started a couple of decisions had to be made, which will be discussed in this section.

One of the decisions is which brands the chain of components should support. For each brand a specific suite of test transactions must be performed. The more brands the chain must support, the more test transactions that must be performed. In Table 3.1 shows the amount of test transactions for each specific brand. There are also brands that are only issued in specific countries, like the Maestro UK brand. Cards for these brands can only be used in the UK.

The reference PSP wants to support the following brands: Visa, MasterCard, Maestro, Interop, Online, and some specific UK brands (Maestro UK, MagStripe, Switch, and Solo). The Visa brand is a separate test suite. MasterCard, Maestro, Interop, Online, and the specific UK brands are collected in the ECMC test suite. These 2 test suites (Visa and ECMC) are the 2 largest test suites on the marked. The ECMC test suite is the largest one, and MasterCard has the largest amount of tests in the test suite. The amount of brands that

REQ01 MASTERCARD	**Test 01**	**Scenario 01**
Objective	To ensure that the terminal correctly behaves when offline CAM (both SDA and DDA) is not supported by the card.	
Applicability Condition	Terminal supports MasterCard. Terminal is offline with online capacity.	
Transaction Type	Online Credit-Debit	**Online Test**: Yes
Reference Documentation	See document [2], chapter 3: CAM requirements for terminals.	
Card configuration	The AIP (tag 82) returned by the ICC during GET PROCESSING OPTION command indicates that ICC does not support Offline Data Authentication (tag 82 = 18 00 => only CVM and Terminal risk management supported), and no data related to data authentication in the ICC.	
User Action	Please, use the following test card: REQ01 MASTERCARD / 5.0.A Insert card in the chip reader and follow the instructions. Amount must be equal to 000000001500 or 000015000000. For REQ01 MASTERCARD / 5.0.A test card, PIN value is 4315 (if requested).	
Issuer simulator Configuration	Issuer response message: DE 039 (Response code) = '00' (Approved). DE 055 - PDS 91 (Issuer Authentication Data) is present. Issuer script = none.	
Pass Criteria	MasterCard application is selected. In response to the Get Processing Options command with AIP indicating that chip card does not support offline Data Authentication, the terminal must continue the transaction without performing either Static or Dynamic Data Authentication. The following TVR bit(s) must be set: TVR byte 1, bit 8 = '1' --> Offline data authentication was not performed As per TAC settings, the terminal must request an online authorization. The transaction will be approved.	
Note	N/A	

Figure 3.2: Scenario for MasterCard REQ01 Test 01 Scenario 01

will be supported by the chain also influences the time of the certification process. The more and bigger the brands, the longer the certification will take, because the amount of tests that need to be performed increases.

Within each test suite of a brand there are some test transactions that must be performed in a certain way, depending on the kind of terminal that is used. An import difference is attended and unattended terminals, because there is no merchant present at an unattended terminal. For example, at an unattended terminal the shopper can not write down his signature, because the merchant can not verify this signature. Therefore, an unattended terminal

can not fall back to signature when the shopper has 'forgotten' his PIN code.

An other important decision is which components must make up the chain, because the certificate is only valid for a specific chain. The terminal that is used for the certification is the Trintech Smart 5000 (Figure 2.4). The reason why this terminal is picked is because this terminal was the first terminal that came available when the reference PSP started the process to make the PSP application EMV enabled. The Trintech terminal is EMV compatible and EMV level 2 certified. This means that the terminal is aloud (by the Certification Authority) to process EMV transactions.

During the certification process the Certification Authority makes a difference between 4 types of terminals:

1. attended device
2. unattended device
3. attended device with separate reader
4. attended device with combined reader

There are general tests that must be performed for all 4 types of terminals, but there are also specific tests for attended and unattended terminals. For example: a test to verify a signature is only applicable for attended terminals, because this involves human interactions.

The reference PSP is used as PSP (of course). The reference PSP has an alliance with an acquirer, which is also the reference acquirer.

Because the acquirer (and all the components behind the acquirer) are EMV compatible, and the terminal is EMV compatible, the only thing that must be made EMV compatible is the reference PSP. This was done by extending the current functionality with the EMV functionality.

The communication between the terminal and the PSP is handled by a POS application that had to be build from scratch. The POS application is the interface to the merchant where he can enter a description and an amount for the transaction. The POS application is also able to handle keyed transactions, and refunds.

The first step of the certification process is to fill in a Chip & Pin Solution Questionnaire. By filling this in the Certification Authority can collect all the relevant tests for the chain that the PSP wants to certify.

3.4.2 Pre-certification

When all relevant test scripts were known, and all test cards were available, the pre-certification started. During the pre-certification the PSP itself performs all tests. Most of the time there will be a couple of failing tests, at the beginning. These tests should be investigated, and figured out what went wrong. After the issue is found, it can be resolved.

After all the issues are resolved, the failed tests must be performed a second time. When they still fail, the process must be repeated until all tests have a successful result.

3.4.3 Send in Results

After all tests are performed and when they all have a positive result, all information must be sent to the Certification Authority. This information includes:

1. Test results
2. All the receipts from every transaction (merchant receipt and customer receipt)
3. All log files of the communication of the terminal and the card
4. capture file

The log files of the communication of the terminal and the card are also called sniffer logs or smartspy logs. These logs are retrieved with a sniffer device (see Figure 3.3). This is a piece of equipment which must be put between the card and the terminal. The card is not inserted into the terminal, but into the sniffer device (1), and the sniffer device is inserted into the terminal (2). In this way the sniffer device can collect all the data that is sent between the terminal and the ICC of the card. After the transaction this data can be retrieved by connection the sniffer device to a computer.

The capture file is a separate file that informs the acquirer which amount should be captured from which credit card account.

3.4.4 Results Back

After the Certification Authority had sent back the results from the first pre-certification, a couple of major, and minor issues were found. One of the issues was about the sequence number of the authorisation message that was sent to the acquirer. Because the intention was to collect for each transaction a separate log file of the PSP, the system was started and stopped before and after each transaction. This resulted in a reset of the transaction counter for each transaction. This was not allowed by the acquirer, but was not specified. After fixing these issues, a whole new pre-certification was needed.

After the second pre-certification there were still new issues that were not found during the first pre-certification round. An issue that came up during the second pre-certification was that there were no receipts. This was also the case with the first pre-certification, but was not mentioned at that time. The requirement of collecting the receipts of each transaction was also not specified. An other issue was about the handling of referrals by the reference PSP. This is different then described by the Certification Authority. Some explanation and discussions were the result.

After 7 pre-certifications almost all issues where solved. A lot of issues that were found during each pre-certification could difficult be discovered on beforehand, because they were not specified, or they were only explained in less detail.

3.4.5 Onsite Testing

When almost all the issues were solved after the 7^{th} pre-certification, an onsite testing was arranged. During this onsite testing an employee of the Certification Authority came onsite

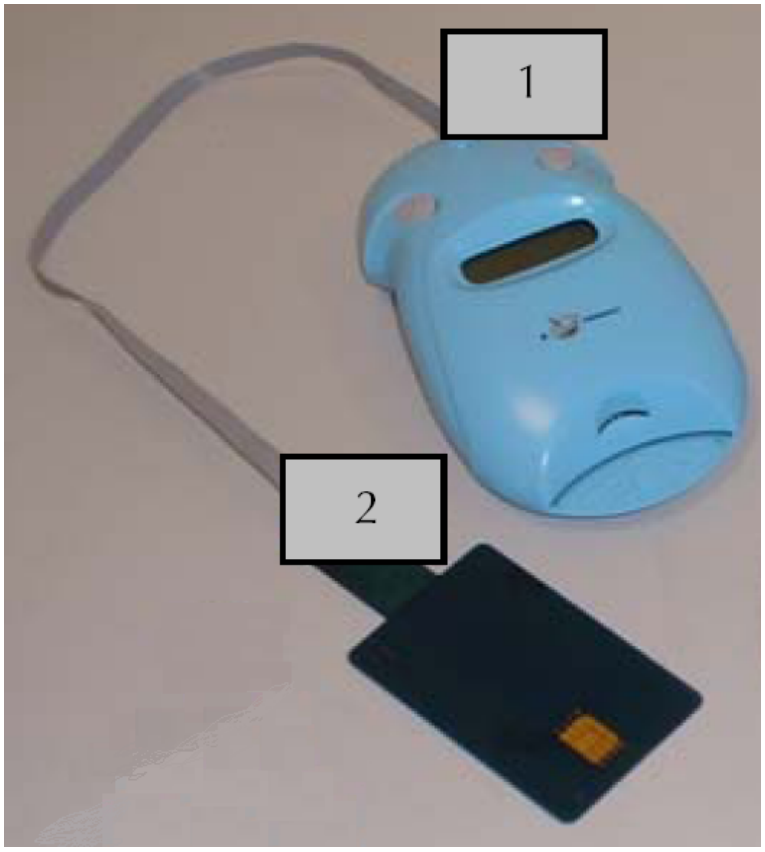


Figure 3.3: Sniffer Device (Smartspy)

at the reference PSP to perform all the required tests. During the onsite certification the sniffer logs are inspected in more depth by the Certification Authority then during the pre-certification.

MasterCard has a much more strict policy than for example Visa. Therefore all the MasterCard tests must be performed onsite by the Certification Authority, but not all Visa tests. It is enough that all the Visa tests are checked during the pre-certification, and only a subset of this during the onsite testing. The onsite testing was performed on February 27 and February 28, 2007.

After the onsite testing, two new issues were found. One of the tests had the correct outcome, but one of the last steps in the process was missing. This was only clear after studying the sniffer log of the specific test in more detail. For this reason the issue was not revealed during the pre-certification. The other issue was seen during the pre-certification by the Certification Authority, but was not indicated as an issue.

3.4.6 Extra Pre-certification

Because there were still some minor issues during the onsite testing these had to be resolved. After resolving, it was not necessary to do a new onsite certification. The tests that indicated an issue should be retested, and all the test results should be committed to the Certification Authority (as in the pre-certification).

3.4.7 Certificate

After the results of the onsite certification (including the results of the extra pre-certification that was performed after the onsite certification) were checked by MasterCard, the certificate was granted on May 22, 2007. During the official certificate give out ceremony one week after, a delegation of the Certification Authority came to the reference PSP to grand the certificate (see Figure 3.4).

Figure 3.4: The Head of Development congratulates the author with passing EMV certification while the Certification Authority delegation is watching

On the 15^{th} of June, 2007, the first real certified EMV transaction was performed by myself. See Appendix B for screenshots of the merchant interface screens of the transaction.

3.4.8 Conclusions of the Life Certification

The Certification Authority found new issues during the first 7 pre-certifications. The result of this was that a lot of test were performed multiple times. After the onsite certification the Certification Authority found an other issue that was not spotted during the

pre-certifications. Because the high amount of iteration during the pre-certification process, and the issues that were found after the onsite certification, the whole certification process took about 9 months.

3.5 Individual Components of the Chain

The chain that is being certified during a EMV certification process consists of different components. When one of these components is changed, the whole chain must be certified again. When it would be possible to reuse certain certified parts of the chain (so that these parts do not have to be re-certified in the chain) the certification process could be optimized. In order to arrive at this point, in this section an overview is given of the different components in the chain. This is done by discussing the specification, and how this specification is tested, of each component in the chain. With this information an evaluation can be done what the test quality is of the used components in the chain.

3.5.1 Card

The card specification is given by the EMV standard. Each card that is issued is configured by the issuer. This process and the testing of a card is out of scope, because no inside information is available.

3.5.2 Terminal

The EMV specification specifies the terminal component. There are different levels of specification. For example: a part of the specification described the value of the voltage that the ICC on the card must use, and an other part of the specification describes the bit that must be set in the TVR when the card is expired.

Every terminal that is used for EMV transactions must be have an EMV Level 2 certificated before can be used for the certification process [10]. This EMV Level 2 certificated indicates that the terminal is already certified, tested, and is aloud to process EMV transactions. Therefore the testing of the terminal component is already handled by an other certification process. When the terminal has no EMV Level 2 certificate, the Certification Authority will never certify the chain with such a terminal.

3.5.3 PSP

The reference PSP has a very large application written (mostly) in Java. An important thing to mention is that there is almost no specification of the application! The PSP is started as a small company and is extended every time with new functionality, but without any specification of the application.

It is unfeasible to come up with a specification of this PSP component, because taking the size of the application into account, it will take a long time. The most important functionality of a PSP is that transactions can be authorised, cancelled, captured, and refunded.

The testing of the PSP component is done with JUnit [23]. JUnit is a powerful tool written in Java that is able to run different test cases automatically. With these JUnit tests the internal functionality is tested. There is also a home-made application for regression testing. This application sends requests to the PSP and analyses the response.

A technique to test the coverage of the JUnit tests is Clover [8]. This technique is currently not used by the PSP. Therefore now exact knowledge about the test coverage is known. The senior developers estimate that the coverage of the JUnit tests is less then 25%. The regression testing tests the whole transaction process from begin to end. These test have an estimated coverage of 40%.

3.5.4 Acquirer

There is almost no specification available of the reference acquirer's system. An acquirer should be able to authorise, cancel, capture, and refund a transaction. There are also acquirers that can handle an authorisation and a capture request at once. How an acquirer implemented this functionality, and how it is tested, is out of scope, because of the lack of information.

3.5.5 Credit Card Companies

The communication with the credit card companies is done through the acquirer, so there is no direct communication with the credit card companies. The credit card companies should provide the same functionality as the acquirer, and must have a connection with all the issuers. How the credit card companies implement and test this functionality is also out of scope, because there is no information available how this is done.

3.5.6 Issuer

The credit card companies handle the communication with the different issuers, a process of which we do not have visibility. This component is not part of the EMV standard, and out of scope.

3.6 Integration of Components of the Chain

Different component providers (terminal manufactures, PSPs and acquirers) have already specified protocols between the components. In this section the integration of the components that are used during the life certification is discussed. Most of them use their own specification and protocol. Because a PSP only communicates with the terminal on one side, and the acquirer at the other side, the most important protocols in the chain for the PSP are the protocol between the terminal and the PSP, and the protocol between the PSP and the acquirer.

3.6.1 Terminal and POS Application

The specific implementation of the specification for the Trintech Smart 5000 terminal was given by the Terminal Manufacturer. This specification was very brief: a small text document, and a Microsoft Windows help file containing a list of all the (simplified) requests and responses that the terminal can handle. To retrieve the exact interface of the terminal's dll it was analysed with a simple text editor. This was a very time consuming and primitive way, but there was no other solution. Because the POS application was planned to be written in Java, a new dll (written in C++) was implemented to communicate through native methods with the terminal. This communication process is proprietary, and therefore only used for this POS application. A flow of commands that must be sent from the POS application to the terminal can be seen in Figure 3.5, Figure 3.6, and Figure 3.7.

To initiate the terminal a separate initiate command must be given. After this initiate command, the POS application can communicate with the terminal by different command codes. For example, the 02 command is to read the magnetic stripe and the 03 command is to read the ICC (Figure 3.5).

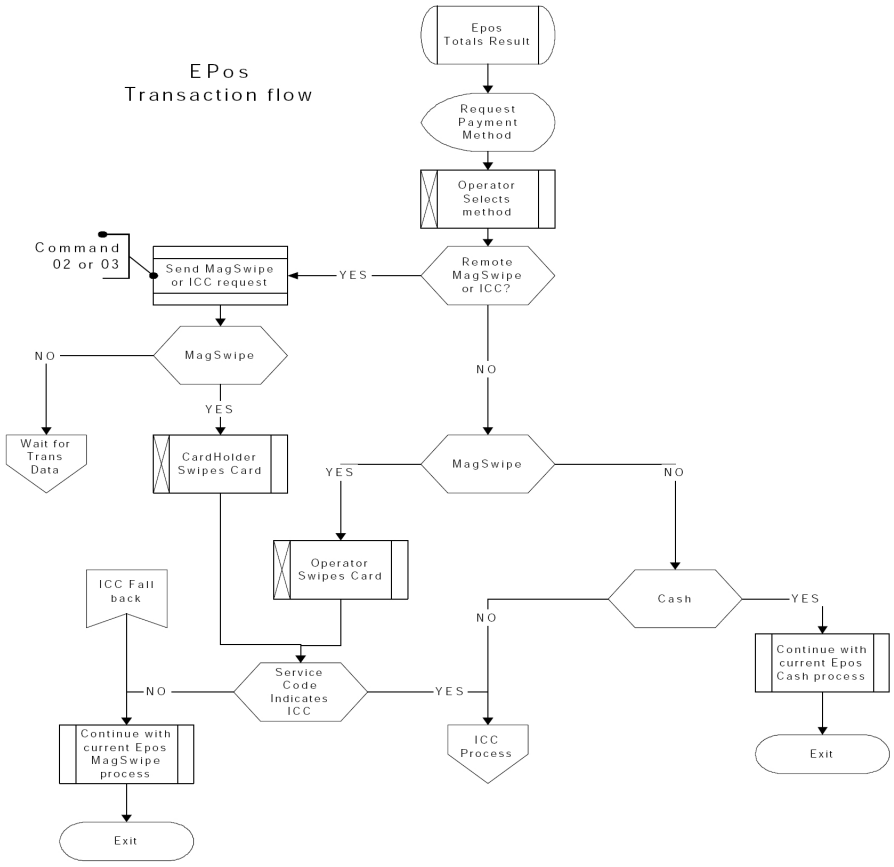


Figure 3.5: POS Transaction Flow

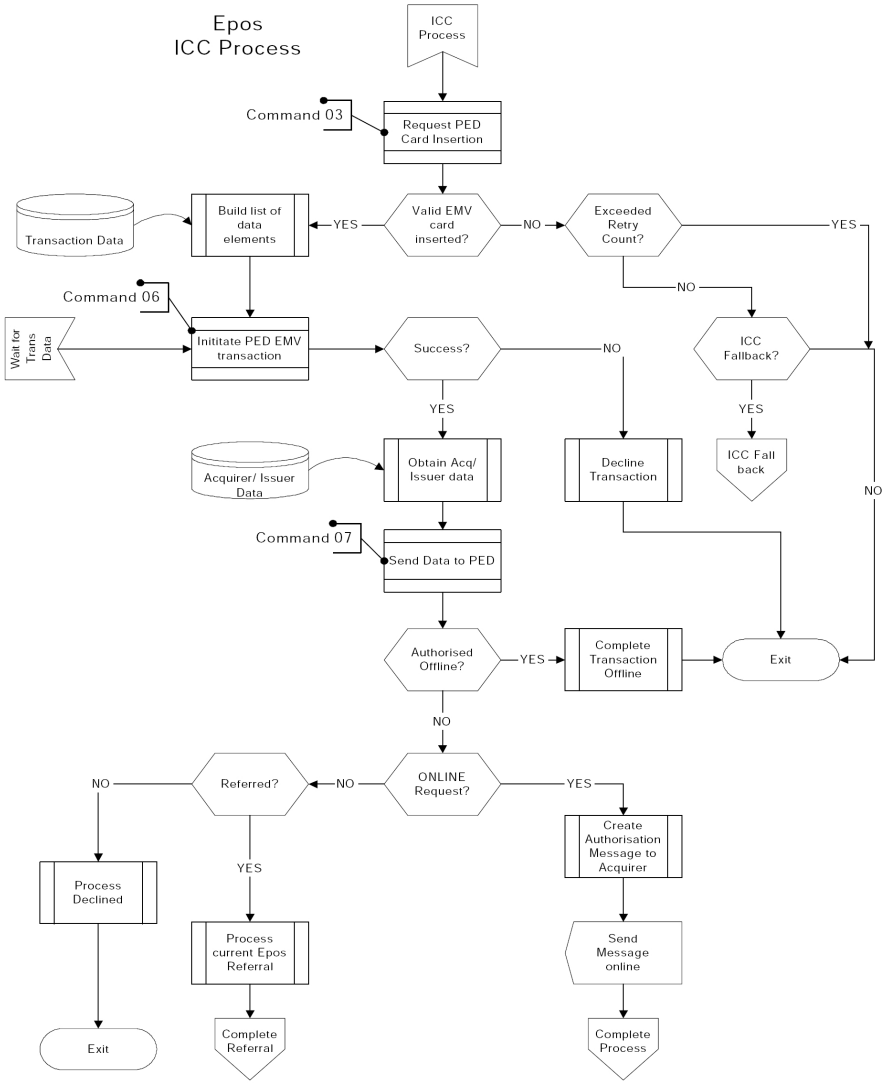


Figure 3.6: POS ICC Process

3.6.2 POS Application and PSP

The reference PSP is using a Document Type Definition (DTD) [34] as protocol specification. The DTD specifies how a XML response and request looks like, and what sort of information each field contains. Because EMV needs more data fields then the standard swipe transactions, the reference PSP's DTD needed to be extended when EMV was introduced. This new functionality, including the new tags, are described in a new document, which is an extension of the PSP's current documentation [25].

The reference PSP has already a testing mechanism implemented. Instead of the life url that is used in life production, a test url can be used. Behind this test url a simulator is

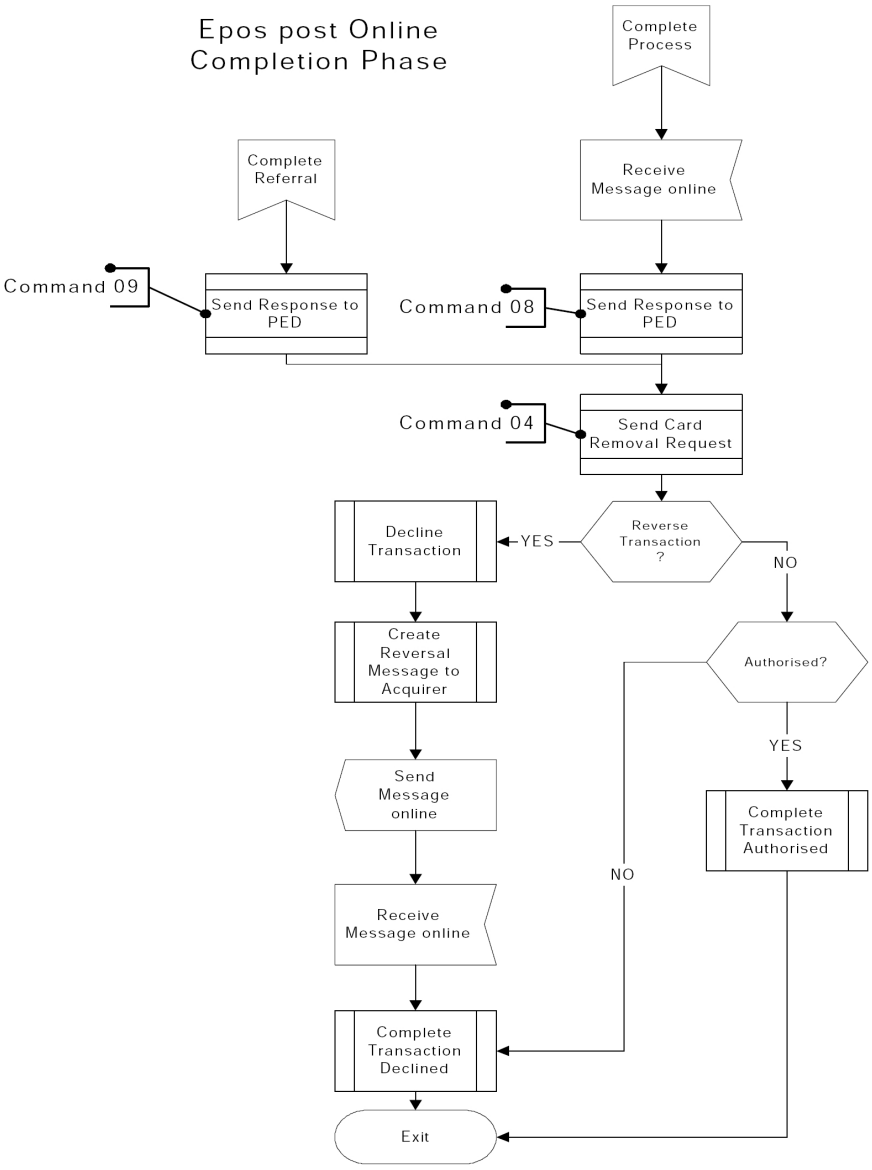


Figure 3.7: POS Online Completion Phase

running which sends a different response back depending on certain values in the request.

To be able to test the new EMV functionality, the simulator is extended with a connection to the simulator of the acquirer (see next section). When the PSP receives a response, the response is forwarded to the acquirer. The response that comes back from the acquirer is converted to proper XML response and returned to the POS application. In this new situation the PSP simulator works the same as in life, but without really processing the transaction (transferring money).

3.6.3 PSP and Acquirer

The protocol that is used for the communication between the PSP and the acquirer is APACS30 [5, 4]. The connection to the reference acquirer can be tested to the simulator of the acquirer. Depending on the request that the acquirer receives, a proper response is returned to the PSP.

3.6.4 Acquirer and Issuer

Because there is no information available about which protocols are used between the acquirer and the different issuers. This part of the communication is therefore out of scope.

3.7 Critical Evaluation

3.7.1 Certification test suites

To investigate the quality of the EMV certification process research has been done after the test suites of the two main credit card companies, Visa and MasterCard. For each test suite all the tests are investigated and checked which part of the specification of the EMV standard is tested (see Appendix C). Also the performed live certification was very helpful, because by performing each test in live, the outcome of the tests, and what is tested by each test, is checked in more detail.

To be able to draw conclusions about the quality of the EMV certification process, test coverage criteria must be selected. To achieve 100% path coverage is in general not possible. Therefore branch and statement coverage are accepted today as the minimum mandatory testing requirement. This can be done by executing enough test to assure that every branch alternative has been exercised at least once under some test [6]. In other words, the minimum testing that should be done for the EMV certification process is 100% branch coverage.

With the knowledge what is tested by which test (Appendix C), the branch coverage for each test suite can be calculated. This is done by mapping this knowledge to the specification of the EMV implementation. This mapping is done for each step of the 11 steps of the EMV specification. A more detailed description of the results of this mapping can be found in Appendix D. A summary of the number of covered branches can be found in Table 3.4.

The branch coverage of the two discussed test suites can be calculated by dividing all the covered branches by all branches:

1. Visa: 67% branch coverage
2. MasterCard: 66% branch coverage

The total coverage of both test suites together is 73%. Now we come back to the first research question: ”How do the provided test scripts of the card companies meet the requirements/ specification of the EMV standard? In other words,what’s the quality of the current EMV certification process?”. For both test suites the minimum mandatory testing requirement of 100% branch coverage is not met, which indicates a pour test quality of the EMV certification process.

EMV step	# branches	# covered branches		
		Visa	MasterCard	together
1	48	35	34	37
2	14	11	10	11
3	60	38	33	38
4	22	15	12	15
5	49	34	30	37
6	27	18	22	22
7	22	15	15	15
8	0	0	0	0
9	12	7	8	8
10	8	1	7	7
11	16	12	13	13
	278	186	184	203

Table 3.4: Covered branches of the test suites

3.7.2 Individual Components of the Chain

The individual components in the chain that is being certified are all very different. The EMV specification only specifies the functionality of the card and the terminal component. The testing of these components is handled by other parties. Therefore there is no knowledge about how this is done, and what the coverage of the tests is.

Testing the reference PSP is done with JUnit. 100% test coverage for unit test is essential. For larger systems, like the reference PSP, unit test coverage of 75% - 85% is acceptable [6]. The reference PSP has an estimated unit test coverage of less then 25%. This is much less then the accepted coverage percentage. Some parts of the system are also tested with regression testing, which has an estimated specification coverage of 60%.

Both coverage percentages are very low, and do not met the acceptable values described by the literature, but in practise it seems enough for the PSP to process millions of transactions each month.

3.7.3 Protocols Between Components of the Chain

To judge the quality of the protocol between the terminal and the POS application is very hard, because there was almost no protocol description. This makes it even harder to test, because the results can not be compared to the expected results.

The protocol between the POS application and the reference PSP is specified by a DTD and some extra documentation. Each incoming and outgoing message are checked by the reference PSP if they match the DTD. When the request ore response does not match with the DTD specification, an error is thrown.

3.8 Summary and Conclusions

In this chapter the need of a certification process, and what is included in a certification process, is explained. A life certification process is performed to gain more experience with the certification process. A description is given of the individual components in the chain, and how these components are integrated. At the end a critical evaluation is given of the quality of the certification test suites, and the certification process itself. Also the individual components are evaluated, as the protocols between the components.

From the performed research and life certification came out that the EMV certification process has a very poor quality. The test suites of Visa and MasterCard have an individual branch coverage of respectively 67% and 66%. Together they have a branch coverage of 73%. The most important component of the chain, the PSP, has a very poor unit test coverage, namely less then 25%. This 25% is much less then the 73% branch coverage of the two test suites together. Even though the literature says the 25% is not acceptable, in practise the PSP processes millions of transactions each month. Because the other components are out of scope, no conclusions or statements can be made for these components.

In the next chapter a proposal is done to change the EMV certification process to optimise it in time, but also to increase the quality.

Chapter 4

Proposed Improvements to the EMV Certification Process

In the last chapter we have proven that the EMV certification process has a poor quality. In this chapter some proposals will be presented to improve the EMV certification process. Not only to increase the quality of the certification process, but also to decrease the amount of time and effort.

4.1 Certification Authority

Because there were a lot of issues found during the life certification, 7 pre-certifications were performed before the onsite testing. Two new issues were spotted during the onsite testing. This causes that an extra pre-certification iteration was needed after the onsite testing. During each iteration of the pre-certifications new issues where found that had no relation with the issues that where solved in the previous pre-certification. This implies that the Certification Authority only checks the results of the tests roughly, because else all issues should be found during the first pre-certification. The Certification Authority admitted that the sniffer log files are not checked during the pre-certification. Only when the test does not have the expected result, the Certification Authority will investigate the transaction in more depth. For this investigation they sometimes use the sniffer log, but not always. The main reason why they do not check these on before hand, is because this will take too much time.

It would be better for the Certification Authority to pay more attention to specific tests that test do not have a standard result. An example a MasterCard test cases where MasterCard tests if the Track 2 data is used for the transaction came from the magnetic stripe and not from the ICC. Therefore this test needs some special attention that this is also really checked by the Certification Authority.

4.2 Sniffer Logs

The Certification Authority informed that during the pre-certification the sniffer log files are not checked. Only when the test does not have the expected result, the Certification Author-

Test suite	# offline declined tests	percentage of total
Visa	4	8.5%
MasterCard	7	22.5%

Table 4.1: Number of offline declined tests

ity will investigate the transaction in more depth. For this investigation they sometimes use the sniffer log, but not always. Because collecting these sniffer logs during the certification process takes time, it will save time when this is not needed. Therefore it would be better to collect these logs only for the tests that the Certification Authority indicates after they have checked the results.

4.3 Redundancy in Test Suites

There is a lot of redundancy between the test suites of the different brands. This means that the same functionality is tested multiple times, only for an other brand. The Certification Authority specifies the tests of different test suites that need to be performed. The Certification Authority should allow parties that want to certify, to perform all the redundant test scripts between the different test suites only for one brand. For this, a new generic test suite should be introduced. This suite must contain all the main tests that are the same for each brand, which tests the main functionality. For brands that have functionality that is specific for that brand, an additional test suite must be included. After this improvement, the EMV certification process will only contain the generic test suite, and all the small test suites of the brands that need to be supported (if these brands need such an extra test suite). This will decrease the amount of work, and time.

4.4 The Quality of the Visa and MasterCard Test Suites

The test suites of the 2 main credit card companies do not have a 100% branch coverage of the specification. To improve this, the test suites need to be changed/ expanded with new tests. These test must be configured in such a way that they cover all the uncovered branches. Adding new tests will increase the quality of the test suites, and therefore the certification process, but will also increase the time that the certification process will take.

Both test suites also have some tests that are offline declined (see Figure 2.6 for the control flow). These tests could be skipped, because this functionality does not need any communication with the PSP (and the acquirer, and the issuer). This functionality should already be tested with the Level 2 certification of a terminal. Therefore these tests should be left out of the test suites. The number of offline declined tests, and the percentage of the amount of tests for each test suite is shown in Table 4.1.

4.5 Improve Reference PSP

The reference PSP has a very low JUnit test coverage (estimated less then 25%). According to the literature, this should be increased to met an acceptable coverage of 75% - 85%. To achieve this increment more JUnit tests need to be developed. For a more precise mechanism to calculate the coverage a coverage measure tool like Clover [8] should be considered to be introduced.

During the certification process the transaction is sent through the PSP to the acquirer. A disadvantage of this is that the acquirer will not directly check if the given data in the request is correct for a certain test transaction. For example: there is a MasterCard test in place where the Track 2 data must be extracted from the magnetic stripe (ICC Fallback), and not from the ICC. This is not checked by the acquirer when the transaction is transmitted.

A solution would be to extend the current simulator PSP in an other way then described in Section 3.6. Not by sending the transaction directly to the acquirer, but first to check it on the PSP's site. The PSP could check if the request contains specific data. If not, a proper error response can be sent back which indicates what is wrong. This will increase the error handling during testing, and will save time during issue solving/ finding.

4.6 Chain of Components

It would reduce the certification time if different certified components (of the same type) can be connected to build a certified chain. When the new environment of a reused component differs from the environment where it was designed for, the argument that the quality of an assembly of components is at least as good as the quality of the individual components does not hold [16].

To achieve the reduction in time and effort, other actions have to be taken. When a component of the chain is reused it must have the same functionality and must be used in the same environment as for which it had been designed for. When the terminal component in the chain is replaced by an other terminal this terminal must use the same interface as the previous terminal. Both of them must be able to communicate with the reference PSP in XML specified by the DTD.

For testing an EMV chain of components and be able to draw conclusions about the different requests/ responses between the components we introduce a new architectural pattern: "Bi-Directional Pipes & Filters". This new architectural pattern is an extension of the existing pattern "Pipes & Filters" [7]. See Figure 4.1 for an overview how the new pattern looks like.

During the performed life certification that was described in Section 3.4, components were adapted so that the Bi-Directional Pipes & Filters pattern could be used to retrieve all the requests and responses between the component in the chain that are in scope. It is only possible to retrieve these data from the terminal, POS application, and the PSP [15]. This results in the following communication lines/ protocols between the components that can be taken into account:

1. card and terminal

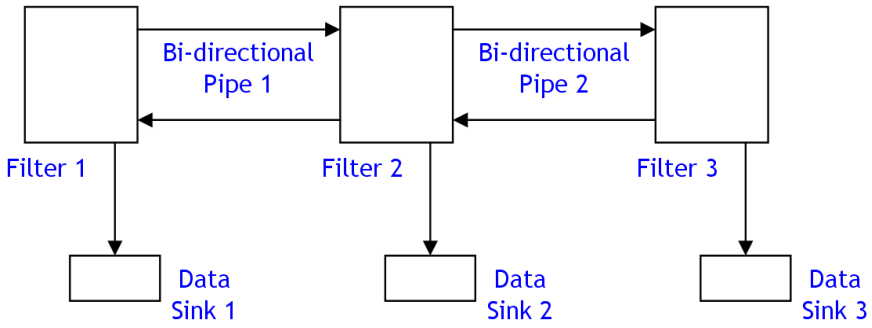


Figure 4.1: Bi-Directional Pipes & Filters pattern

2. terminal and POS application
3. POS application and PSP
4. PSP and acquirer

For the first life certification process all these data is already collected. Examples of a request and a response of each protocol is described in more detail in Appendix G. For a second life certification process the retrieved data can be used to compare it to the retrieved data of the second life certification. By comparing this data, issues can easily be found and located. This will save time, and will therefore decrease the elapsed time of the certification process.

4.7 Summary and Conclusions

With the described research of the previous chapter some improvements of the EMV certification process are proposed in this chapter:

- Better checking by the Certification Authority during the pre-certification
- Do not collect all the sniffer logs during the pre-certification
- Introduce a generic test suite, and small specific test suites for each brand
- Extend the current EMV test suites
- Remove the tests which test functionality that is already tested with the Level 2 certification of a terminal
- Improve the reference PSP unit testing coverage, and introduce a coverage measure tool
- Improve the response that the reference PSP sends back

- Collect data during the certification process by using the Bi-Directional Pipes & Filters pattern

By changing the use of the sniffer logs the elapsed time of the EMV certification process can be decreased. When the Certification Authority will improve their way of working, issues will faster be found, and more than 2 pre-certification will not be needed. The quality of the EMV certification process if very poor. By removing redundant tests, and by introducing a new generic test suite with new tests that cover the missing branches, the quality of the EMV certification process can be improved. Also the reference PSP component can be improved by better unit testing, and by increasing the error handling of wrong (or faulty) EMV test transactions. By collecting data of the certification process using the introduced Bi-Directional Pipes & Filters pattern, data can easily be compared with different tests, and certification processes. In the next chapter the proposed improvements will be evaluated.

Chapter 5

Evaluation of the Proposed Improvements to the EMV Certification Process

In the previous chapter some improvements are proposed of the EMV certification process. In this chapter these proposes are evaluated to see what the effect of the improvement is of the EMV certification process. Also the effects of the improved EMV certification process for the PSP and the Certification Authority are discussed. With the evaluation of the proposed improvements, the research questions stated in the introduction of the Thesis are attempt to be answered.

5.1 Certification Authority

To move the Certification Authority to change their way of working, and to improve their testing, a meeting must be planned to discuss these issues with them. This is not done yet, and will be part of the future work.

If the Certification Authority is willing to change their way of working by improving the way they check the results of the pre-certification, the time for the EMV certification process will decrease. When the Certification Authority checks the results of the pre-certification not roughly like they do now, but more strict, almost all issues will be found during the first pre-certification. Therefore not more than 2 pre-certifications are needed, when all issues are solved after the first pre-certification. This will be much better than during the performed life certification. During the life certification 7 pre-certification round were needed before the onsite testing could take place. And after the onsite testing even still issues were found.

This decrease of the amount of pre-certifications will decrease the elapsed time of the whole EMV certification process, because one of the steps of the whole process takes less time. This contributes to the fifth research question: with this improvement, the improved EMV certification process will take less then the 3 to 6 months that it takes with the current EMV certification process.

The decrease of time will effect in a decrease of costs. Not only employee costs for the PSP, but also employee costs for the Certification Authority. An other effect is that the

whole certification process takes less time, and that the PSP can put the chain of components sooner to the marked, and will also generate incomes sooner.

5.2 Sniffer Logs

To collect the sniffer logs some additional actions must be performed. When these actions are not part of the pre-certification anymore, this will save time. Especially when the amount of tests of the pre-certification is more then 100.

From practical experience, it will decrease the elapsed time of the pre-certification with around 10% when most of the sniffer logs are not collected. Some transactions need the sniffer log to be able to check the test script, but most of them do not. When a test does not have the required result, the Certification Authority can request the sniffer log from the PSP to be able to perform a better analysis on why and where the transaction went wrong.

When there is an agreement with the Certification Authority that the sniffer logs are not needed on before hand, the time to perform the pre-certification will decrease with 10%. The decrease of time will lead to a decrease in time of the whole certification process. Therefore this improvement also contributes to the answer of the fifth research question, like the previous proposed improvement.

5.3 Redundancy in Test Suites

The Visa test suite contains 51 tests that are applicable, and the MasterCard test suite contains 31 tests. This are 82 tests together. When the Visa and the MasterCard test suites are compared, 41 tests of the Visa test suite are redundant. This means when only Visa and MasterCard must be certified, the 41 Visa tests, test functionality that is already tested by the MasterCard tests. When a generic test suite is used, these 41 tests can be left out. This will decrease the amount of tests that must be performed from 82 test, to 41 tests. This is a decrease of 50%. This also means that the time that it will take to perform a pre-certification, or onsite testing, almost decreases with 50%.

By improving the test suites a reduction of time of almost 50% can be achieved for the pre-certification, and the on-site testing. This means that with the proposed new generic test suite a PSP can do a pre-certification in 50% of the time comparing to the currently used test suites. The decrease of time will have the same effect as described in the previous first proposal.

The introduction of a new generic test suite can only be achieved in practise when the Certification Authority creates such a test suite, because they decide which tests are applicable. The Certification Authority must also agree that the new generic test suite is sufficient to grant the certificate.

5.4 The Quality of The Visa and MasterCard Test Suites

The current EMV test suites are of very poor quality, because there is only a branch coverage of 73%. To improve the test suites, so that we can conclude that the test suites have a 100%

branch coverage of the whole EMV specification, the credit card companies need to expand/ change their test suites with new tests that cover all the missing branches. When 22 test are added, and some of the existing tests are changed, a 100% branch coverage can be achieved.

There are also branches that result in a offline decline of the transaction. The branches to decline a transaction offline should already be tested, before a terminal receives a Level 2 certificated. These branches should therefore be removed from the branch calculation. This will reduce the amount of extra tests from 22 to 16.

As described in the precious section, 41 tests of the Visa test suite test the same functionality as the MasterCard test suite. With a generic test suite the result is a test suite that contains 41 tests. When this test suite must have a 100% branch coverage 16 tests must be added. This will come to a total of 57 tests, which is still a reduction of 30% of the tests that must be performed.

The 16 new tests must be made by the credit card companies, or the Certification Authority, because the cards for the new tests need to be configured with private keys that are only known at their side. This could be a problem, because the credit card companies, or the Certification Authority, must take actions to improve the quality of the EMV certification process.

5.5 Improve Reference PSP

The proposed improvements for the reference PSP to meet the literature unit test coverage standards are not implemented. The implementation of the extra JUnit tests will take a long time. A lot of functionality is implemented by people who are not longer working for the reference PSP. Therefore the code must be investigated how it should work, and how proper JUnit tests can be implemented.

The improvements of the test environment of the reference PSP will have some advantages, but also some disadvantages. When the PSP receives a request it will probably not be possible to send a response back directly to the terminal, because the response also needs a certificate. This certificate must be create by the issuer for a correct transaction result in the Second Generate AC command between the terminal and the card. Therefore the transaction must always be sent to the acquirer who will send the request to the issuer.

Because the test suites of the different brands change over time, the extension of the reference PSP must also be changed. Also different test suite versions can be used. This must also be supported. This means that when every time a new test suite is out, the system of the PSP must be updated to be up to date for the next new life certification process.

5.6 Chain of Components

There is, unfortunately, no second terminal (or acquirer) to compare all the retrieved data. Because the protocol between the POS application and the terminal is not a standard, this data is hard to compare. On the other hand, the messages between the POS application and the PSP, and the messages between the PSP and the acquirer could be easily compared to each other.

5.7 Summary and Conclusions

We have proved in this Thesis that the current EMV certification process has only a branch coverage of 73%. With this knowledge we can answers the first research question: ”what’s the quality of the current EMV certification process?”. The quality is very poor.

There are different tools available to specify and test individual components. The reference PSP uses text documentation, and JUnit and regression tests to test its system. The specification (for what is available) is done with text documents, and comments in the code. The second research question is: ”How can we specify and test individual components to verify that they satisfy the requirements/ specifications?”. A solution for this are the tools that are used by the reference PSP. With a coverage measure tool the coverage can be measured.

When a second terminal (with POS application) uses the same protocol as the first one (the DTD of the reference PSP), the terminal component can easily be replaced. But even when the new component is tested very strict, we can state that the terminal can safely be replaced, according to the literature [16]. This answers the third research question: ”How can we specify and test the protocols used between the individual components in the chain (request-response) in such a way that we could safely replace individual components in the chain?”.

The argument that the quality of an assembly of components is a least as good as the quality of the individual components does not hold [16]. Therefore that answer to the fourth research question: ”Can we make the statement that the whole chain is certified when all the individual components in the chain are certified?” is ’no’. Even when all the individual components are certified, it does not have to hold the the whole chain of certified components is certified.

Most of the proposed improvements of the current EMV certification process will decrease the amount of time that the certification will take. The fifth research question: ”can the current certification process be optimized so it will take less time than 3 to 6 months?” can be answered with ’yes’. When all the proposed improvements are applied on the current EMV certification process, the elapsed time will probably decrease to 3 months max.

All the answers to the sub research questions lead to the answer of the main research question: ”If each of the components is certified and if all the protocols are certified between these components, would this not be sufficient to conclude that individually certified components could be exchanged, without the requirement to certify the whole chain again?”. It is not possible to draw conclusions about the quality of the chain of components, even when you know that all the individual components and protocols are certified. Therefore the answer to the main research question is, unfortunately, ’no’. In the future it will still be needed to certify the whole chain of components, when one of the components in the chain is changed.

Chapter 6

Summary, Conclusions, Future Work

6.1 Summary

To reduce credit card fraud, a new worldwide standard has been introduced called EMV, which stands for Europay, MasterCard, and Visa (three of the main credit card companies in the world). An EMV credit card does not contain a magnetic strip, but a chip that is protected by cryptographic algorithms to authenticate the card, and a PIN to authenticate the cardholder.

This new EMV standard also introduces a new certification process that is needed for PSPs to be allowed to process credit card transactions. With this new EMV certification process not only every component of the transaction chain must be certified, but also the whole chain of components. This implies that when one component in the chain is changed, the whole chain of components must be re-certified. For a PSP who wants to support multiple merchants, in multiple countries, with multiple currencies and multiple terminals, the certification process must be repeated an endless number of times, which is a very time consuming operation. This leads us to the key question of this Thesis, which is: ”If each of the components is certified and if all the protocols are certified between these components, would this not be sufficient to conclude that individually certified components could be exchanged, without the requirement to certify the whole chain again?”.

To be able to answer this key question, research is performed regarding the current EMV certification process. As part of this research, a life EMV certification process is performed at the reference PSP, and with success. At the end all issues were resolved, and the certificate was granted by the Certification Authority. As a cherry on the pudding, a life EMV transaction was performed to proof that the certified chain of components works in real life. During the research some issues were encountered:

- The Certification Authority does not check the results of the pre-certification very carefully, only roughly. This can result in multiple pre-certification rounds which increase the time of the whole certification process.
- The different test suites that are used for the different credit card brands during the EMV certification process have a lot of redundancy. This results in testing the same functionality multiple times without any need.

- The test suites of Visa and MasterCard have an individual branch coverage of respectively 67% and 66%. Together they have a branch coverage of 73%. According to the literature a branch coverage of 100% is only acceptable. This indicates that the test suites have a very poor quality.
- The test suites of Visa and MasterCard contain tests that should already be tested during the Level 2 certification of the terminal component. During the EMV certification process these tests are performed without any need, and only take extra time.
- The reference PSP has a very poor unit test coverage of less then 25%. In practise this low coverage does not mean that the reference PSP has a very poor quality of service. The reference PSP (as other PSP's) is successfully processing millions of transactions and is transferring millions in monetary funds every day, while fraud is kept below accepted limits.

By evaluating the research outcomes and issues, the following recommendations are proposed:

- Do not collect all the sniffer logs during the pre-certification
- Introduce a generic test suite, and additional specific test suites for each brand to cover the particular brand specifics
- Extend the current EMV test suites to increase coverage
- Remove the tests which test functionality that is already tested with the Level 2 certification of a terminal component
- Improve checking by the Certification Authority during the pre-certification
- Improve the reference PSP unit testing coverage, and introduce a coverage measure tool, like Clover
- Improve the response that the reference PSP sends back
- Collect data during the certification process by using the Bi-Directional Pipes & Filters pattern

Executing these recommendations will have the following effects. When the sniffer logs are not collected during pre-certification, the elapsed time will decrease with 10%. When a new generic test suite is used, it will result in a decrease of 50% in the amount of tests that need to be performed. When also the tests that test the functionality that is already tested during the Level 2 certification of a terminal are removed, and when some tests are added to cover the missing branches, the amount of tests that need to be performed will decrease with 30%. The new test suite will lead to a decrease in time of around 30%, and will have a branch coverage of 100%: it is faster, and it has a higher quality.

Unfortunately, the answer to the mean research question: "If each of the components is certified and if all the protocols are certified between these components, would this not be

sufficient to conclude that individually certified components could be exchanged, without the requirement to certify the whole chain again?" is 'no'. But the current EMV certification process can be optimized with the proposed improvements to decrease the time that it takes to perform a certification. What the exact total decrease of time of the EMV certification process will be after all improvements is not clear. This could be evaluated by performing a life certification with all the proposed improvements. This will need the help of the Certification Authority.

Because of the time restriction there was no time left to improve the unit test coverage of the reference PSP, or to improve the response of the reference PSP. Also all the improvements of the EMV certification process that needs assistance from the Certification Authority are not done. There was also no time to check the collected data with the proposed pattern with a second terminal. All these improvements are actions for the future work.

6.2 Conclusions

Before this Thesis no research was apparently done of the EMV certification process. This Thesis gives a clear introduction to the EMV standard, the different EMV transactions, and the EMV certification process.

The test suites that are used for the EMV certification process are very poor. For Visa and MasterCard together, there is only a branch coverage of 73%. With the results of the performed research, and the proposed improvements, the EMV certification can be improved in quality, which will overcome issues in the future. Issues that were not found before, because it was not tested. The proposed improvements will also decrease the amount of time that the EMV certification process will take. Therefore the proposed EMV certification process is a very good improvement, especially for PSPs, because different chain of components (with for example an other terminal) can faster be certified. When a chain is certified in less time, the time to marked with this specific chain of components is also faster, which will reduce costs and increase the income of the PSPs.

Unfortunately, the answer to the mean research question is 'no', at least when also from a business perspective full coverage is required. So, re-certification will be needed when one of the components in the chain is changed. But the EMV certification process itself can be improved: better quality, and decrease in time of the whole process.

With the proposed improvements in the test suites, the branch coverage of the EMV certification process can be increased to 100%. This 100% branch coverage can be achieved with 25 less tests then the Visa and MasterCard test suites have together. Instead of 82 tests, only 57 test should be performed, which is a decrease of more than 30%.

The decrease of the amount of tests will lead to a decrease of elapsed time of the EMV certification process. For some of the proposed changes cooperation of the Certification Authority and credit card companies is needed. To achieve this will be very hard, because big companies like these would probably not change their way of working easily.

The Certification Authority states that certification process is a very time consuming task, and will take 3 to 6 months. In my case, the performed live certification took almost

9 months. In this 9 months I have also done other work in between, like the performed literature study, and research of the test suites of Visa and MasterCard.

The elapsed time of the certification process also depends on the system which needs to be adapted to be able to handle EMV transactions. The reference PSP system that was changed, processes up to 13 transactions per second. For this reason, changes should be made with caution.

Also the complexity of the PSP system can vary of course. The consequence of this is that the implementation time, problem analysing, bug fixing, etc. will take different amounts of time. Therefore the certification process could have taken less time then 9 months if an other PSP was used.

6.3 Future Work

In this section the future work will be discussed that can be performed with the gained knowledge of this Master Thesis. All the future work could not be performed during the Thesis' research because of the time, or because it was out of scope.

6.3.1 Second Terminal

With the gained experience in hand, the certification process of a second terminal will probably be much shorter then the first certification. Therefore the terminal component of the chain could be exchanged. The whole PSP application is already EMV compatible. By performing a second certification with an other terminal more information can be given about how much time the second certification will differ from the first.

6.3.2 Second Acquirer

Not only the terminal component can be changed. The PSP can also use an other acquirer for the transactions. It would be good (from PSP point of view) to have a second acquirer to be able to handle the transaction, as backup. When the primary acquirer is not reachable, the PSP can fallback to an other acquirer. This fallback functionality is already available in the PSP, but a certificate is needed for the second acquirer to be able to process EMV transactions.

A good choice for a second acquirer would be an acquirer that also uses the APACS30 standard as protocol. This will make the integration much easier, because less implementation work has to be done.

6.3.3 Certification Quality

The test scripts that are used for the EMV certification process are not testing all the branches. Are the credit card companies aware of this? If so, what is the philosophy behind this? For example: why does Visa not test the Issuer-to-card script processing functionality? Is Visa not using this, and planning not to use this in the future? These questions could be verified with the credit card companies. With this information paths that are not tested

could probably be discarded from the flows, because they will never be used. In this case the proposed improvement of a generic test suite would take even less time. This will lead to an even faster improved certification process then proposed in this Thesis.

6.3.4 Certification Authority

During a discussion with the Certification Authority the described proposed improvement for the Certification Authority, that came up during the research, can be discussed. As outcome of this conversation the Certification Authority can decide to change the way how they check the results of the pre-certification. This will have the effect that issues will be found much sooner, and that more than two pre-certification are not needed.

Chapter 7

Reflection

Having dealt with the (narrow) scientific approach of this problem, I would like to reflect, contemplate and relativise a bit in a (broader) sense and try to place the scientific conclusions within the business perspective of the financial industry. The major research question was whether there really is a need for such a cumbersome testing process that needs to be repeated all over again, causing so much pain for the business.

It is clear that the scientific answer to that question is that in order to test a chain of components, one has to test the whole chain, when one of the components change. From a business perspective however, one can ask the question whether or not a 100% prove of correctness is required. In other words what are actually the requirements for the quality and coverage of the tests that need to be met in order for the business to accept a chain of applications in a particular business process.

The financial industry is an industry in which an error in the most basic sense translates directly into a loss of money, since the main object of the business is to deal with amounts of money. The common practice in the financial industry regarding credit card payments is, and has always been, that a certain amount of fraud is accepted and the costs of writing these damages off is incorporated in the transaction rates. So, the business does not strive towards banning fraud for 100%, but towards keeping it to an acceptable level. So, translating this common practice to the certification process would lead to the conclusion that a 100% coverage would not be required, but only a certain coverage by which the losses caused by errors would stay within acceptable limits.

Another interesting aspect from a business perspective is also that the checks that are performed on EMV cards, and subject to the certification, are not the only checks that are executed to verify that the intended transaction is not fraudulent. The reference PSP uses a very sophisticated Risk Management Module to carry out numerous checks before a transaction is authorised, so the EMV checking, though important, is 'only' one of the checks carried out, and this 'chain of components' is just a component in another 'chain of components'.

If we take a step back then and look at our findings from the business perspective, then first of all, we concluded that the coverage of tests in the current production environment is less then 25%. This coverage is acceptable to set a chain of applications live that processes almost a million transactions every month, and transfers hundreds of millions in monetary

funds each day. This leads to a percentage of fraudulent transactions and associated losses that are well below the generally accepted levels. The reference PSP sees this as an excellent result compared to the competition.

We also concluded that in a theoretical and scientific sense, the EMV certification has a very poor coverage (73%), but the interesting thing now is that from a business perspective, the coverage is extremely good, say almost three times as good as what is accepted today.

The interesting conclusion therefore is that from a scientific perspective , the certification is poor, but from a business perspective it is extremely good.

This reminds me to a theme of two famous Dutch philosophers from the last century, Koos Koets and Robbie Kerkhof, that in their native language wrote:

> 'pak het op, keer het om en zet het neer,
>
> dan kijk je er heel anders tegen aan'

In translation:

> 'pick it up, turn it around and place it down,
>
> then suddenly you get a different view'

Figure 7.1: Koos Koets and Robbie Kerkhof

I would now like to look back on my works of the last few years in the payment industry, in particular the processing of credit card payments, starting with a Bachelors Thesis and now followed by my Masters Thesis.

During the preparation of my Bachelors Thesis and Master Thesis, I learned a lot about the EMV standard, and by going through the live certification process I was forced to even study the most intimate details of the EMV protocols.

When I started the work, I asked myself: ”how difficult can it be to make a credit card payment, where you only have to provide a credit card number, an expiry date and an amount”, but I know now how wrong I was. Hence the theme of my Thesis: ”Oh, what a tangled web we weave”.

I had my initial fears, when the reference PSP, without hesitation, set me free to change their live payment system. It started an adventurous quest that granted me my first job in the international payment system arena. The journey was great fun, and the reward an interesting position.

So, here are my final words in this Thesis. From a scientific viewpoint, in a chain of components, the whole chain needs to be tested when components change and the certification coverage of 73% is very poor. From a business perspective, I believe that a once certified component, does not have to be certified again as part of the chain, when one of the other components is changed and a coverage of 73% is really excellent.

Bibliography

[1] ABN AMRO Bank N.V. Welcome to ABN AMRO. http://www.abnamro.com/.

[2] Reference Acquirer. Certification Process - Technical Schedule. Technical report, Reference Acquirer, October 2006.

[3] Reference Acquirer. Chip & PIN Solution Questionnaire. Technical report, Reference Acquirer, October 2006.

[4] APACS. Common attachment to standards 29, 30, 40 & 50, version 18. Technical report, Association for Payment Clearing Services, February 2003.

[5] APACS. Standard 30, Specification for an authorisation terminal, version 18. Technical report, Association for Payment Clearing Services, February 2003.

[6] Boris Beizer. *Software Testing Techniques*. International Thomson Computer Press, second edition, 1990.

[7] Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad, and Michael Stal. *Pattern-Oriented Software Architecture Volume 1, A system of patterns*. John Wiley & Sons Ltd., 1996.

[8] Cenqua. Cenqua: Clover. http://www.cenqua.com/clover/.

[9] Gerardo de Geest, Etienne Gerts, Thomas Kraus, and Maikel Lobbezoo. Emv project - bachelor thesis, 2005.

[10] EMVCo. EMVCo - manage, maintain and enhance the EMV Integrated Circuit Card Specifications for Payment Systems. http://www.emvco.com/.

[11] EmvCo. EMV2000 Integrated Circuit Card Specification for Payment Systems – Application Independent ICC to Terminal Interface Requirements, V4.1. Technical report, EmvCo, 2004.

[12] EmvCo. EMV2000 Integrated Circuit Card Specification for Payment Systems – Application Specification, V4.1. Technical report, EmvCo, 2004.

[13] EmvCo. EMV2000 Integrated Circuit Card Specification for Payment Systems – Cardholder, Attendant, and Acquirer Interface Requirements, V4.1. Technical report, EmvCo, 2004.

[14] EmvCo. EMV2000 Integrated Circuit Card Specification for Payment Systems – Security and Key Management, V4.1. Technical report, EmvCo, 2004.

[15] Etienne Gerts. EMV Credit Card Certification, December 2006.

[16] Hans-Gerhard Gross. *Component-based Software Testing With UML*. Springer–Verlag, 2004.

[17] Trintech Group. Unattended Payments Resources - openpaynews.com - your unattended and outdoor payments news and resource site. `http://www.openpaynews.com/payments/faqs_security_certification.html`.

[18] ING Groep N.V. ING Groep N.V. `http://www.ing.com/`.

[19] Visa International. Visa Integrated Circuit Card Application Overview, V1.4.0. Technical report, Visa International, 2001.

[20] International Herald Tribune. Credit card fraud keeps growing on the Net - International Herald Tribune. `http://www.iht.com/articles/2007/05/11/news/mcredit.php`.

[21] MasterCard. Terminal Integration Process (TIP) Guide. Technical report, MasterCard International Incorporated, 2006.

[22] MasterCard. User Guide for ETEC Subset 1 - Jan2006A. Technical report, MasterCard International Incorporated, May 2006.

[23] Object Mentor, Incorporated. JUnit, Testing Resources for Extreme Programming. `http://www.junit.org/`.

[24] PCI Compliance Guide.org. PCI Compliance Guide - FAQs and Tips on PCI Compliance. `http://www.pcicomplianceguide.org/`.

[25] Reference PSP. Submitting EMV Transactions. Technical report, Reference PSP, June 2007.

[26] Reference Acquirer. ICC test scripts, Version 11.0.2. Technical report, Reference Acquirer, August 2006.

[27] Triple Deal. Triple Deal – Multi-Channel Payment Solutions. `http://www.tripledeal.com/`.

[28] Visa International. Visa - Credit Cards and Other Payment Solutions. http://www.visa.com.

[29] Visa International. Visa Integrated Circuit Card Card Overview, V1.4.0. Technical report, Visa International, 2001.

[30] Visa International. Visa Integrated Circuit Card Terminal Overview, V1.4.0. Technical report, Visa International, 2001.

[31] Visa International. Chip Card Acceptance Device Reference Guide. Technical report, Visa International, January 2005.

[32] Visa International. Smart Debit / Credit Acquirer Device Validation Tool Kit, Version 3.2.3. Technical report, Visa International, March 2006.

[33] Wikipedia. Chip and PIN - Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Chip_and_PIN.

[34] Wikipedia. Wikipedia – Online Encyclopedia about DTD. http://en.wikipedia.org/wiki/Document_Type_Definition.

Glossary

Acquirer
: The Acquirer is the (Merchant's) bank that will collect the money for the Merchant. The Acquirer will remit the money to the bank account of the Merchant and inform him by a periodic bank statement.

Application Identifier (AID)
: Each application on the ICC has an AID which indicates the brand of application. For example MasterCard, or Visa.

Credit Card Company
: The Credit Card Company is the credit card company that takes care of the processing between Issuers and Acquirers.

Cardholder Authentication Method (CAM)
: Validation of the card by the issuer to protect against data manipulation and skimming. The CVM indicates which method should be used for cardholder authentication.

Cardholder Verification Method (CVM)
: A method used to confirm the identity of a cardholder.

Ceiling limit
: The ceiling limit indicates the maximum transaction amount. All transactions that have a transaction amount above this limit will be declined.

Data Object List (DOL)
: A DOL is a list of tags and lengths of data elements.

Dynamic Data Authentication (DDA)

A type of Offline Data Authentication where the card generates a cryptographic value using transaction-specific data elements for validation by the terminal to protect against skimming.

Europay, MasterCard and Visa (EMV)
: Europay, MasterCard and Visa introduced a new worldwide standard (EMV) to reduce credit card fraud.

Floor limit
: The floor limit is a terminal setting. This setting indicates above which transaction amount the transaction must be authorised online.

Issuer
: The Issuer is the (Shopper's) bank that has issued a credit card to the Shopper who is using this credit card to pay for the transaction. The Issuer will bill the Shopper and inform him by a periodic bank statement.

Merchant
: The Merchant is the shop owner who is selling goods or services to the Shopper.

Offline Data Authentication
: A process whereby the card is validated at the point of transaction using RSA public key technology to protect against counterfeit or skimming. It includes two forms: Static Data Authentication (SDA) and Dynamic Data Authentication (DDA).

Payment Service Provider (PSP)
: The PSP is the Payment Service Provider that is providing the above services in one integrated package to the Merchant. A PSP is offering one single standardized interface to the "Merchant" for processing payments. By doing so the PSP is taking away the burden for the Merchant to interact with many different financial institutions. The PSP furthermore is offering additional services to the Merchant like currency conversions and reconciliation.

Processing Options Data Object List (PDOL)
: The PDOL is a DOL of of terminal data elements needed by the ICC in processing the Get Processing Options command.

Shopper
: The Shopper is the consumer who is buying goods or services from a Merchant.

Static Data Authentication (SDA)

A type of Offline Data Authentication where the terminal validates a cryptographic value placed on the card during personalization. This validation protect against some types of counterfeit, but does not protect against skimming.

Terminal Integration Process (TIP)
: The TIP describes different test that has to be performed during the certification process.

Appendix A

Sequence Diagram of the Payment Transaction Process

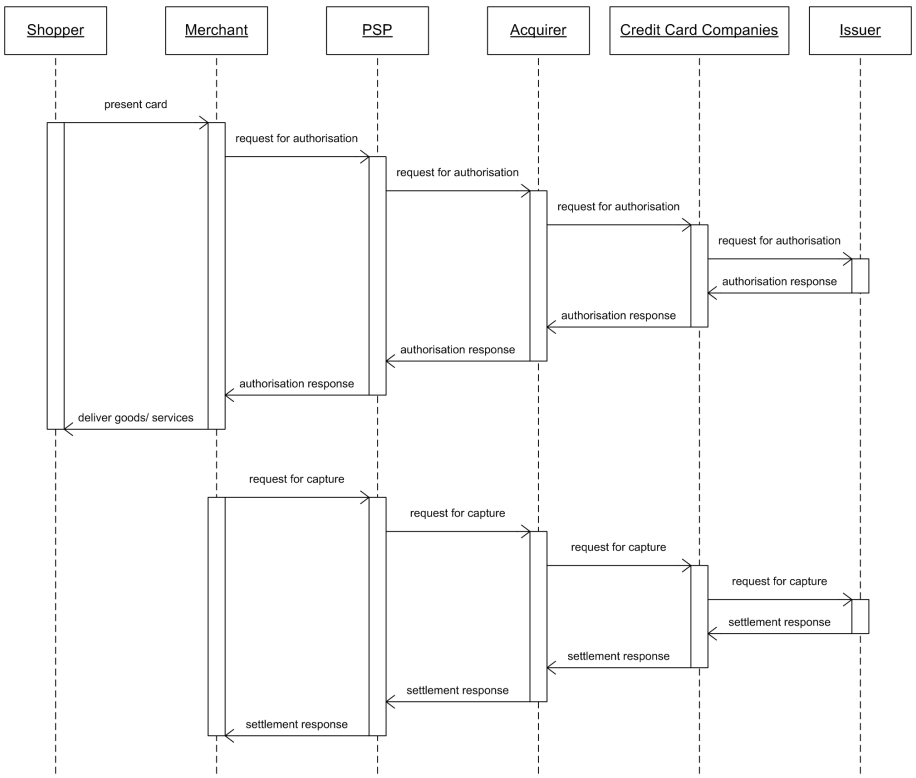


Figure A.1: Sequence Diagram of the Payment Transaction Process

Appendix B

Screenshots of the First Certified EMV Transactions

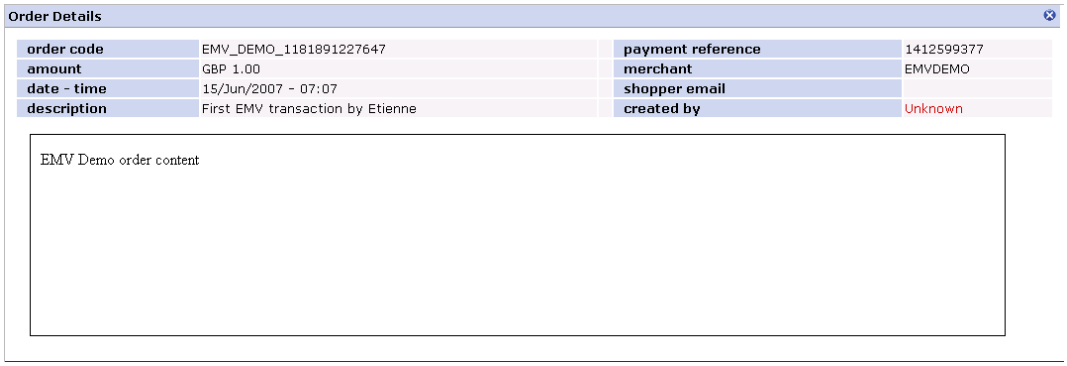
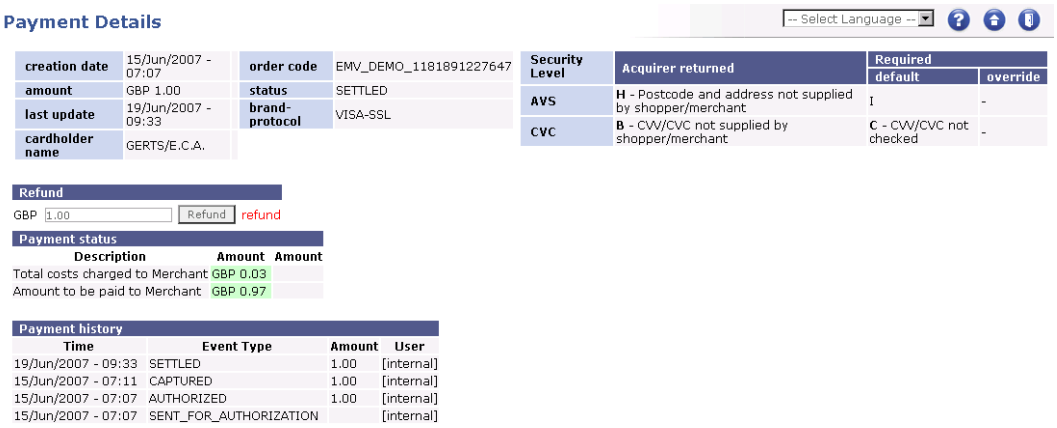


Figure B.1: Order Details of the First Certified EMV Transaction



Payment Details

-- Select Language --

creation date	15/Jun/2007 - 07:07	**order code**	EMV_DEMO_1181891227647
amount	GBP 1.00	**status**	SETTLED
last update	19/Jun/2007 - 09:33	**brand-protocol**	VISA-SSL
cardholder name	GERTS/E.C.A.		

Security Level	**Acquirer returned**	**Required**	
		default	**override**
AVS	**H** - Postcode and address not supplied by shopper/merchant	I	-
CVC	**B** - CVV/CVC not supplied by shopper/merchant	**C** - CVV/CVC not checked	-

Refund

GBP 1.00 Refund refund

Payment status

Description	Amount	Amount
Total costs charged to Merchant	GBP 0.03	
Amount to be paid to Merchant	GBP 0.97	

Payment history

Time	Event Type	Amount	User
19/Jun/2007 - 09:33	SETTLED	1.00	[internal]
15/Jun/2007 - 07:11	CAPTURED	1.00	[internal]
15/Jun/2007 - 07:07	AUTHORIZED	1.00	[internal]
15/Jun/2007 - 07:07	SENT_FOR_AUTHORIZATION		[internal]

Figure B.2: Payment Details of the First Certified EMV Transaction

Appendix C

Certification Test Suites

The certification process is mainly about performing different tests that must have a specific outcome. In this appendix the test suites of two credit card brands will be discussed: Visa and MasterCard.

C.1 Visa

The current EMV Visa test suite contains 51 tests. These tests must be performed with 47 different cards in 47 test cases. For the most of the tests there is a specific card. For some cards/ test cases there are two tests. The difference between the these two tests of a test case is always the amount of the transaction. All tests are applicable for attended, combined terminals like used the Trintech Smart 5000. In the next sections the 47 test cases of the Visa test suite will be discussed including the part of the EMV specification that is covered by each test case. All the information about the test cases is gained during the life certification and retrieved from the literature [32, 19, 29, 30].

C.1.1 Visa ADVT Test Case 1

Each terminal must be configured with a list of applications (indicated by the application identifiers called AIDs) that are supported by the terminal. For example the applications MasterCard and Visa. There are two ways for a terminal to match the terminal applications to the ICC applications. The result of both methods is a list of applications: candidate list. One of these applications can be used for the transaction.

The first method constructs such a list of applications by matching all the application identifiers in the list of the terminal to the application identifiers in the ICC. The main idea of the method is that the terminal tries to match all the application identifiers in his list to the applications of the card. This process is explained in more detail in Figure C.1.

The test card that is used for the first test is the basic Visa credit card. The test exists actually of tow tests: the first with an amount below the terminal floor limit and the second with an amount above the terminal floor limit. The floor limit of a terminal indicates above which transaction amount the terminal should force the transaction to go online. For certi-

fication purpose this value must be 5.00 GBP. The tests are successful if both transactions are authorised.

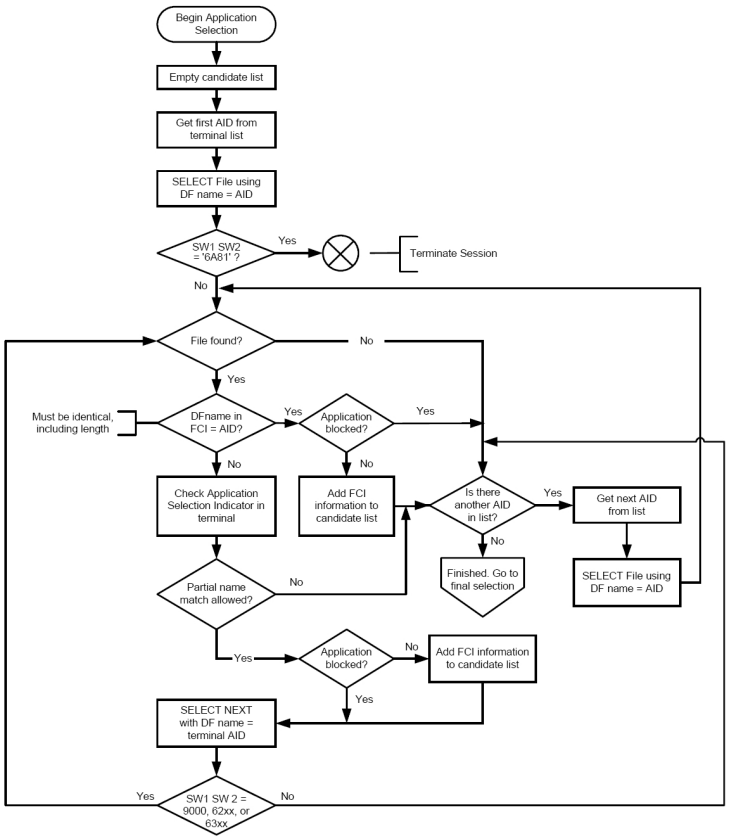


Figure C.1: Create application list using the list of AIDs in the terminal

C.1.2 Visa ADVT Test Case 2

Test 2 tests the second method of retrieving the application candidate list: retrieving the list by using the Payment Systems Environment (PSE). The PSE is a sort of directory structure for payment systems on an ICC. The main idea is that the terminal walks through the PSE (directory structure) and compares all the applications of the ICC to the applications in the list of the terminal. This process is explained in more detail in Figure C.2.

The test card is specially configured so it contains a PSE. The terminal must process the PSE and select the Visa application. The test is successful if the transaction is authorised.

C.1.3 Visa ADVT Test Case 3

Before an EMV transaction is started the communication between the card and the terminal must be suite up and configured. To process the commands initiated by the terminal for

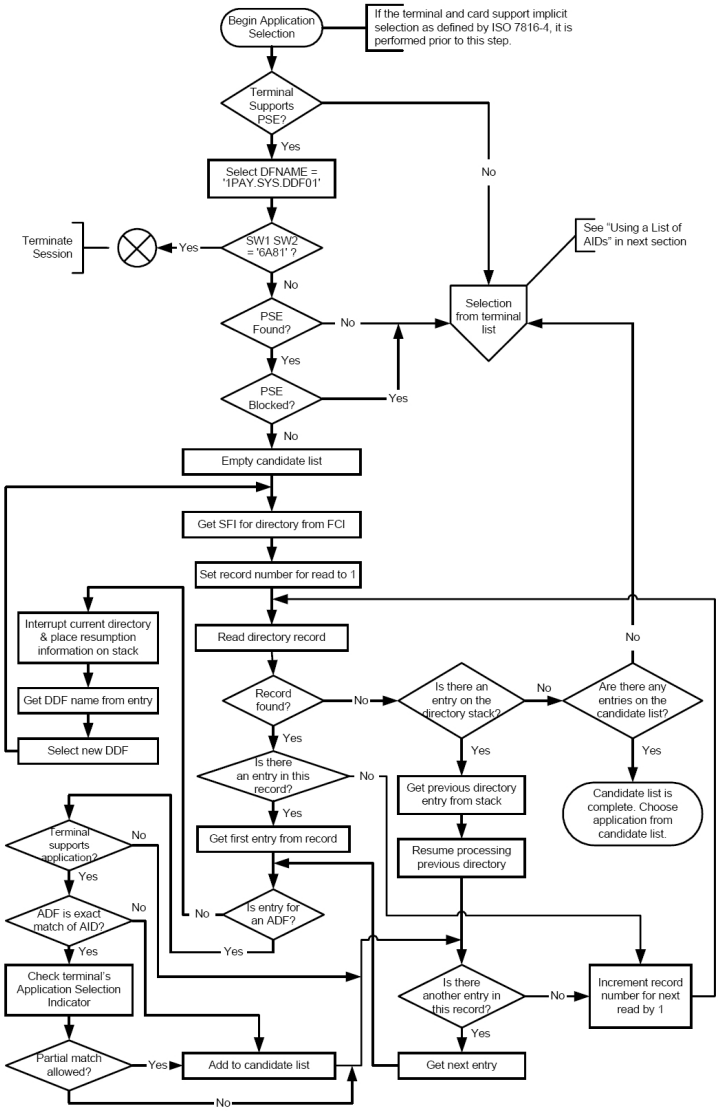


Figure C.2: Create application list using the Payment Systems Environment

transmission control and for specific control in asynchronous half duplex transmission protocols, two types of protocols are defined. The first protocol is the character protocol (T=0), and the second protocol is the block protocol (T=1). ICCs must support either protocol T=0 or protocol T=1. Terminals must support both protocol T=0 and T=1. The protocol to be used for subsequent communication between the ICC and terminal is indicated by the ICC in a specific field which is read during the initiation of the communication.

Most cards support protocol T=0, therefore this card is configured that is supports protocol T=1. The terminal must process the transaction normally, and the transaction must be authorised for a successful test result.

This test has nothing to do with the communication to the acquirer. The main purpose for this test is to check if the terminal can handle both protocols.

C.1.4 Visa ADVT Test Case 4

Test Case 4 tests Static Data Authentication (SDA) when this is supported by the terminal. This test is only in place for 'Informational Purpose Only', because the 896-bit CA Public Key that is used by this test has reached the end of it's life. Therefore the test is not mandatory anymore.

C.1.5 Visa ADVT Test Case 5

This test also tests the SDA functionality, but in a different way. All the CA Public Keys that are used should be configured in the terminal. This test uses a CA Public Key that is not configured in the terminal, which will result in a SDA failure. Each Issuer can indicates by configuring the issuer action codes which action should be taken when, for example, SDA fails. For Visa holds that, when SDA fails, a transaction should be send online. When the terminal is not capable of going online, the transactions should be declined. Else the transaction must be declined online.

C.1.6 Visa ADVT Test Case 6

The issuer may include the optional data element that indicates a preferred language. The card that belongs to this test case has this optional field set to Japanese, Korean, and Chinese. This means that when a terminal supports one (or more) of these languages, the terminal must show the messages on the terminal display in this language. When the terminal does not support these languages, it must display the messages in the standard language (for example English). The test is successful when it is approved. Because the Trintech terminal does not support one of the configured languages, it should process the transaction in English.

C.1.7 Visa ADVT Test Case 7

A terminal can support different parts of the ISO 8859 standard. The test card that belongs to this test has a Application Preferred Name in Cyrillic. This name can only be displayed correct if the terminal supports the ISO 8859, part 5 (which is not mandatory). When the terminal does not supports this part it must display the standard name. The transaction of the test must be approved for a successful result. The Trintech terminal does not supports part 5 of the ISO 8859, and must therefore display the standard name.

C.1.8 Visa ADVT Test Case 8

The application within both the terminal and the ICC should maintain an Application Version Number assigned by the payment system. The terminal uses these version numbers to ensure compatibility between the card and the terminal. If the Application Version Number

is not present in the ICC, the terminal shall presume the terminal and ICC application versions are compatible, and transaction processing shall continue. If the Application Version Number is present in the ICC, it is compared to the Application Version Number maintained in the terminal. If they are different, the terminal shall set the 'ICC and terminal have different application versions' bit in the TVR to 1.

The card that belongs to this test has a version number of 131. The terminal, and all the other Visa test cards, have a version number of 130. For a successful result the indicated bit must be set, and the transaction must be approved.

C.1.9 Visa ADVT Test Case 9

The application on the ICC has a specific expiration date that is configured by the issuer. The terminal must check if the current date is less than or equal to the Application Expiration Date. If it is not, the terminal must set the 'Expired application' bit in the TVR to 1.

This test has a test card that is configured with an Application Expiration Date that is set to September 2002. Therefore for a successful test result the 'Expired application' bit must be set, and the terminal must send the the transaction online for issuer's decision. The issuer's decision will be a decline. When the terminal can not go online it should decline the transaction offline.

C.1.10 Visa ADVT Test Case 10

Besides the Application Expiration Date, the application can also have a Application Effective Date. If this date is present in the ICC, the terminal must check that the current date is greater than or equal to the Application Effective Date. If it is not, the terminal must set the 'Application not yet effective' bit in the TVR to 1.

This test has a test card that is configured with an Application Effective Date that is set to January 2049. The ICC is also configured with specific action codes. These codes indicate that, when an application is not yet effective, it should be declined offline. This test is successful if the 'Application not yet effective' bit in the TVR is set to 1, and the transaction is declined offline.

C.1.11 Visa ADVT Test Case 11

As part of the application selection process an application can indicate that the shopper must confirm the use of the application (optional for application and terminal). When both the application and the terminal support this, the terminal must display a proper message for the shopper that must confirmed. If this message is not confirmed, or when the terminal does not support Cardholder Confirmation the transaction must be aborted. The test card for this test case has is configured with this Cardholder Confirmation. When the terminal supports this functionality (which the Trintech terminal does), the transaction must result in an approval. Else the transactions must be declined.

C.1.12 Visa ADVT Test Case 12

A card can be personalized by the issuer so that it can only be used for domestic transactions. The test card of this test has this Geographic Restrictions bit set to 1. Also the issuer country code of the application is set to a not existing country code value. With this configuration the card can only be used in this not existing country. Because this will never be the case, the application should not be selected. The test card has only this application and should therefore decline. If the terminal accepts the card and completes the transaction, it fails the test.

C.1.13 Visa ADVT Test Case 13

A card can contain proprietary data. This is data that can be configured by each issuer individual. A terminal must be able to handle cards that have these data set. Therefore the card that belongs to this test has this data configured. The data should be ignored by the terminal and process the transaction normally. The test is successful if the transaction is authorised.

C.1.14 Visa ADVT Test Case 14

In several steps during the transaction process, the terminal is asked to build a flexible list of data elements to be passed to the card. To minimise processing within the ICC, such a list is a single constructed field built by concatenating several data elements together. Since the elements of the constructed field are not know, it is imperative that the ICC knows the format of this field when the data is received. This is achieved by including a Data Object List (DOL) in the ICC, specifying the format of the data to be included in the constructed field. This methodology is also used for the Processing Options Data Object List (PDOL) which is optional. Because of the DOL structure, this test tests if the terminal can handle a card that contains a PDOL that contains a request of a long string of data. The terminal must respond to the request and handle the transaction properly. The transaction must be approved for a successful test result.

C.1.15 Visa ADVT Test Case 15

Each record in the ICC has a length field and a data field. Normally when the data value is less than 128 bytes in length, the length field is only 1 byte. When the data value is greater than 128 bytes in length, the length field is 2 bytes. Issuers, however, can use a length of 2 bytes even when the data value is less than 128 bytes in length. The card that belongs to test 15 has a data element where the length of the record is specified in 2 bytes. Because a terminal should be able to process such a card, the test is successful if the transaction is approved.

C.1.16 Visa ADVT Test Case 16

iCVV is an optional Visa EMV risk control feature that facilitates detection of skimmed chip data being used to counterfeit magnetic stripe cards. Issuers may elect to implement an

iCVV encoded in the track data stored on the chip, which is different from the CVV encoded on the magnetic stripe. As by definition the iCVV value on the chip will be different to the CVV value on the magnetic stripe, devices must not compare the two values during transaction processing. Whenever magnetic-stripe information is taken from the chip, the terminal must ensure the transaction is marked as a chip transaction. The terminal must also ensure that the only data elements used are from the chip and not from the magnetic stripe. When the magnetic stripe information is taken from the magnetic stripe, the device must ensure the transaction is marked as a magnetic stripe transaction, and it must not use any data elements from the chip, otherwise iCVV will fail. [31] Put another way, the use of an iCVV logically separates the card data stored on the smartcard from the data stored on the magnetic stripe, preventing the use of data 'cloned' from a smartcard to produce a fraudulent magnetic stripe. This extra information is only needed for Acquirer, therefore test 16 is specifically defined as an online test for Acquirers. For Visa Acquirers, the transaction should be sent online to the Visa Certification Management Service (VCMS) where the VCMS will perform iCVV. For this test iCVV must be performed, and be successful. The transaction must be approved online. There is also a 6 digit PIN value on the card. During the transaction the terminal is tested if it can handle this.

C.1.17 Visa ADVT Test Case 17

The minimum amount of data fields on an EMV credit card is the same as a magnetic stripe image. This also implies that Static Data Authentication and Dynamic Data Authentication are not supported, and can not be performed with this card. Test case 17 has a card with this minimum amount of data fields. The terminal must process the transaction normally, the test is successful if the transaction is approved.

C.1.18 Visa ADVT Test Case 18

As described before, there are different specifications of the EMV standard, because each Credit Card Company has his own implementation. Visa also has an additional feature called Visa Low-Value Payment (VLP). This is a Visa only feature that a terminal can implement (optional). The VLP feature provides cards with an optional source of pre-authorised spending power that is reserved for rapid processing of offline low-value payments. The main idea is that the card has a pre-authorised amount. For low-value payments (a configured amount) the card will authorise the payment offline. The transaction amount is subtracted from the VLP Available Funds. When the VLP Available Funds is less then the transaction amount, the transaction must be authorised online. During every online transaction or message (for example: check available funds online) the VLP Available Funds is reset to the VLP Funds Limit. [30] Test Card 18 supports VLP. When the terminal does not support VLP, the PIN must be checked and the transaction must be authorised online. When the terminal does support VLP, the transaction is authorised offline without the PIN check. Because this functionality is not mandatory and Visa specific, it is not implemented into the Trintech terminal.

C.1.19 Visa ADVT Test Case 19

Each application on an EMV credit card has an Application Identifier (AID). A terminal should no accept a card as the AID on the card is not a valid AID. When a transaction is performed with such a cart the terminal should display 'Not Accepted'. In these cases the terminal may fallback to the magnetic stripe on the card to perform the transaction. This part of the specification is tested in test case 19. Because the end of the transaction can be different for different terminals this is out of scope of the test.

C.1.20 Visa ADVT Test Case 20

The brand Visa has also a sub-brand, called Visa Electron. A Visa Electron credit card has a different AID then the normal Visa credit card. The test card that belongs to this test is a Visa Electron credit card. When a terminal supports the Visa Electron brand, this transaction must approved. The reference PSP wanted to support this brand. The transaction must therefore be approved for a successful test result.

C.1.21 Visa ADVT Test Case 21

A Visa account number/ credit card number is 16 digits long. A credit card number in general can be maximum 19 digits long [12]. The card that belongs to this test has a 19 digits account number. Supporting 19 digits card numbers is not mandatory for Visa. Therefore this test is only for information gathering. When the test fails, because the terminal does not support 19 digits card numbers, the terminal should be adapted for the future. The used Trintech terminal already supports credit card numbers of 19 digits. The transaction must therefore be authorised.

C.1.22 Visa ADVT Test Case 22

Besides the sub-brand Visa Electron, Visa has an other sub-brand: Visa Debit. This is not a credit card, but a debit card. The card that belongs to this test contains two applications: Visa (Credit) and Visa Debit. This is in place to ensure that a terminal can handle a card that contains two different applications. When the terminal supports 'Cardholder Selection' (like the used Trintech terminal), the available applications for cardholder selection must be displayed. The Visa Credit application should be showed first, because this application has a higher Application Priority Indicator. For terminals that support 'Cardholder Confirmation', the terminal must first display the Visa Credit application. When this application is rejected by the shopper, it should display the Visa Debit application. For terminals that do not support both of these features, the terminal should select the Visa Credit application, because it has the highest Application Priority Indicator. The transaction should be approved for a successful result of the test.

C.1.23 Visa ADVT Test Case 23

A credit card can be configured with different Application Usage Control settings. One of these settings can indicate that the card can not be used for international transactions. If

it is used for such transactions, the bit 'service not allowed for card product' in the TVR will be set. The terminal should be configured in such a way, that when it wants to process a transaction where the 'service not allowed for card product' is set, the transaction is declined. The card that belongs to this test has this Application Usage Control setting and an unknown country code. The transaction should therefore be declined offline. When the transaction is sent online for authorisation, or when the transaction is approved offline, the test fails.

C.1.24 Visa ADVT Test Case 24

Test case 24 only applies to terminals that support Dynamic Data Authentication. The terminal should be configured that when DDA fails, the transaction is declined offline. The card is configured in such a way that DDA will fail. Therefore the transaction should be declined. When the transaction is sent online for authorisation, or when the transaction is approved offline, the test fails.

C.1.25 Visa ADVT Test Case 25

The card that belongs to test case 25 is configured so that it has Issuer Authentication as mandatory setting. This means that a transaction must always be send online for issuer decision. Therefore, the transaction must be authorised online for a successful test result. When the transaction is not sent online the test fails.

C.1.26 Visa ADVT Test Case 26

This test tests the magnetic stripe fallback functionality (for backwards compatibility). Because this functionality is not mandatory for all countries, this test is for information gathering purpose only. The test card that belongs to this test has a faulty chip. When the terminal tries to read the chip, realize it is faulty, is must prompt for a swipe transaction. When the chip reader and magnetic stripe reader are separate the terminal should clearly indicate during the attempt to read the chip that the 'chip can not be read'. To indicate that fallback is supported, the terminal should provide a message such as 'Swipe Magnetic Stripe'. When the terminal has a combined reader is should be transparent for the shopper, because the magnetic stripe is already read when the shopper inserts his card. Therefore is should be printed on the receipt to inform the shopper that it was a fallback transaction. The terminal fails the test when the terminal does not allow the magnetic stripe to be read.

C.1.27 Visa ADVT Test Case 27

This test only applies to terminals that support Dynamic Data Authentication. The card that belongs to this test supports DDA. The transaction must be approved, and DDA must not fail, for a successful test result.

C.1.28 Visa ADVT Test Case 28

Test case 28 is only applicable to terminals that support Static Data Authentication. The card that belongs to this test supports SDA. The transaction must be approved, and SDA must not fail, for a successful test result.

C.1.29 Visa ADVT Test Case 29

The card that belongs to test case 29 has as first CVM 'Offline Enciphered PIN'. For POS devices supporting Offline Enciphered PIN, Offline Enciphered PIN should be used. For POS devices supporting Offline Plaintext PIN (the next CVM in the CVM list), and not supporting Offline Enciphered PIN, Offline Plaintext PIN should be used. For POS devices only supporting signature (third CVM in the CVM list), signature should be requested while ATM's should proceed to Online PIN (fourth CVM in the CVM list). The terminal should indicate that Cardholder Verification is successful, and that the CVM is recognized. The transaction must be approved for a successful result for the test.

C.1.30 Visa ADVT Test Case 30

Test case 30 tests if a terminal can process a card containing a CVM that the terminal does not recognize and where the CVM is not in the list of CVMs that are recognized by the terminal. The card that belongs to this test has as first CVM in the list a 'Reserved For Future Use' CVM, with instructions to apply the next CVM is the CVM processing fails. The next CVM in the list is signature. Because the terminal will first find the unrecognized CVM, part of the pass criteria is that the terminal must set the Unrecognized CVM bit in the TVR, and go to the next CVM. The transaction should be approved to totally pass the test.

C.1.31 Visa ADVT Test Case 31

In test case 31 the first CVM in the CVM list of the card is also Reserved For Future Use, but has the instruction to stop when the CVM is not recognized. When the transaction is performed with this CVM the terminal must set the Unrecognized bit in the TVR, but also the Cardholder Verification Failed bit. The card is configured that when Cardholder Verification fails, the transaction must be declined. The test result is successful if the test is declined and all the needed TVR bits are set.

C.1.32 Visa ADVT Test Case 32

A card can have a PIN Try Limit that indicates how many times the shopper can press a wrong PIN. For example, when the PIN Try Limit is 3, the shopper must press a correct PIN within 3 times. When the shopper also presses a wrong PIN during the third possibility, the PIN will be blocked. The card that belongs to this test case is configured with a PIN Try Limit of 0. The first CVM is Offline Plaintext PIN which will fail, because the PIN is blocked. The terminal must inform the shopper with a message like 'PIN Try Limit

Exceeded' and the PIN Try Limit Exceeded bit in the TVR must be set. When the terminal supports Online PIN (second CVM), the terminal should check the PIN online. If the terminal does not support Online PIN, it should fallback to signature check (third CVM). When both CVMs are not supported (for example in a Car parking terminal, without Online PIN) the transaction must be decline, because Cardholder Verification was not successful. Else the transaction must be approved.

C.1.33 Visa ADVT Test Case 33

The card that is used for test case 33 has also a PIN Try Limit value of 0, but has only 1 CVM. During the transaction the terminal must therefore set the PIN Try Limit Exceeded bit in the TVR, and also the CVM Failed bit. The card is configured that when CVM fails, the transaction must be declined offline, which is the pass criteria for this test.

C.1.34 Visa ADVT Test Case 34

Test case 34 checks if the terminal can process a card with a CVM List with three CVMs (Offline Plaintext PIN, Signature, and NO CVM Required). Since the card for this test does not support Online PIN, an ATM will arrive at the end of the CVM list, see that the last CVM is 'No CVM Required' and may request Online PIN (ATMs are allowed to use Online PIN as a default CVM when the card does not contain Online PIN in its CVM list). The Cardholder Verification Not Successful bit in the TVR should be set, even where default CVM processing operates, and provided the ATM does not contain the 'No CVM Required' method. POS devices should utilize Offline PIN or signature and set the Cardholder Verification Successful bit in the TVR. The transaction should be approved for a successful test result.

C.1.35 Visa ADVT Test Case 35

This test checks if a terminal can handle a card that supports only Online PIN. For devices that do support Online PIN, Online PIN should be processed and the transaction should be sent online and approved. For devices that do not support Online PIN (like the Trintech terminal), the terminal must set the Cardholder Verification Failed bit in the TVR and decline the transaction offline. Depending on the terminal capabilities the result of this test differs.

C.1.36 Visa ADVT Test Case 36

Test case 36 tests if a terminal can process a card correctly that contains a CVM List where the first CVM is Online PIN, the second CVM is Offline PIN, the third CVM is Signature, and the last CVM is No CVM. The terminal must walk through the CVM List and should pick the first CVM that is supported. The transaction should be approved offline or online. For Online PIN, the transaction must be approved online of course. The first CVM is the list that is supported by the used Trintech terminal is Offline PIN.

C.1.37 Visa ADVT Test Case 37

The card that belongs to test case 37 is configured with a CVM List with No CVM Required and Online PIN. An ATM can not handle the CVM 'No CVM Required'. Therefore an ATM should use the Online PIN CVM. POS applications that support the No CVM Required CVM should use this in the first place. When this CVM is not supported, the terminal should perform Online PIN. When the terminal reaches the end of the CVM List without any matching CVMs, cardholder verification has failed and the Cardholder Verification Failed bit in the TVR must be set. When one of the CVMs is supported, the transaction must be approved for a successful result of this test.

C.1.38 Visa ADVT Test Case 38

The issuer can configure the card that the terminal must pick a certain CVM depending on the amount and the currency of the transaction. For example, a card can be configured that it should use Offline PIN when the amount of the transaction is above 50.00 GBP, else use Signature. The card that belongs to this test has three of these CVMs, but the currency is set to an unknown value. Therefore these CVMs will never match, and must be ignored by the terminal. The card has also has the CVMs Offline PIN, Online PIN, Signature, and No CVM Required. The terminal should pick the first CVM that matches the terminal capabilities and use this CVM for the transaction. The transaction must be approved for a correct result of the test.

C.1.39 Visa ADVT Test Case 39

A CVM can also contain more then 1 cardholder verification check, like signature and offline PIN. In test case 39 this functionality is tested: the card that belongs to test case 39 has a combined CVM of signature and offline PIN. When a terminal only supports 1 of these 2 CVMs, then only that must be used. For ATMs, online PIN should be used. For a successful test result the transactions must be approved.

C.1.40 Visa ADVT Test Case 40

In test case 31 the PIN Try Limit with a value of 0 is tested. In test case 40 the functionality of a PIN Try Limit of 1 is tested. When the PIN Try Limit is 1, the terminal should display the message 'Last PIN Try' to indicate that when the shopper enters a wrong PIN, the PIN will be blocked. After the message is displayed, and the correct PIN is pressed, the transaction must be approved. When the terminal does not display the message, or when the transaction is declined, the test fails.

C.1.41 Visa ADVT Test Case 41

According the EMV specification the account number can be maximum 19 digits long [12]. Currently most credit cards have an account number of 14 or 16 digits. When the account number is less then 19 digits long, the issuer can pad the account number with hexadecimal

'Fs' to the maximum account length. The terminal should be able to handle this format, and ignore the padded hexadecimal 'Fs'. Also on the receipt the normal account number must be printed, and not the padding hexadecimal 'Fs'. The transaction must be approved, with a correct receipt for a successful test result.

C.1.42 Visa ADVT Test Case 42

In test case 2 the Payment Systems Environment (PSE) is tested. In test case 42 the card also contains a PSE, but the PSE contains optional data elements that are not included in the application. Although in most cards, the PSE data and application data matches, the terminal should not terminate the transaction when these date elements do not match. Therefore the pass criteria for this test is that the transaction must be approved.

C.1.43 Visa ADVT Test Case 43

An EMV card can have an PAN Sequence Number which indicates how many times a credit card with the same account number is issued to the shopper. For example, when a credit card expires, the shopper can receive a new credit card with the same account number, but with a new expiration date. The first card has a sequence number of 1, the second card a sequence number of 2, etc. The issuer can also indicate that the sequence number is not used by not configuring the PAN Sequence Number or to set the value to 0. Almost all Visa cards have sequence number present, but the test card of test case 43 does not. A terminal should also be able to handle these cards. The test transaction must therefore be approved for a successful test result.

C.1.44 Visa ADVT Test Case 44

The test card of test case 44 has a PAN Sequence Number with a value of 11. The terminal should be able to handle this transaction, and approve it. When the PAN Sequence Number is available on the card, it must also be printed on the receipt. The pass criteria are that the transaction is approved, and the PAN Sequence Number on the receipt has a value of 11.

C.1.45 Visa ADVT Test Case 45

For card applications supporting Dynamic Data Authentication (DDA), Combined Data Authentication (CDA), or Offline Enciphered PIN, the ICC Public Key Certificate on the card that is used for these functionality needs to fit within the 254 byte record limit. To accommodate the tags and lengths of the certificate and the record template in the record that contains this certificate, the maximum size of the ICC Public Key Certificate is restricted to 247 bytes (1976 bits) [14]. Consequently the Issuer Public Key, which is the same length as the certificate, is also restricted to 247 bytes (1976 bits). Test case 45 has a test card with a Issuer Public Key Certificate based on a 1016-bit Issuer Public Key. The terminal should be able to process this card in the proper way, and approve the transaction. An decline of the transaction indicates a failure of the test.

C.1.46 Visa ADVT Test Case 46

This test case has a card that is configured with an Issuer URL (Issuer Discretionary Data) and an Application Expiration Date that is set to December 31, 2025. The terminal should be able to process a card were the Issuer Discretionary Date field is set. The outcome of this test depends on the terminal settings, but an offline decline of the transaction indicates a failure of the test. An online approval, or an online decline indicates a success of the test.

C.1.47 Visa ADVT Test Case 47

The card of test case 47 has a blocked application. This means that the card can not be used (any more). At the start of the transaction the terminal must display 'Application Blocked' and stop the transaction immediately. When the terminal tries to process the transaction, or tries to fallback to magnetic stripe, the test fails.

C.2 MasterCard

The current EMV MasterCard certification process contains 45 tests. These 45 tests are performed with 18 cards. Only 31 tests must be performed with these 18 cards for attended combined card readers like the Trintech Smart 5000. In the next subsections the 31 tests will be discussed. All the information about the test cases is gained during the life certification and retrieved from the literature [22, 21].

MasterCard has a simulator that sends a different response back depending on the amount of the transaction. In this way MasterCard can use the same card for more then 1 test case.

C.2.1 MasterCard5A REQ01 01 01

The first test of the MasterCard tests will ensure that the terminal correctly behaves when offline Card Authentication Method (CAM) (both SDA and DDA) is not supported. This functionality is part for the CAM requirements for terminals. One of the pass criteria is that the TVR bit 'Offline data authentication was not performed' is set. For a successful test result the transaction must also be approved.

C.2.2 MasterCard5A REQ01 02 01

MasterCard5A REQ01 02 01 is to ensure that the terminal is able to receive and correctly transmit the issuer decision in its final environment of use. Even though the Issuer Authentication Date (IAD) is sent back by the Issuer, the card must not receive an External Authenticate command after the First Generate AC command to check the IAD data, as issuer authentication is not supported by the card. Therefore the TVR bit 8 'Offline data authentication was not performed' must be set to 1, and the transaction must be approved for a successful test result.

C.2.3 MasterCard5A REQ01 04 01

MasterCard has the restrictions that an attended POS may only process MasterCard cards that have a CVM. Test case MasterCard5A REQ01 04 01 is to ensure that an attended POS will never approve a MasterCard transaction with NO CVM. Therefore the card is configured in such a way that the first CVM in the CVM list is 'NO CVM'. The pass criteria are that the transaction is approved with the second or the third CVM: PIN verification, or signature verification.

C.2.4 MasterCard5A REQ02 01 03

This test case checks if the terminal can handle a card that is configured with SDA only. Since the ICC is configured with an Application Interchange Profile (AIP) requesting offline static data authentication, the terminal must continue the transaction until the completion of the offline data authentication process. A successful result for the test is that offline data authentication does not fail. The end of the transaction (approval or decline) is out of scope.

C.2.5 MasterCard5A REQ02 04 01

After the First Generate AC command the terminal should send the data from the issuer's response (which is received when the transaction goes online) to the card during Second Generate AC command.

This test case checks if the terminal can handle a transaction that is decline online by the issuer. Therefore the Terminal must send a decline in the Second Generate AC command. The test is successful if the terminal sends a decline request to the card during the Second Generate AC command, and when the card responses with a decline. When the transaction is not declined by the issuer, or not declined after the Second Generate AC command, the test fails.

C.2.6 MasterCard5A REQ02 05 01

This test case is almost the same as the MasterCard5A REQ02 04 01 test case, but instead of a decline request during the Second Generate AC command, the issuer indicates that the terminal must request a referral during the Second Generate AC command. The card must approve the referral and the terminal must tell the Merchant that he should call the bank for an authorisation code. The merchant must fill in the code 'ABC234' as authorisation code and authorise the transaction for a successful test result.

C.2.7 MasterCard5A REQ02 11 01

Step 10 of the EMV standard is Issuer-to-Card Script Processing. The terminal must be able to receive such a script from the issuer and correctly transmit the script to the card. This script processing can be done before or after the Second Generate AC command. This test case tests the script processing by sending a Pin Change/Unblock command, before

the Second Generate AC command. The issuer only sends this script back to the POS application when the specific amount of 123.00 GBP is used.

Pass criteria for this test are that the script is correctly received and transmitted to the card. Also the TVR bit 'Script Processing failed' must be 0 (indicating that the script is processed correctly) and the transaction must be approved.

C.2.8 MasterCard5A REQ02 20 01

A terminal should be able to handle cards that have an inconsistency between track2 equivalent data and track2 discretionary data in the ICC. Track2 discretionary data is specific data that is configured by the issuer. Visa is not using this field, but MasterCard does. The card for this test is configured in such a way that these 2 fields have a different content. The terminal should process the transaction normally, and approve it for a successful test result.

C.2.9 MasterCard5A REQ02 21 01

The MasterCard5A REQ02 11 01 test is also in place to check script processing. In this test case the terminal receives a wrong formatted script from the issuer. When a terminal receives such a script, script processing will fail.

For a successful test result the 'Script Processing failed' bit in the TVR must be set to 1, the response of the script processing must be '6983', and the response of the Second generate AC command must be '6985' which indicates a decline. When one or more of the criteria are not met, the test fails.

C.2.10 MasterCard5A REQ02 22 01

This test tests if the terminal can process a transaction where some mandatory issuer response data is not returned when the transaction is sent online. When this data is not available, the transaction must be declined. When this data is in the response, or when the transaction is authorised, the test fails.

C.2.11 MasterCard5A REQ02 26 01

During the Second Generate AC command the terminal requests (most of the times) a TC (for approval). The card can response with a TC which indicates that the transaction is approved, but the card can also decline the transaction, indicated by an AAC response. The card for this test responses with an AAC during the Second Generate AC command to test if the terminal can handles this. For a successful test result the terminal must request a TC during the Second Generate AC command and the card must decline the transaction by responding with an AAC. When the card responses with an approval, the test fails.

C.2.12 MasterCard5A REQ02 27 01

Test MasterCard5A REQ02 27 01 is to check that the terminal is able to correctly manage payments of gratuities. The purchase amount for this test transaction must be equal to 26.00

GBP and gratuity amount must be equal to 1.00 GBP. Pass criteria for this test is that the authorised amount that comes back in the issuer response must be equal to 27.00 GBP, and the transaction must be approved.

C.2.13 MasterCard5A REQ02 31 01

This test case is to ensure that the terminal is able to receive more then 1 command in an issuer script and correctly transmit them to the card. In test case MasterCard5A REQ02 31 01 the issuer sends back 7 Application Block commands. All these commands must be send to the card in the order that the issuer has sent them to the terminal. To indicate that all the scripts are processed correctly, the 'Script Processing failed' bit in the TVR must be 0. Therefore, for a successful test result, the scripts must be send to the card in the correct order, the processing of this scripts must be successful, and the transaction must be approved.

C.2.14 MasterCard4C REQ03 01 03

The test card that belongs to this test is configured SDA support. Before the First Generate AC command the terminal must send an Internal Authenticate command to verify the static data. The pass criteria for this test is that the Internal Authenticate command is processed successfully, indicated by the TVR bits 'Offline data authentication was not performed' set to 0, 'Offline static data authentication failed' set to 0, and 'Offline dynamic data authentication failed' set to 0. The end of the transaction is out of scope of the test.

C.2.15 MasterCard6A REQ05 01 01

Test case MasterCard6A REQ05 01 01 checks if the terminal can process a card with a CVM List with three CVMs (Signature, Enciphered PIN, and NO CVM Required). The terminal must select the CVM Signature (if supported) and process the transaction correctly. The Cardholder Verification Successful bit in the TVR must be set, and the transaction must be approved for a successful test result.

C.2.16 MasterCard6A REQ05 02 01

The terminal must not only be able to perform issuer script processing before the Second Generate AC command, but also after this command. This test must be performed with a transaction amount of 20.00 GBP which results in response from the issuer with a script that should be processed after the Second Generate AC command. The script is a Card Block command, but it is not really committed, because this would imply that the test card can only be used for one test iteration.

The test is successful when the script is processed in the right order, the 'Script Processing failed after final Generate AC' bit is 0, and the transaction is approved.

C.2.17 MasterCard6A REQ05 04 01

This test case is almost the same as the previous test case. The only difference with the previous test is that the transaction amount is 30.00 GBP instead of 20.00 GBP. The 30.00 GBP amount will result in a response from the issuer with a script that contains 4 commands. All 4 commands must be processed after the Second Generate AC command for a successful test result. The correct TVR bit must be set (like in the previous test case), and the transaction must be approved.

C.2.18 MasterCard5A REQ06 02 01

This test verifies how the PIN Entry Bypass is managed by the terminal. The card is configured with a CVM List that has plain text PIN as first CVM in the list. When the terminal prompts with the message 'Enter PIN' the PIN must be bypassed. The terminal must then fallback to the next CVM in the CVM List which is Signature. The bit 'PIN entry required, PIN pad present, but PIN was not entered' in the TVR must bet set to 1, and the bit 'Cardholder verification failed' must be 0, because signature check is successful. Depending on the IAC the transaction is approved or declined.

C.2.19 MasterCard5A REQ06 03 01

The previous test case tests PIN Entry Bypass. MasterCard5A REQ06 03 01 checks that a time out on PIN entry is not considered as PIN Entry Bypass. When the terminal prompts with the message 'Enter PIN' nothing must be done. After a certain time the transaction must time out and be declined. A fallback transaction indicates a failure of the test.

C.2.20 MasterCard4C REQ07 01 02

To ensure that the terminal will not perform a fallback transaction when the transaction is completed with chip, the card response with a decline after the First Generate AC command. The transaction must be declined. A fallback transaction indicates a failure of the test.

C.2.21 MasterCard4C REQ07 02 01

When a transaction is declined, the terminal must be able to provide the Merchant with the values of different EMV tags from the transaction (for example the value of the TVR). This information must be provided either by printing it on a display or on an electronic file. The test is successful if the transaction is declined, and when the terminal can provide the required information.

C.2.22 MasterCard4C REQ08 01 01

When the card sends back an invalid response when the terminal tries to read the ICC, the terminal must fallback to the magnetic stripe of the card. This functionality is tested with test card MasterCard4C REQ08. The terminal must continue the transaction according to

the standard rules of magnetic stripe processing. The end of the transaction is out of scope of this test.

C.2.23 MasterCard4C REQ09 01 01

During this test the card sends back a correct response when the terminal tries to read the ICC, but the terminal will end up with an empty candidate list, because there is not application configured on the card. The terminal should fallback to the magnetic stripe of the card, and continue the transaction according to the standard rules of magnetic stripe processing. The end of the transaction is out of scope of this test.

C.2.24 MasterCard5A REQ10 01 01

When the First Generate AC command fails the terminal should fallback to the magnetic stripe. Test card MasterCard5A REQ10 returns the value '6985' which indicates such a failure. The terminal must then continue the transaction according to the standard rules of magnetic stripe processing. A special configuration for this card is that the track2 data of the ICC is different then the track2 data from the magnetic stripe. In this way MasterCard can tell that the track2 data really comes from the magnetic stripe and not from the ICC. The transaction must be approved with the correct track2 data. When the track2 data from the ICC is used instead of the track2 data from the magnetic stripe, or when the transaction is declined, the test fails.

C.2.25 MasterCard4C REQ11 01 02

The card that belongs to this test has a blocked application. When the application is blocked the terminal must not fallback to the magnetic stripe like the previous tests. An offline decline of the transaction indicates a successful test result.

C.2.26 MasterCard4C REQ12 01 02

Not only an application on a card can be blocked, also the card itself. When a card is blocked the terminal should also not fallback to the magnetic stripe of the card. The pass criteria for the test is an offline decline.

C.2.27 MasterCard4C REQ13 02 01

Test card MasterCard4C REQ13 is configured with a CVM List that contains Plaintext PIN, Signature, Online PIN, and No CVM. The POS application must select the right CVM from the list (Plaintext PIN) and approve the transaction for a correct test result. The card does also not support data authentication which much result in that the 'Offline data authentication was not performed' bit in the TVR is set to 1. The test is successful if this bit is set and the transaction is approved.

C.2.28 MasterCard4C REQ15 01 01

Test case MasterCard4C REQ15 01 01 is in place to ensure that the terminal is able to provide the right Transaction Category Code (TCC) value when requested by the card. The TCC is a MasterCard specific field. The card will check the value of the TCC and must respond to First Generate AC by '9000' if the TCC value is correctly set, or '6985' which indicates a failure of the test.

C.2.29 MasterCard4C REQ17 01 01

Like Visa Test Case 8, MasterCard also tests the terminal behaviour when the Application Version Number of the card has a different value then the terminal. Because the test card that belongs to this test has a different version number then the terminal, a pass criteria is that the terminal sets the 'ICC and terminal have different application versions' bit in the TVR to 1. The transaction must also be approved for a successful test result.

C.2.30 MasterCard4C REQ18 01 01

The EMV specification has room for future use. Therefore there are also CVMs that should not yet be processed by the terminal. This test card (like the test card of Visa Test Case 30) has as first CVM in the list a 'Reserved For Future Use' CVM. When the terminal finds such a CVM it must set the Unrecognized CVM bit in the TVR, and go to the next CVM. This is the only pass criteria for this test. The end of the transaction is out of scope.

C.2.31 MasterCard4C REQ22 01 01

When the terminal finds an inconsistency between the credit card number tag of the ICC and the credit card number that is specified in the Track 2 equivalent data tag, it must decline the transaction. This part of the functionality is tested in the last MasterCard test. Because this test card is configured with this inconsistency the terminal must decline the transaction by requesting an AAC in First Generate AC command or by aborting the transaction after Read Record command (after noticing that there is inconsistency). When the terminal sends the transaction online, or approves the transaction, the test fails.

Appendix D

Branch Coverage of the EMV Certification Process

In this appendix the specification of the EMV implementation will be mapped to the test suites of the two main credit card companies: Visa and MasterCard. The mapping is performed by checking the coverage for each test of each test set of the transaction flow. This mapping is illustrated by one ore more transaction flows for each EMV step. Each flow describes the possible branches that can be taken during a transaction. The red arrows in these flows indicate that that specific branch is not covered by all the tests of the test suite.

D.1 Visa test suite

In the next sections the mapping of the specification of the EMV standard with the Visa test set is discussed. In Appendix E the possible flows of the transaction are specified for each step.

D.1.1 Application Selection

The first step of the EMV protocol is Application Selection. The figures that belong to this step are Figure E.1, Figure E.2, and Figure E.3.

There is a Visa test card (Test Case 47) with a blocked Visa application, but there is no test card that is totally blocked. Therefore the branches in the Application Selection flow for Directory Selection Method and the List of AIDs Selection Method for a blocked card are not tested.

There are a couple of cards with a PSE configured but none of them have more then 1 entry in the record. There is no card that has a PSE configured that responses with an error (a response that is not equal to 9000) during the select command. Therefore the branches after this error are also not checked.

The Visa test set does not have a card with an AID file that does not have an exact name and not an partial matched name in the FCI. It has a card with a partial matched name in the FCI, but not a card with this configuration where Partial Selection is not supported.

Visa does not test the functionality when there is no application selected, or when the cardholder does not confirm a certain application. Also the select command to retrieve the FCI for a requested AID is always successful (response is 9000).

D.1.2 Initiate Application Processing/ Read Application Data

The figures with the processing flow that belong to step 2 are Figure E.4, and Figure E.5.

The read record command that is used in the Read Application Data step is always successful for all the Visa test cases. There is also no card which has not all the mandatory data configured, or where the terminal received data element tags that are already received.

D.1.3 Offline Data Authentication

Visa does not test the Combined DDA/AC Generation with the Visa test set as can be seen in Figure E.6. By default the test cards of Visa support SDA, but there is no card that supports SDA and does not have SDA data present (Figure E.7). There are also a couple of cards that support DDA. For all these cards hold that DDA must successfully be handled. Therefore DDA failure is not tested as indicated in Figure E.8, Figure E.9, and Figure E.10.

D.1.4 Processing Restrictions

There are a lot of branches in the Processing Restrictions step that are not tested. These can be found in Figure E.11. For example, there is no card that has not an Application Version Number configured, or a card that does not have an AUC and an Issuer Country Code.

Test card 23 is not allowed for requested services, because the issuer country code is not equal to the terminal country code, and the card is not allowed to process international transaction. But there is no card with different country codes that is allowed to process international transactions. There is also no card with where the issuer country code is the same as the terminal country code, and where the card is not allowed for domestic transactions.

D.1.5 Cardholder Verification

The first flow in step 5, Cardholder Verification, is CVM List Processing (see Figure E.12). As can be seen in this figure, there is no card that is configured with no CVM List present.

Visa does not test a unsuccessful result on the Get PIN Try Counter command (Figure E.13). There is also no test case where Visa tests how the terminal will respond when the shopper presses the wrong PIN. Therefore not only this branch is not tested, but also all the branch that are reachable through this branch, as indicated by all the red arrow in Figure E.14.

There is one test card (no. 29) with has an enciphered PIN configured. Because this test card has an ICC Public Key Certificate available, the Fail CVM Processing branch will not be tested (Figure E.15.

D.1.6 Terminal Risk Management

The first flow of Terminal Risk Management, step 6, is tested depending on the settings of the terminal. Therefore the Figure E.16 does not have any red arrows. The second flow, Figure E.17, contains almost only red arrows. The reason for this is that the Visa test set does not use Lower and Upper Consecutive Offline Limits.

D.1.7 Terminal Action Analysis

Terminal Action Analysis depends on the Issuer Authorisation Codes (IACs) and Terminal Authorisation Codes (TACs). As part of the setup for the certification, the Terminal Authorisation Codes must be loaded into the terminal. Also all the test cards have IACs configured. Therefore the branches that use a default value for these codes are never tested (Figure E.18).

D.1.8 Card Action Analysis

During step 8 the card performs action analysis as described in section 2.2.8. These are all actions that are performed in the ICC. During this step there is no communication with the terminal. Therefore there is no process flow for the step.

D.1.9 Online Processing

As stated in step 3, there is no card in the Visa test set to test Combined DDA/AC Generation. Therefore that part of the functionality is also not tested in this step, indicated by the red arrows in Figure E.19.

When the card indicates that the terminal must send an authorisation request to the issuer, the issuer always sends Authorisation Data back in the response. The branch where this data is not available is Therefore not covered. The response from the issuer also always indicates that the result is passed.

D.1.10 Issuer-to-Card Script Processing

Script processing is a powerful part of the EMV standard. With a script the issuer can change or adapt the configuration of the card. During Online Processing the response of the issuer never contains a script. The issuer-to-Card Script Processing is not a mandatory step, but this should not be a reason not to test this part when it is supported by the terminal. Because script processing is never done, Figure E.20 shows a lot of red arrows.

D.1.11 Completion

The final step of the EMV standard, step 11, is completion. In the last step there are again branches not tested, because no card contains Combined DDA/AC Generation (see Figure E.21). Also for all test card hold that the Second Generate AC command always responses with a TC.

D.1.12 Remarks

Part of the EMV specification are is referral transactions as described in section 2.4.1. Referrals are not tested by Visa.

There is one card in the Visa test set (no. 26) that tests Fallback functionality (see section 2.4.1), but this test is not sufficient. When the transaction is a Fallback transaction is should use the track2 data from the magnetic stripe and not from the ICC. The way to test this is to use different track2 data for the magnetic stripe and the ICC, like MasterCard. For the test card that Visa uses to test the Fallback functionality both values of the track2 data are the same. In this way, Visa is never able to tell if the track2 data if retrieved from the magnetic stripe or from the ICC. There is also more then one place where the card can indicate that the terminal should fallback to the magnetic stripe. Not all these positions where this can happen are tested.

When the CVM indicates that a PIN is required, the terminal must have the ability to bypass this PIN. This functionality is not tested by the Visa test set.

D.2 MasterCard test suite

There are a lot of branches in the Visa Specification that are not tested by the Visa ADVT Test Cases. The same holds for the test cases of MasterCard. In this section for each EMV step the missing branches for MasterCard are discussed. In Appendix F also the flows of the MasterCard test cases are specified for each step.

D.2.1 Application Selection

The coverage of the tests of MasterCard for the first step of the EMV protocol is almost the same as Visa. The figures that belong to this step are Figure F.1, Figure F.2, and Figure F.3.

A difference with Visa is that MasterCard has a specific test card (REQ09) that is configured with an empty candidate list, and Therefore falls back to the List of AIDs Method instead of PSE. But MasterCard does also not test partial match FCIs, like Visa does.

D.2.2 Initiate Application Processing/ Read Application Data

The processing flow that belong to step 2 can be found in Figure F.4, and Figure F.5.

The branch that is not tested by MasterCard is that the conditions of the card are not satisfied (Visa does check this).

Like Visa, the read record command that is used in the Read Application Data step is always successful for all the MasterCard test cases. There is also no card which has not all the mandatory data configured, or where the terminal received data element tags that are already receives.

D.2.3 Offline Data Authentication

There is no MasterCard configured that supports Combined DDA/AC Generation, as can be seen in Figure F.6. There are some cards that support SDA, but when it is supported, it never fails. For this reason Figure F.7 indicates a lot of red branches.

There is one MasterCard that is configured for DDA. For DDA holds the same as SDA: it never fails. For this reason the figures that belongs to this step (Figure F.8, Figure F.9, and Figure F.10) indicate many red arrows.

D.2.4 Processing Restrictions

The tests for the Processing Restrictions step of MasterCard are worse then the tests of Visa. The flow of this step can be found in Figure F.11. There is no MasterCard that has a different Issuer Country Code then the Terminal. Like Visa, there is no card which is not yet effective, but there is also no MasterCard that is expired.

D.2.5 Cardholder Verification

The first figure of step 5, Figure F.12, indicates that there are also for this step a couple of branches not tested. There is no MasterCard that has no CVM List present, and there is no card where the CVM fails and where there is no other CVM in the list available.

The flow that belongs to the PIN Try Counter Checking, which is done when the CVM is PIN, can be found in Figure E.13. As can be seen in the figure, MasterCard does not have a card with no PIN Try Counter value. There is also no card where the PIN Try Counter is equal to zero.

PIN Processing flow can be seen in Figure F.14 and in Figure F.15. Because MasterCard does not test Enciphered Offline PIN, Figure F.15 is totally filled with red arrows. The Offline PIN Processing flow also indicates that the PIN verify command never fails. This means that there is no test where a wrong PIN must be entered.

D.2.6 Terminal Risk Management

The first flow of Terminal Risk Management, step 6, is tested depending on the settings of the terminal. Therefore the Figure F.16 does not have any red arrows. MasterCard does test the Lower and Upper Consecutive Offline Limits, in contrast to Visa which does not test the use of these values. Therefore the second flow, Figure F.17, has less red arrows then the Visa flow (Figure E.17) for this part of Terminal Risk Management.

D.2.7 Terminal Action Analysis

Terminal Action Analysis depends on the Issuer Authorisation Codes (IACs) and Terminal Authorisation Codes (TACs). As part of the setup for the certification, the Terminal Authorisation Codes must be loaded into the terminal. Also all the test cards have IACs configured. Therefore the branches that use a default value for these codes are never tested (Figure F.18).

D.2.8 Card Action Analysis

During step 8 the card performs action analysis as described in section 2.2.8. These are all actions that are performed in the ICC. During this step there is no communication with the terminal. Therefore there is no process flow for the step.

D.2.9 Online Processing

For step 9, Online Processing, the flow of MasterCard (Figure F.19) is almost the same as the flow of Visa (Figure E.19). The only difference is that MasterCard has a test where there is no Issuer Authentication Data in the response of the issuer.

D.2.10 Issuer-to-Card Script Processing

In contradiction to Visa, MasterCard does test Issuer-to-Card Script Processing. In the flow of this step, Figure F.20, can be seen that there is only one red arrow. The reason for this is that MasterCard does not have a test where the Issuer sends back more then one script.

D.2.11 Completion

Step 11, Completion, is the final step of the EMV standard. In the last step there are again branches not tested, because no card contains Combined DDA/AC Generation (see Figure F.21). In contrary to the Visa tests, not all test cards response with a TC in the Second Generate AC.

D.2.12 Remarks

The main branches of the EMV specification are tested by the MasterCard test cases, but as stated in the previous subsections, not all. There are a lot of small functionality that are not covered. This lead to a lot of red arrows in the processing flows of the 11 EMV steps.

Appendix E

Visa Transaction Flows

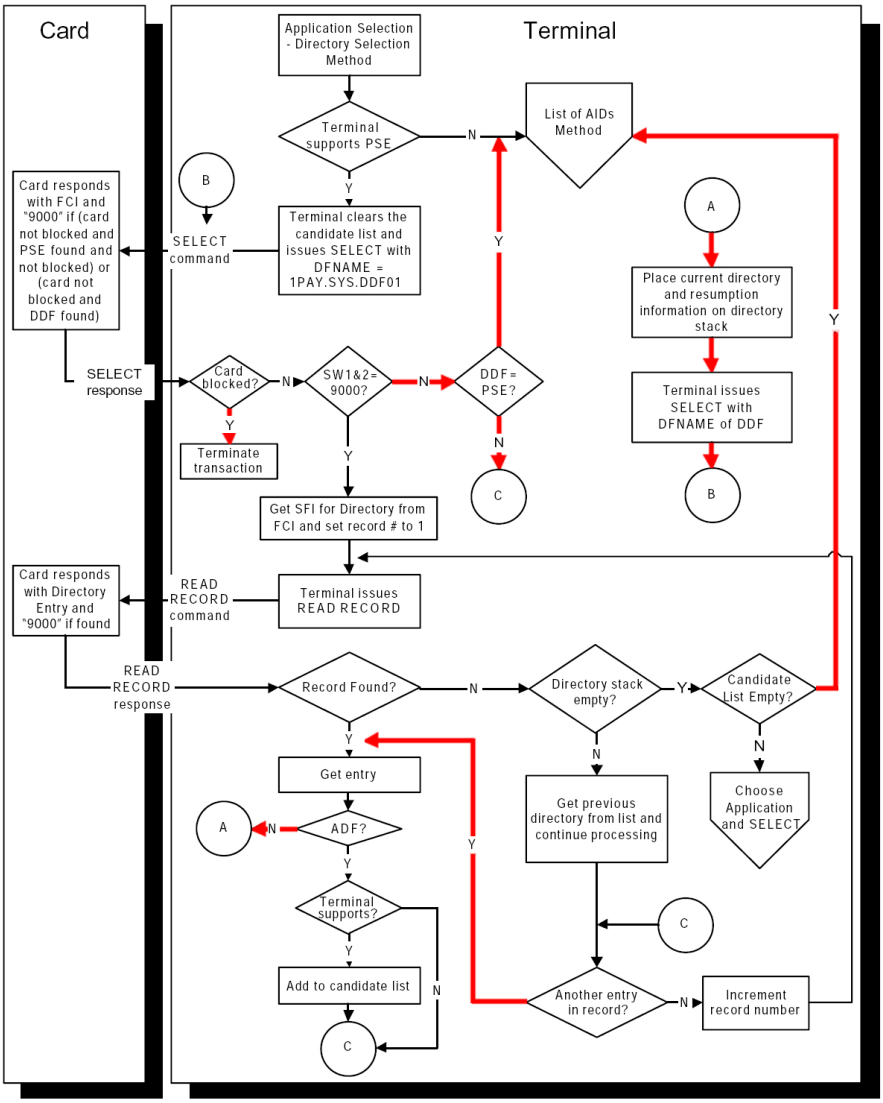


Figure E.1: Step 1: Application Selection Processing Flow (1 of 3)

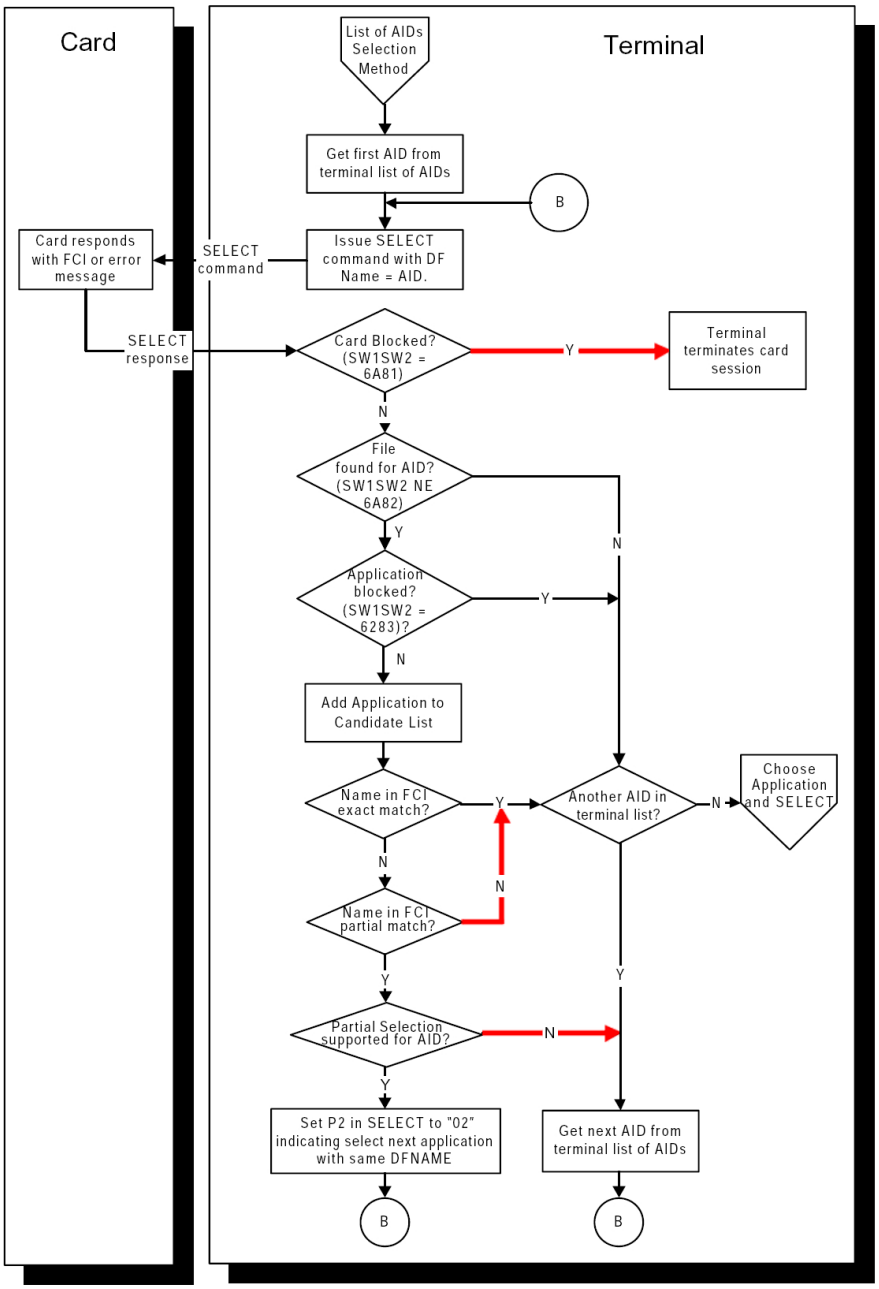


Figure E.2: Step 1: Application Selection Processing Flow (2 of 3)

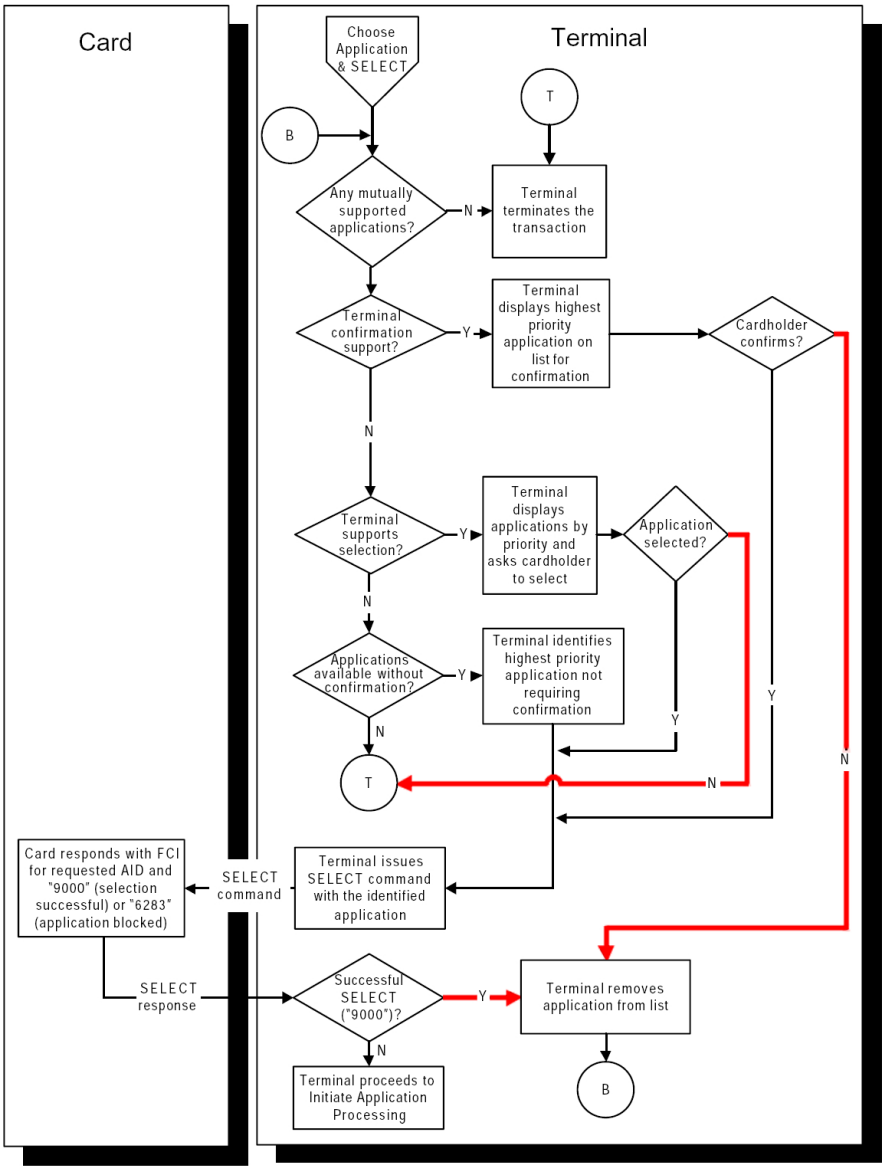


Figure E.3: Step 1: Application Selection Processing Flow (3 of 3)

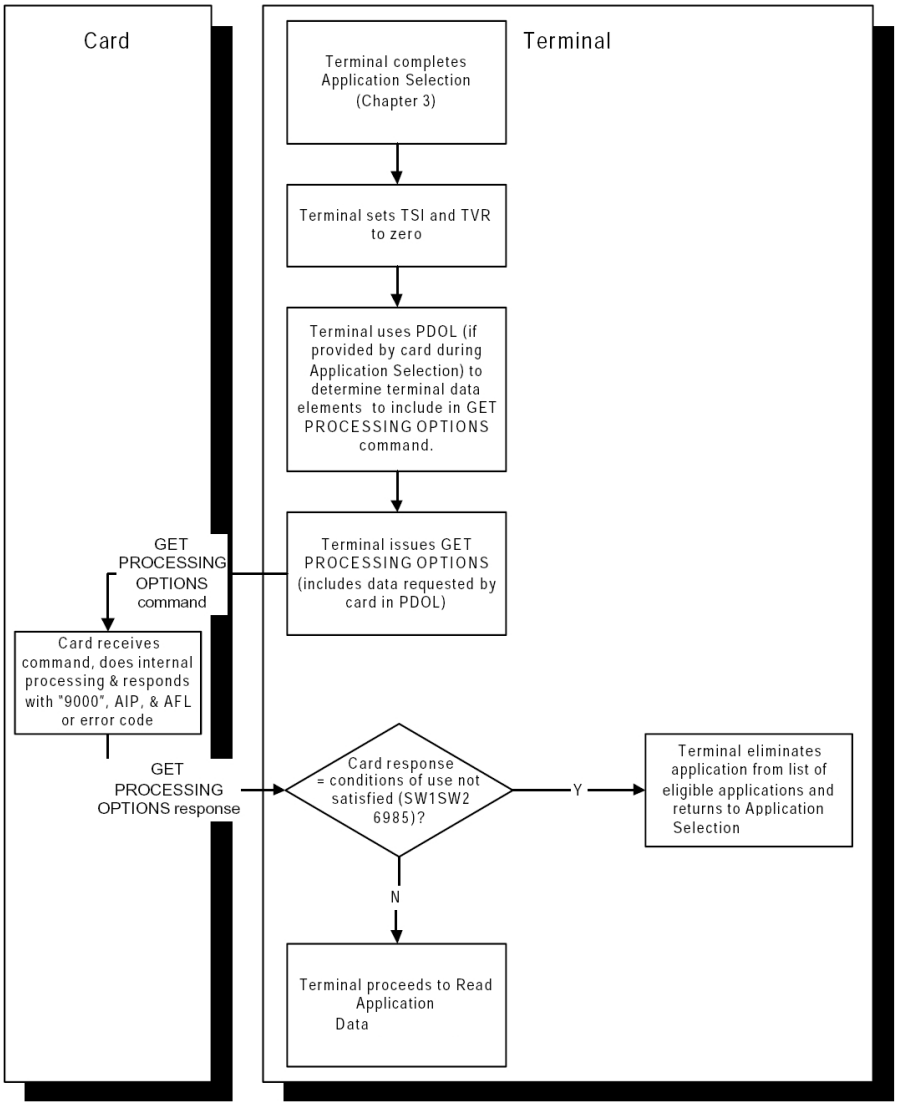


Figure E.4: Step 2: Initiate Application Processing Flow

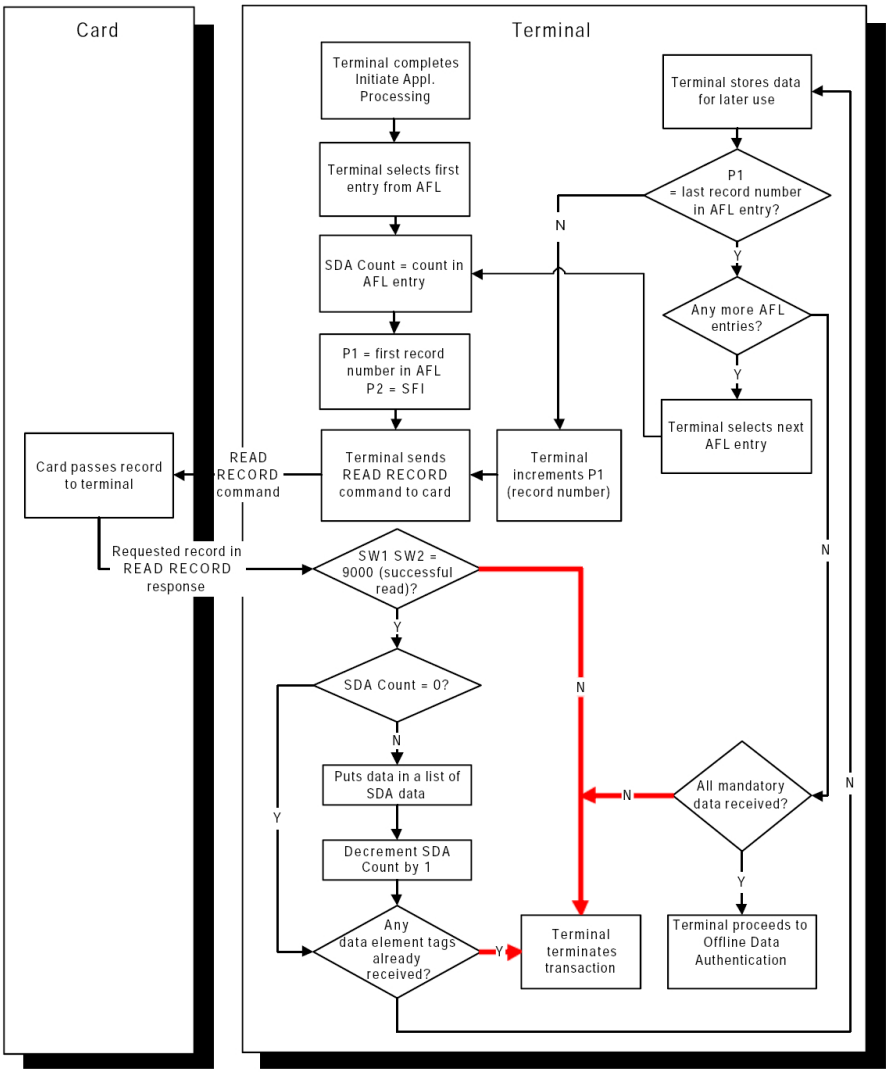


Figure E.5: Step 2: Read Application Data Processing Flow

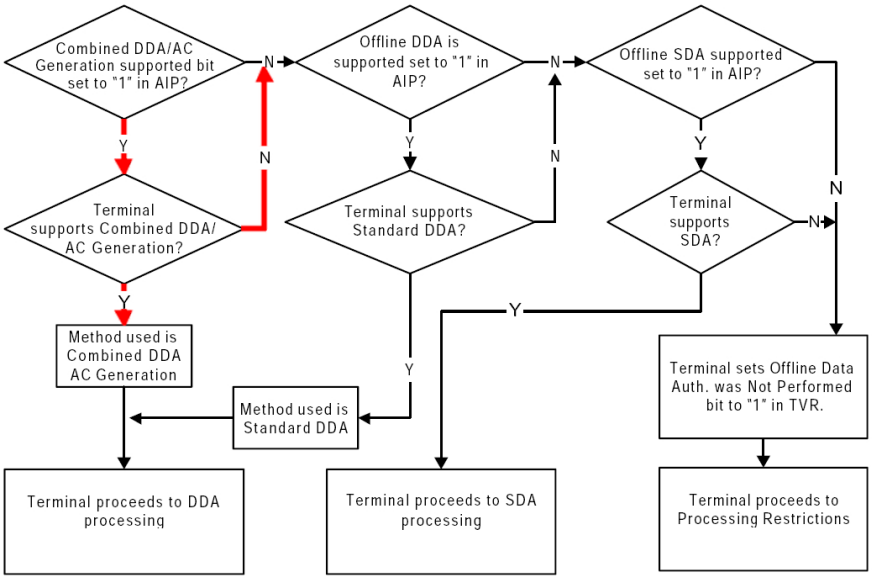


Figure E.6: Step 3: SDA or DDA Determination

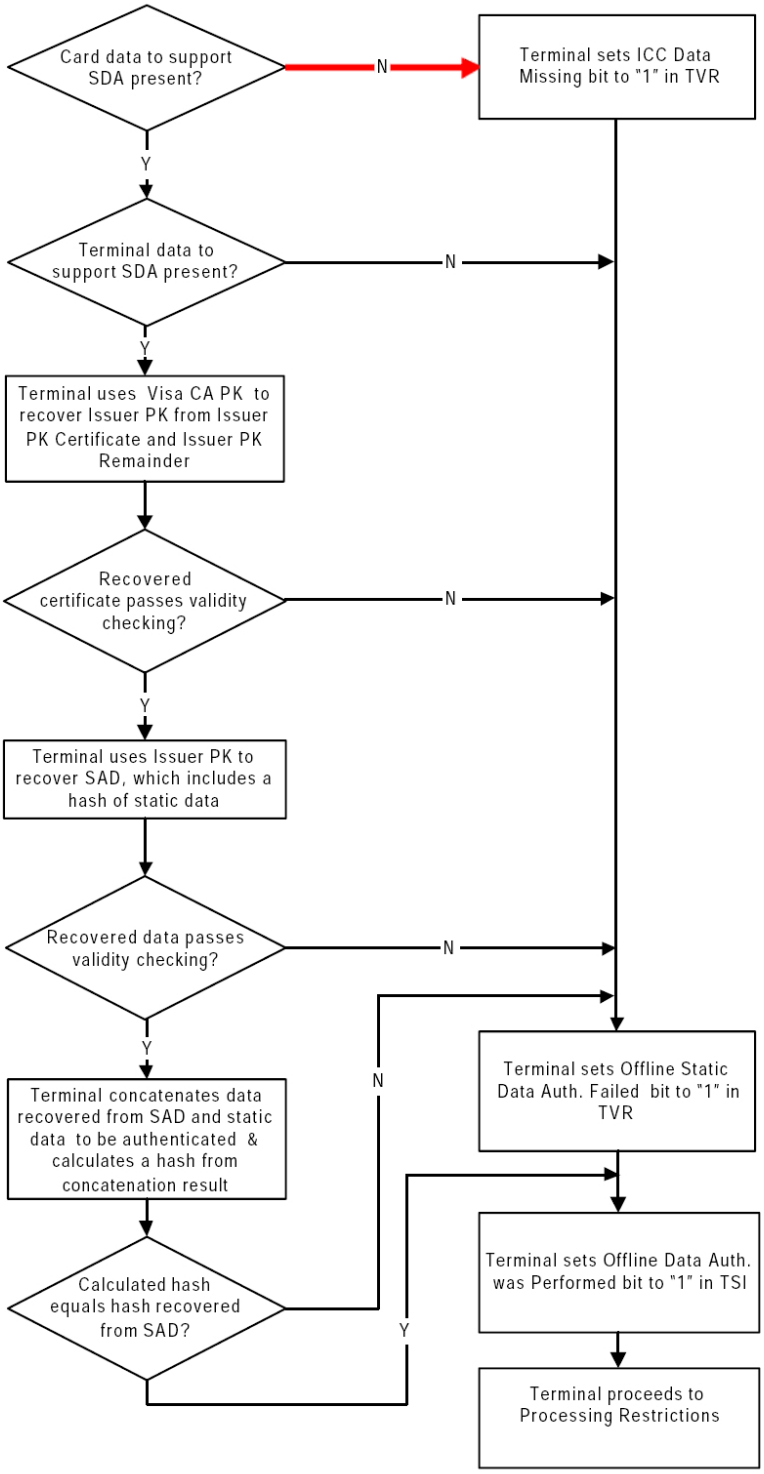


Figure E.7: Step 3: SDA Flow

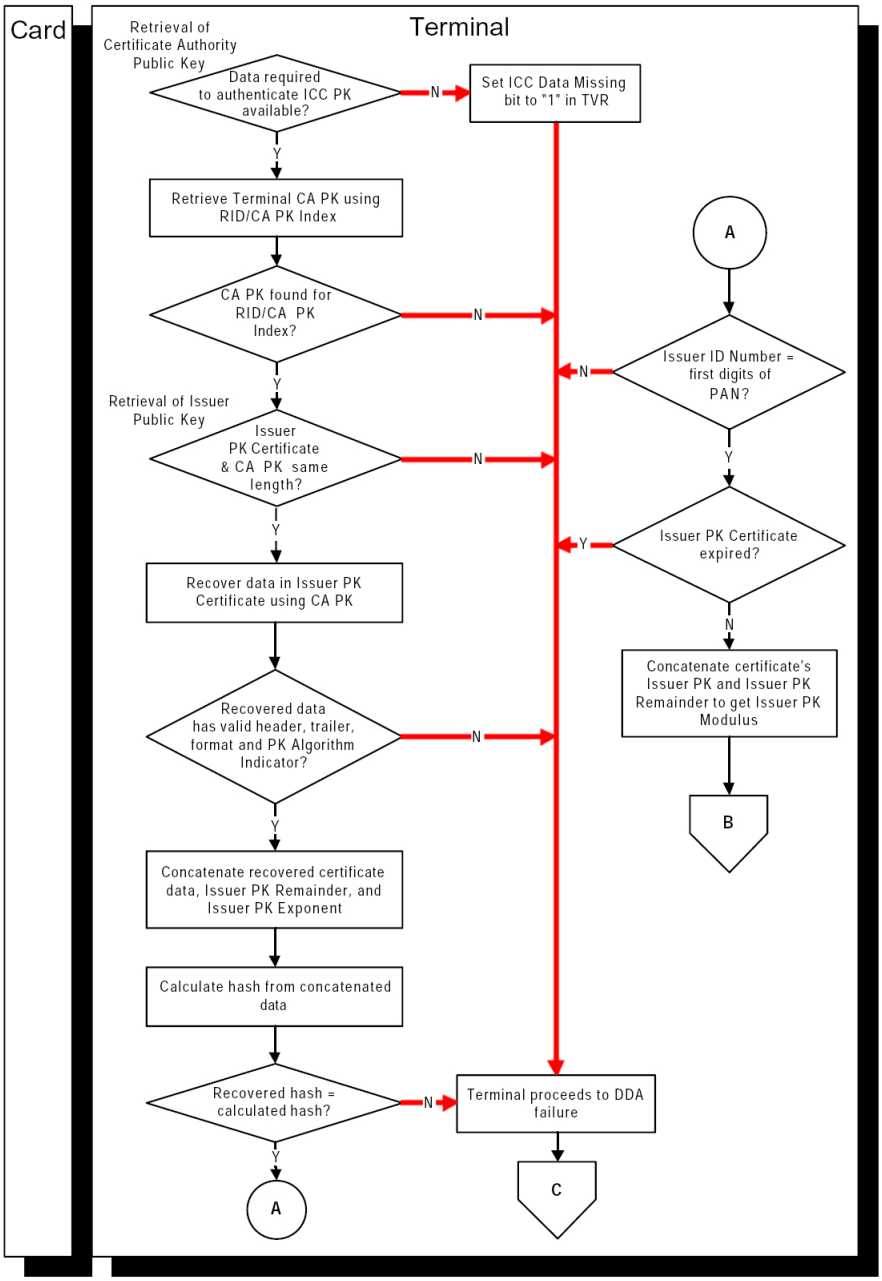


Figure E.8: Step 3: DDA Flow (1 of 3)

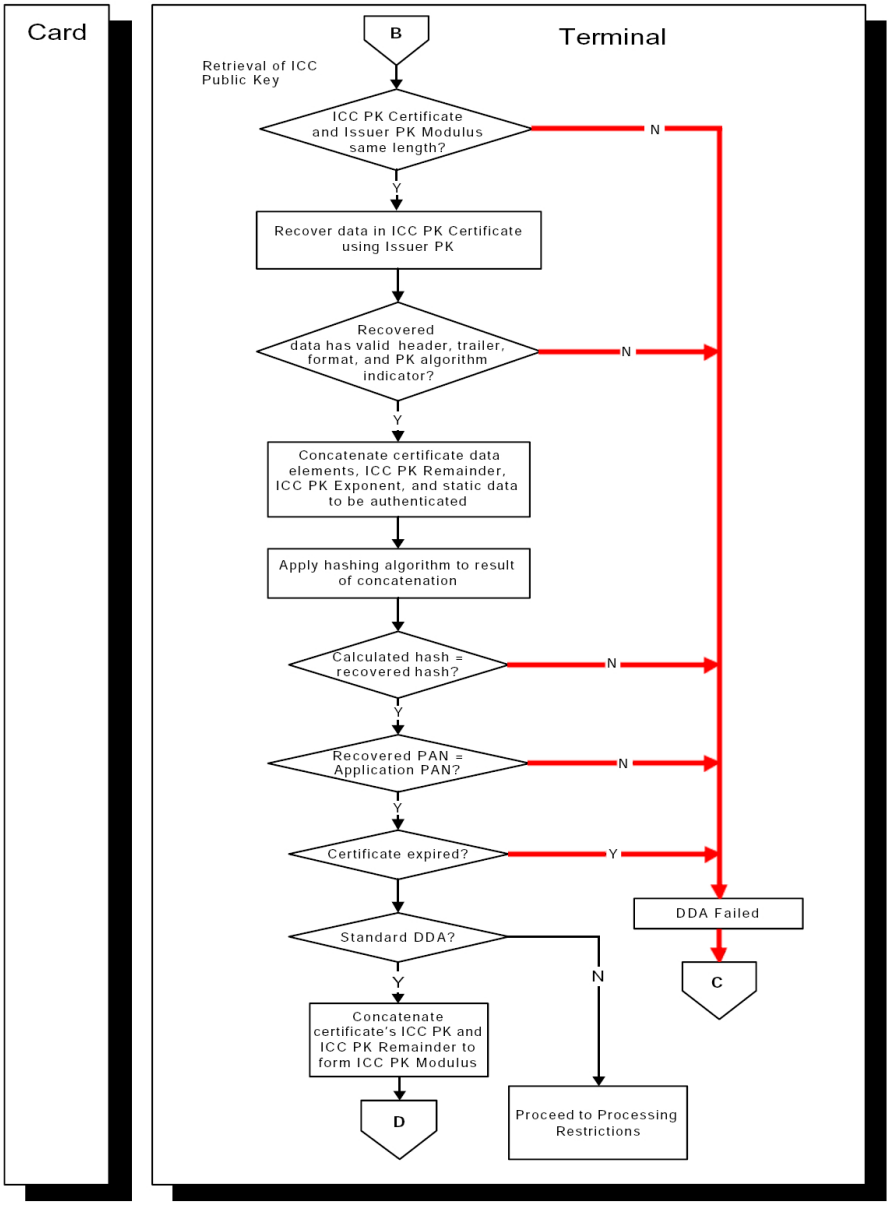


Figure E.9: Step 3: DDA Flow (2 of 3)

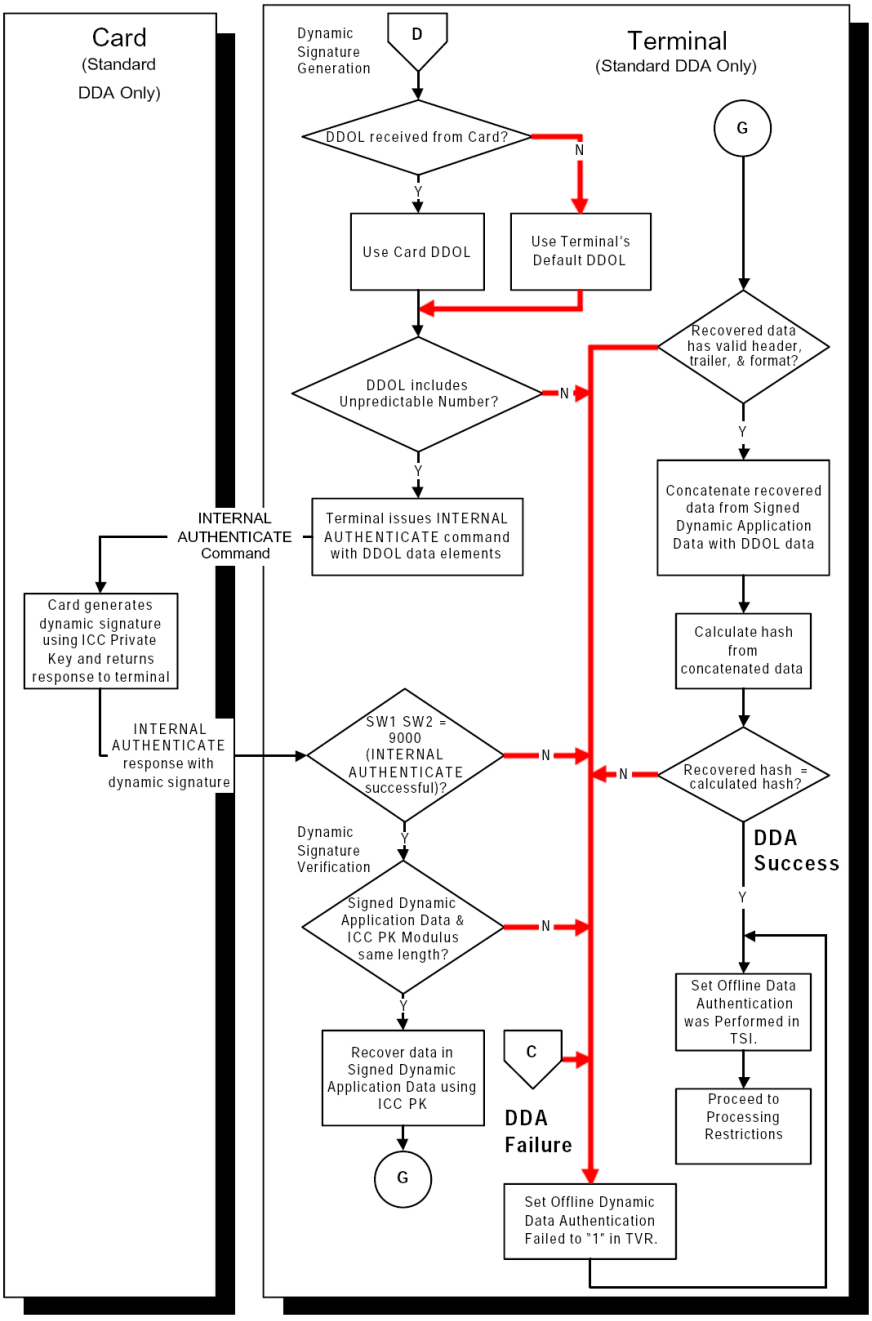


Figure E.10: Step 3: DDA Flow (3 of 3)

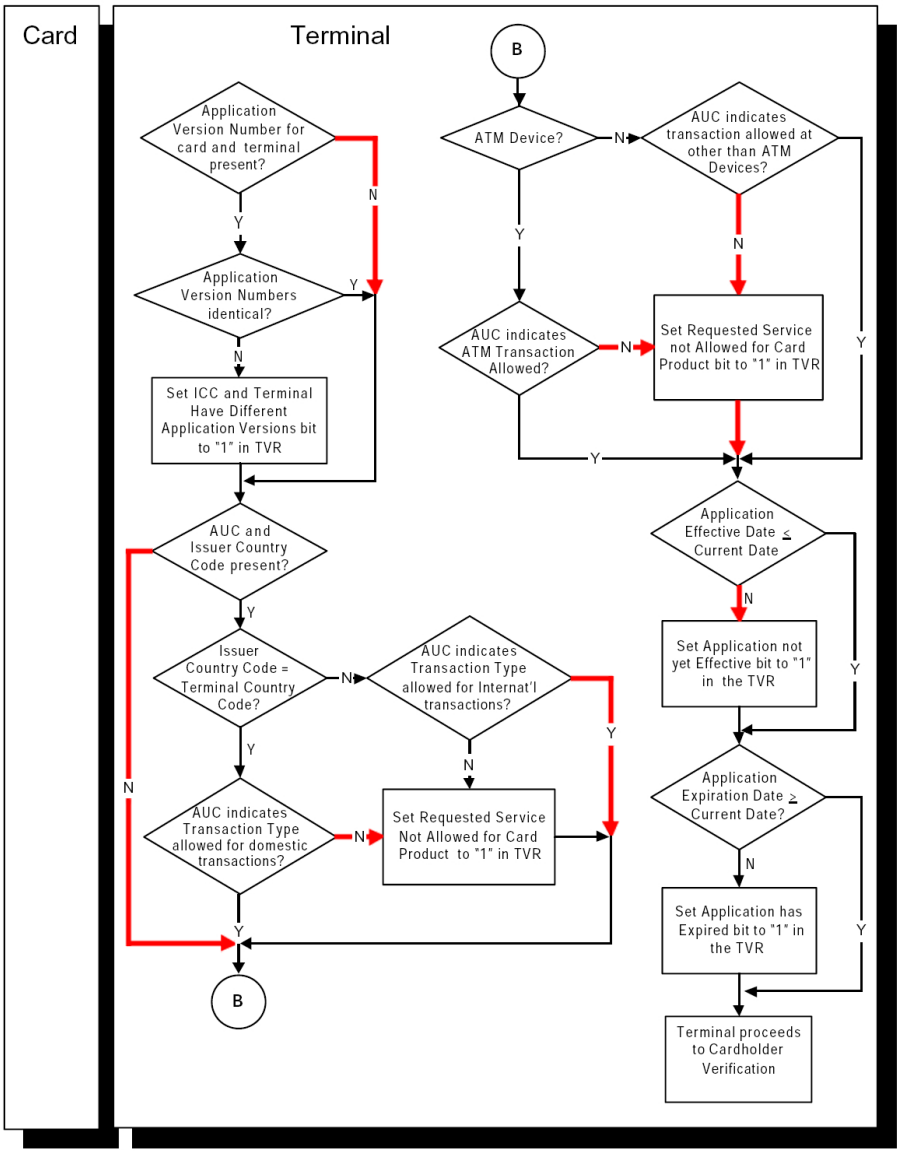


Figure E.11: Step 4: Processing Restrictions Flow

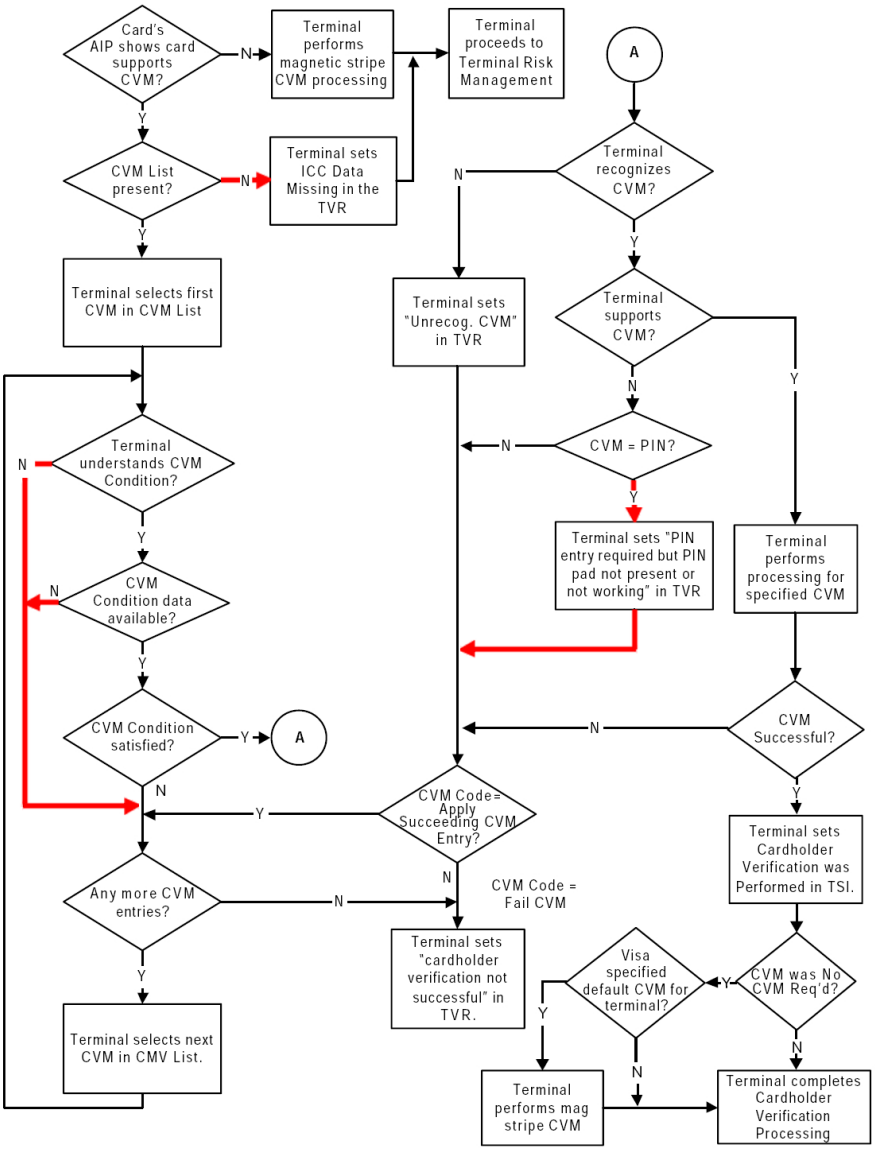


Figure E.12: Step 5: CVM List Processing Flow

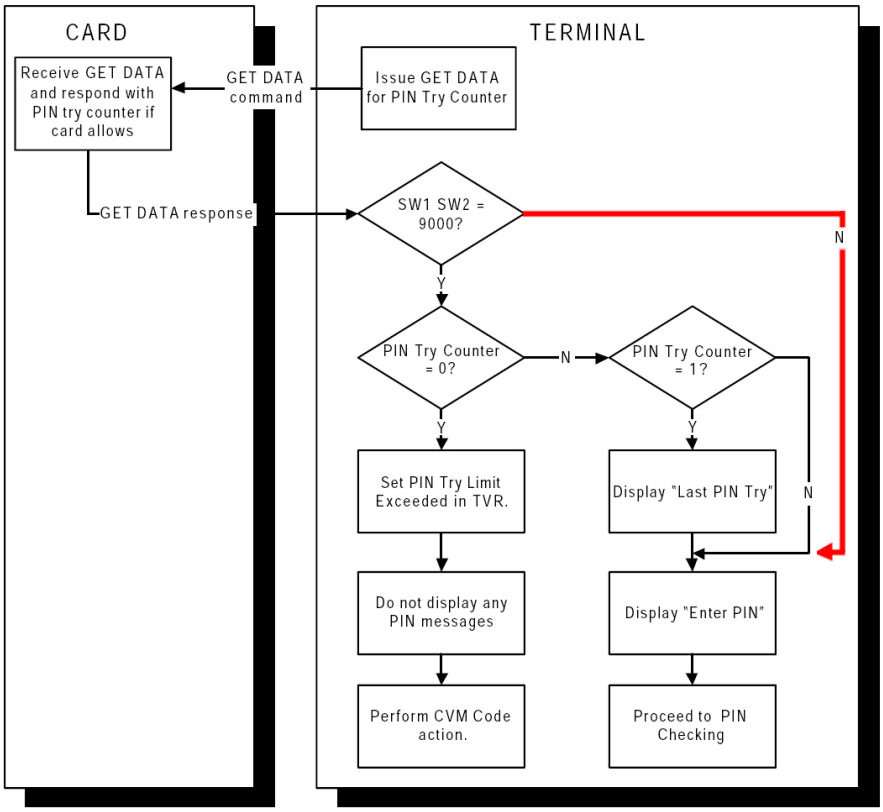


Figure E.13: Step 5: PIN Try Counter Checking Flow

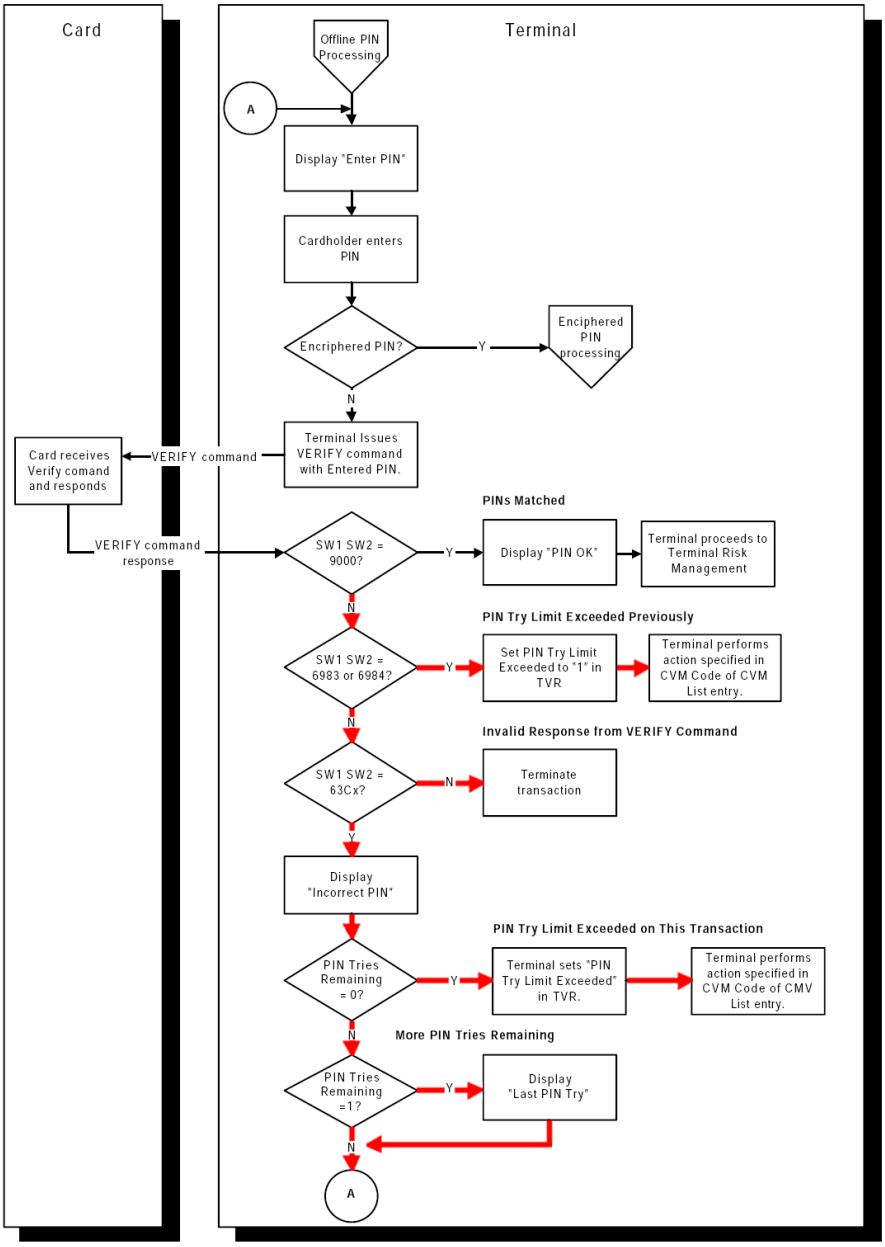


Figure E.14: Step 5: Offline PIN Processing Flow

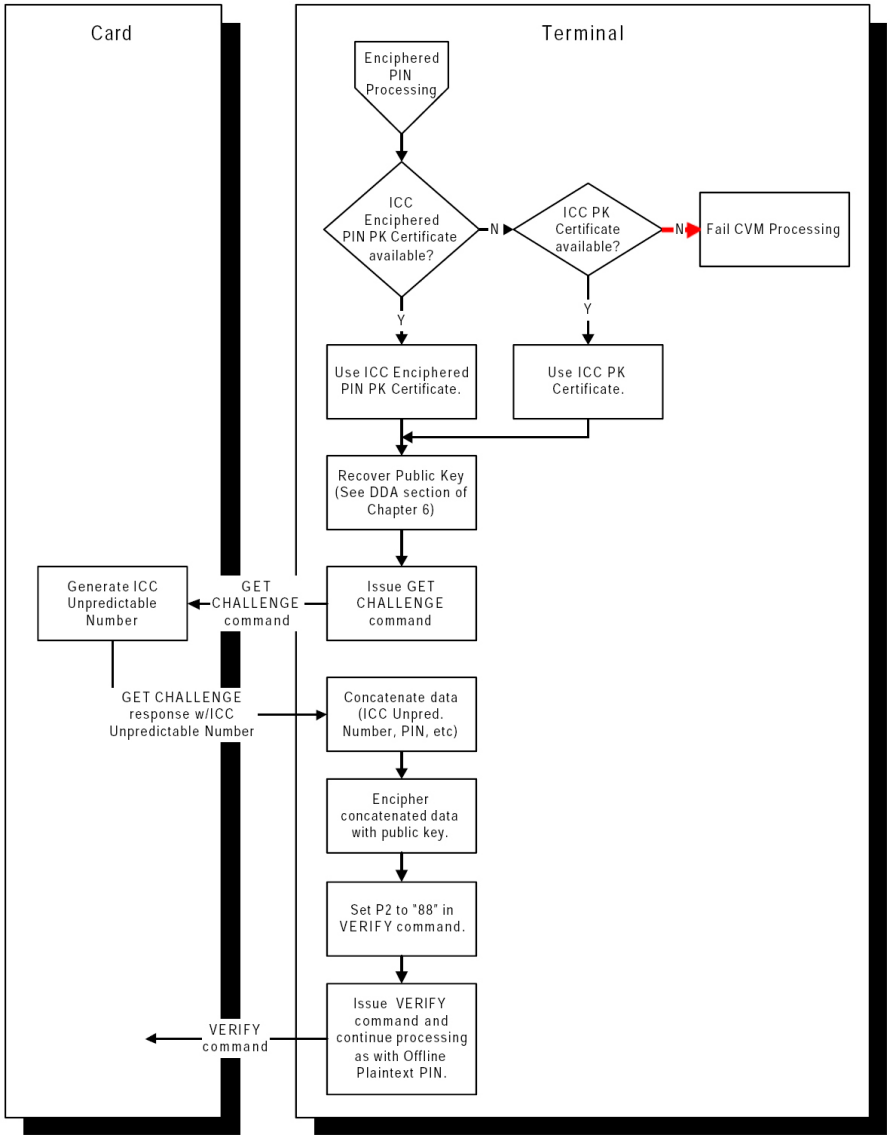


Figure E.15: Step 5: Offline Enciphered PIN Processing Flow

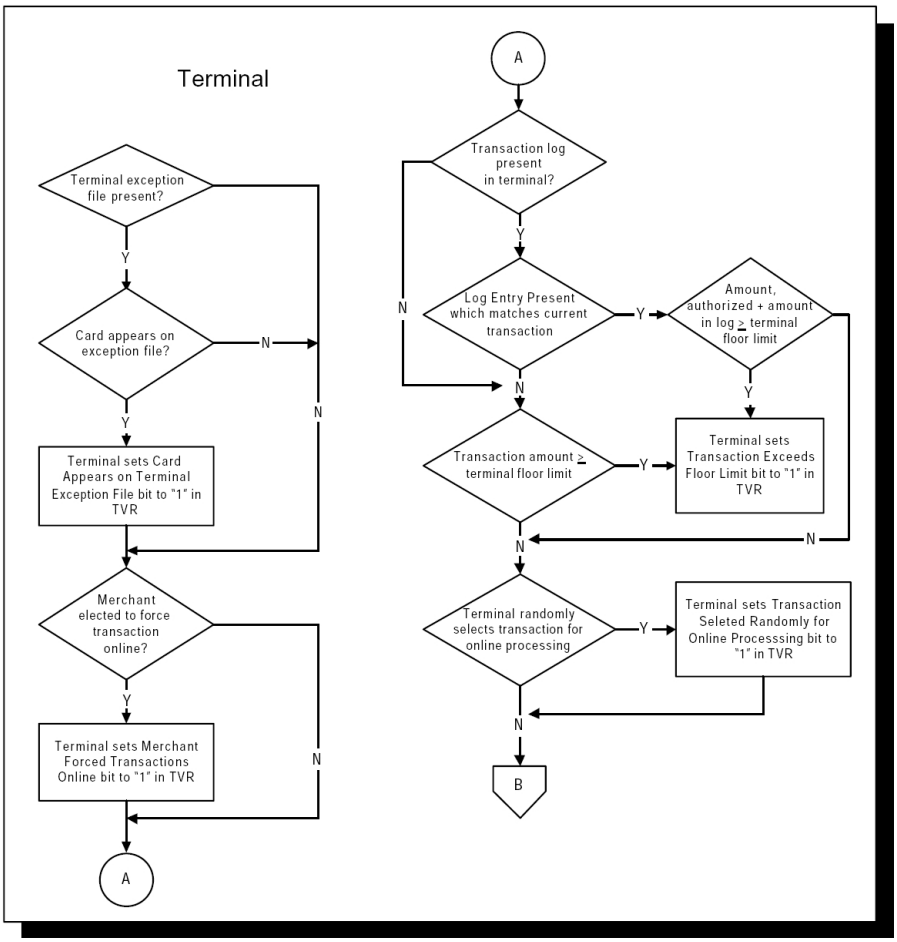


Figure E.16: Step 6: Terminal Risk Management Processing Flow (1 of 2)

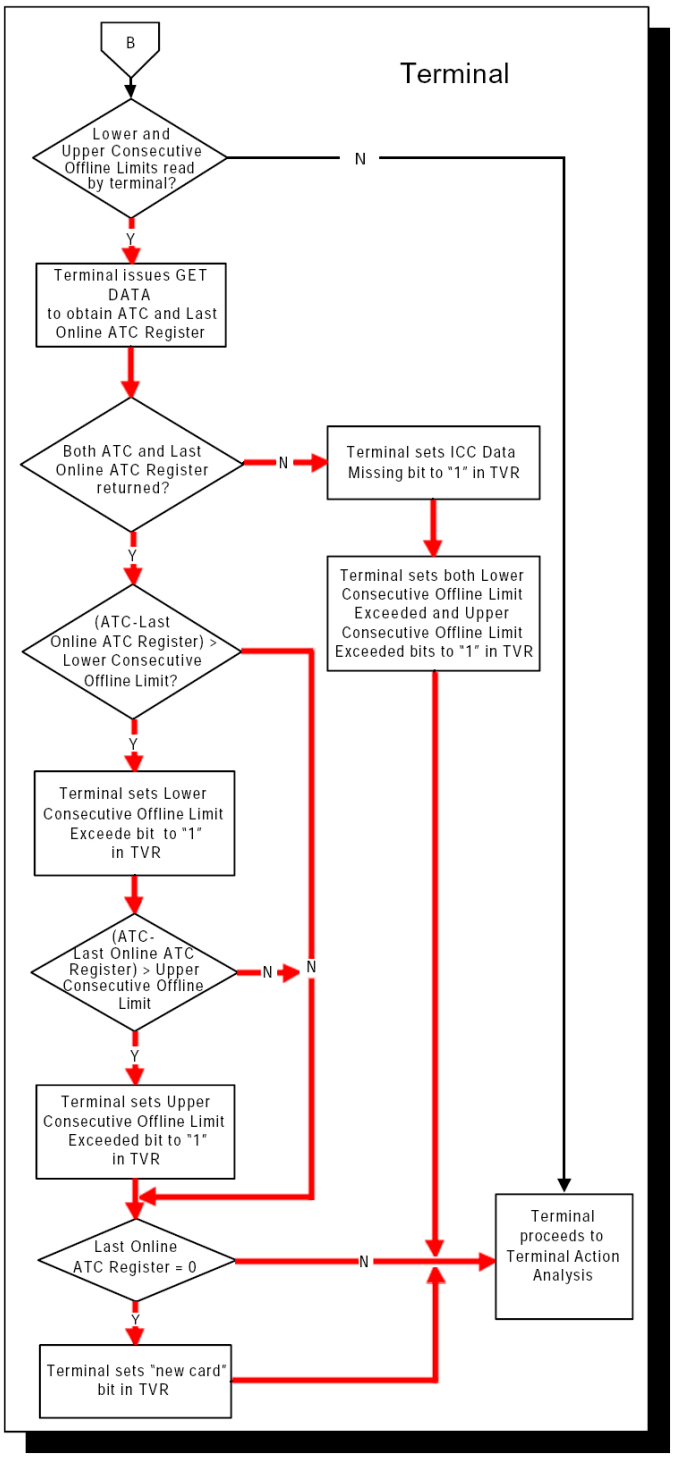


Figure E.17: Step 6: Terminal Risk Management Processing Flow (2 of 2)

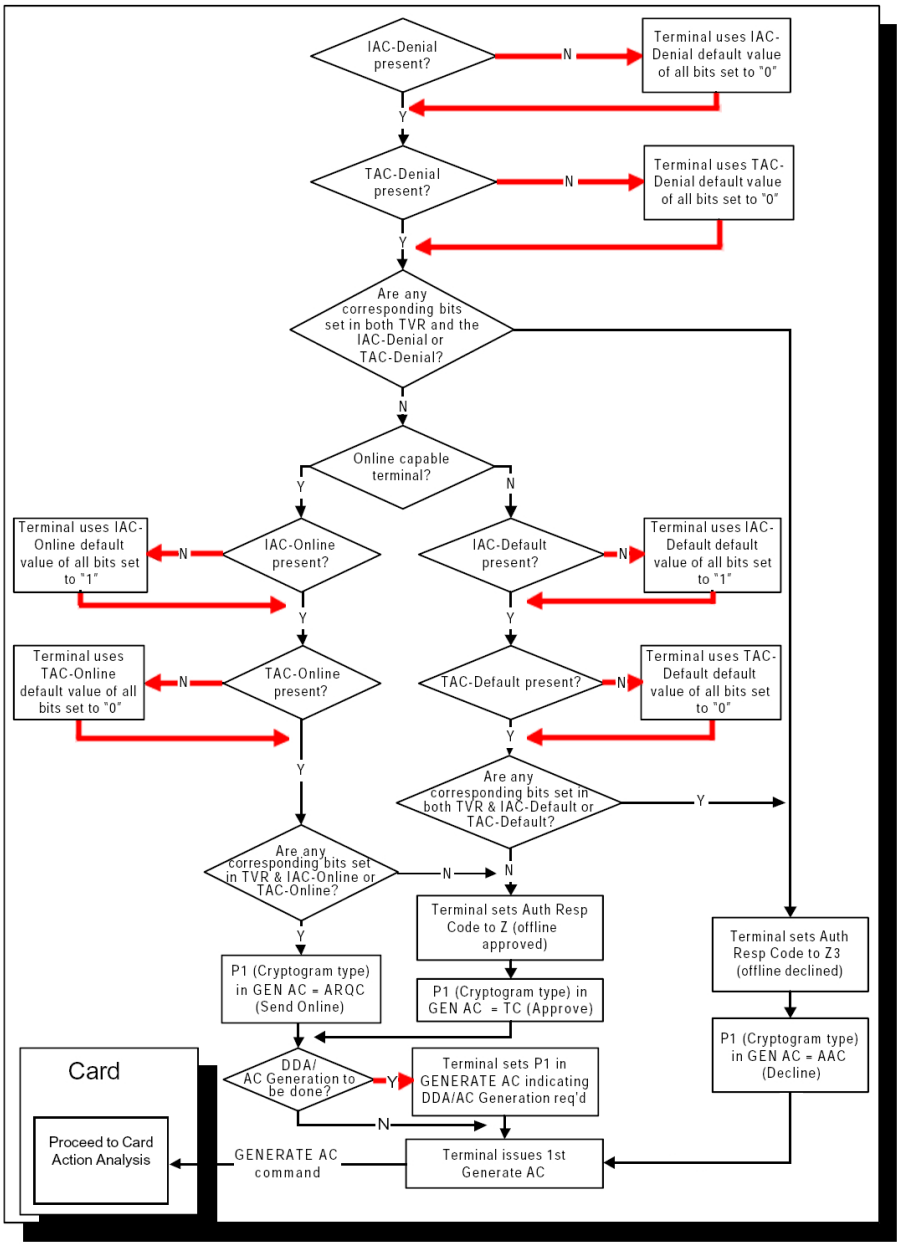


Figure E.18: Step 7: Terminal Action Analysis Flow

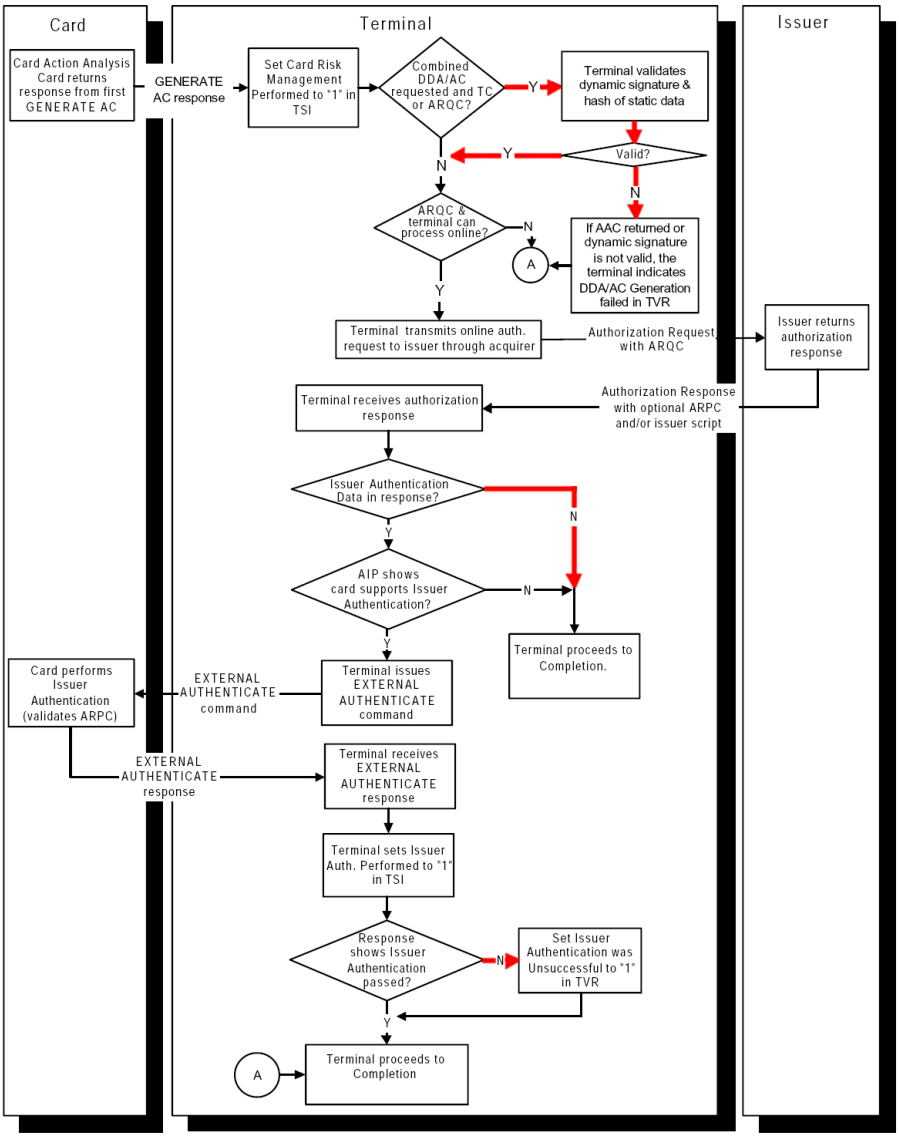


Figure E.19: Step 9: Online Processing Flow

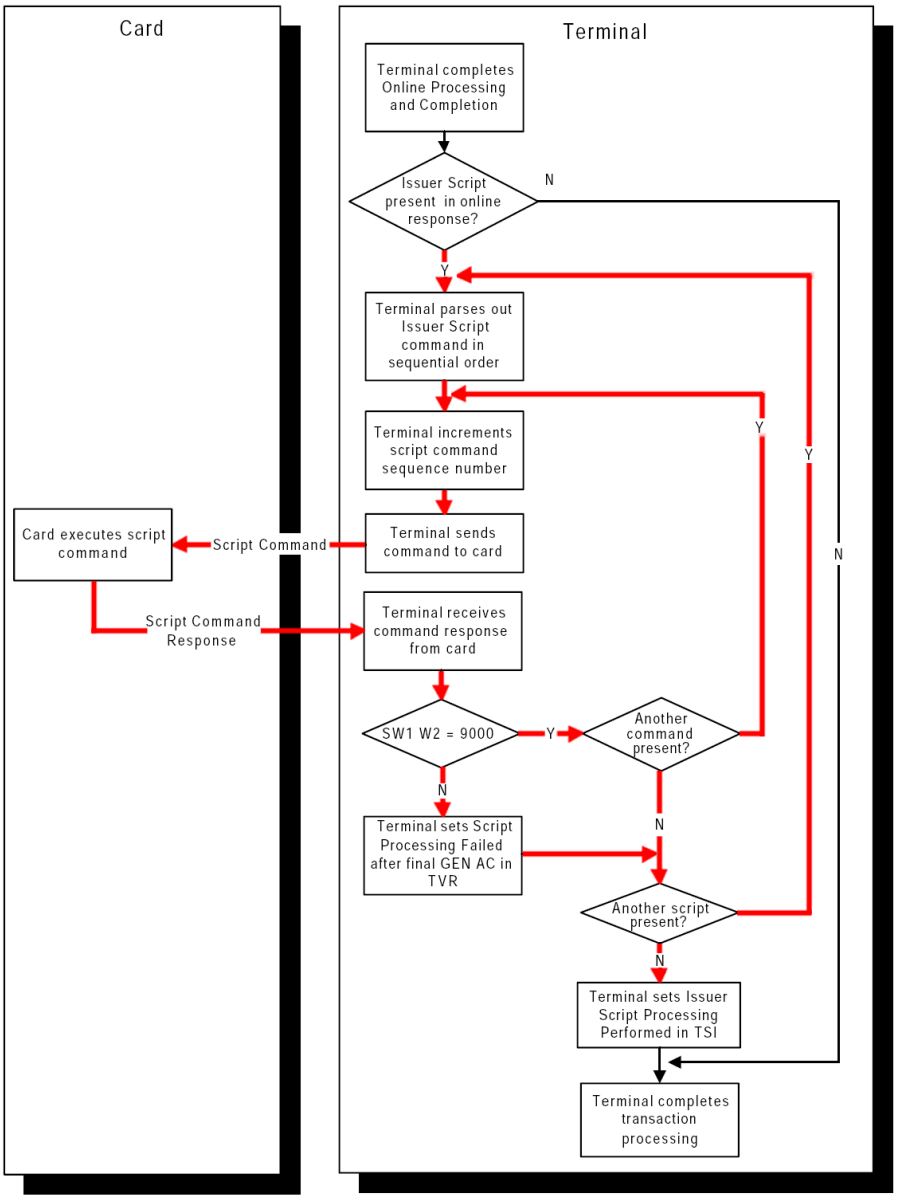


Figure E.20: Step 10: Issuer Script Processing Flow

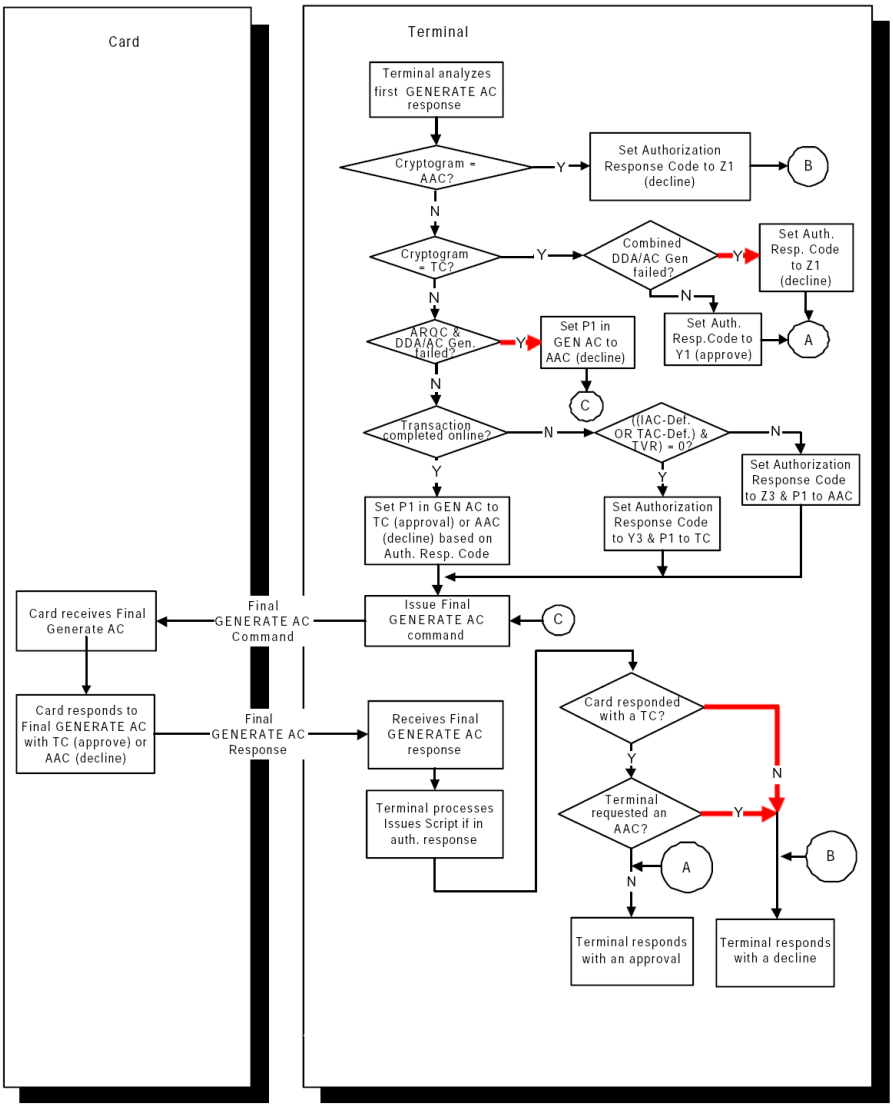


Figure E.21: Step 11: Completion Flow

Appendix F

MasterCard Transaction Flows

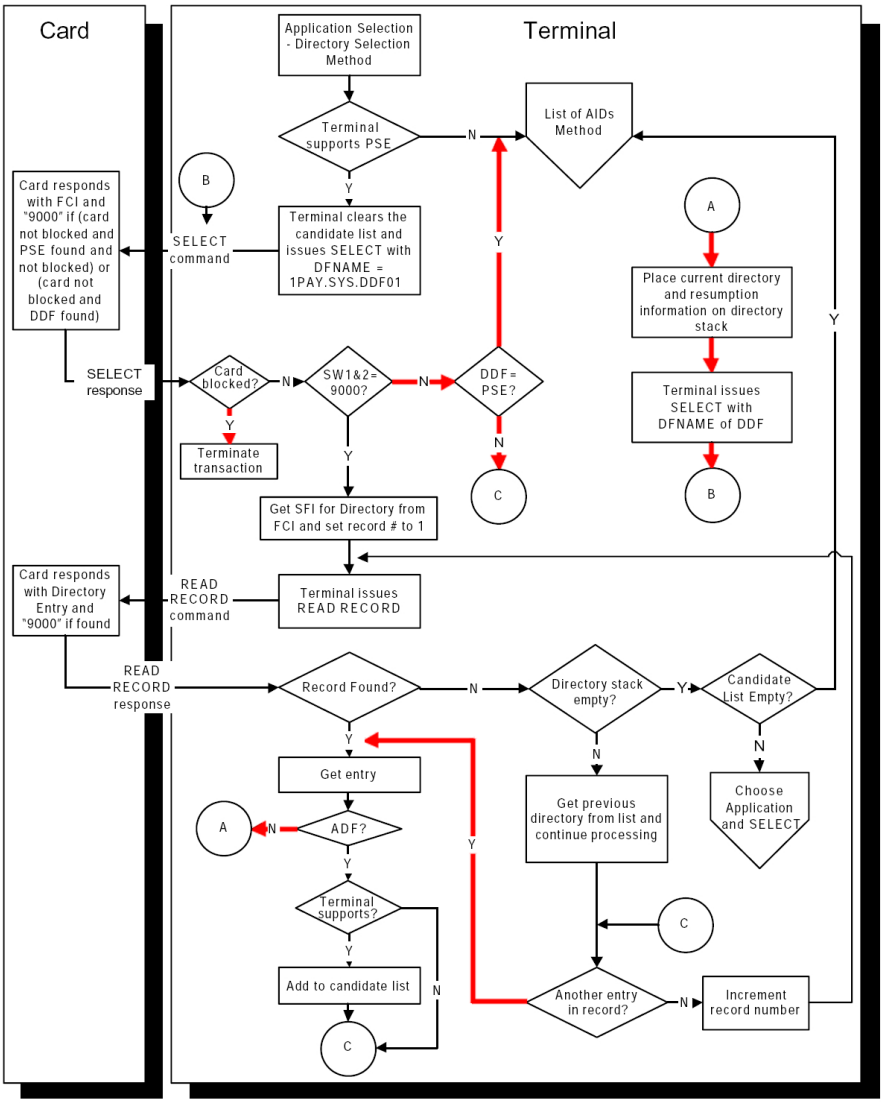


Figure F.1: Step 1: Application Selection Processing Flow (1 of 3)

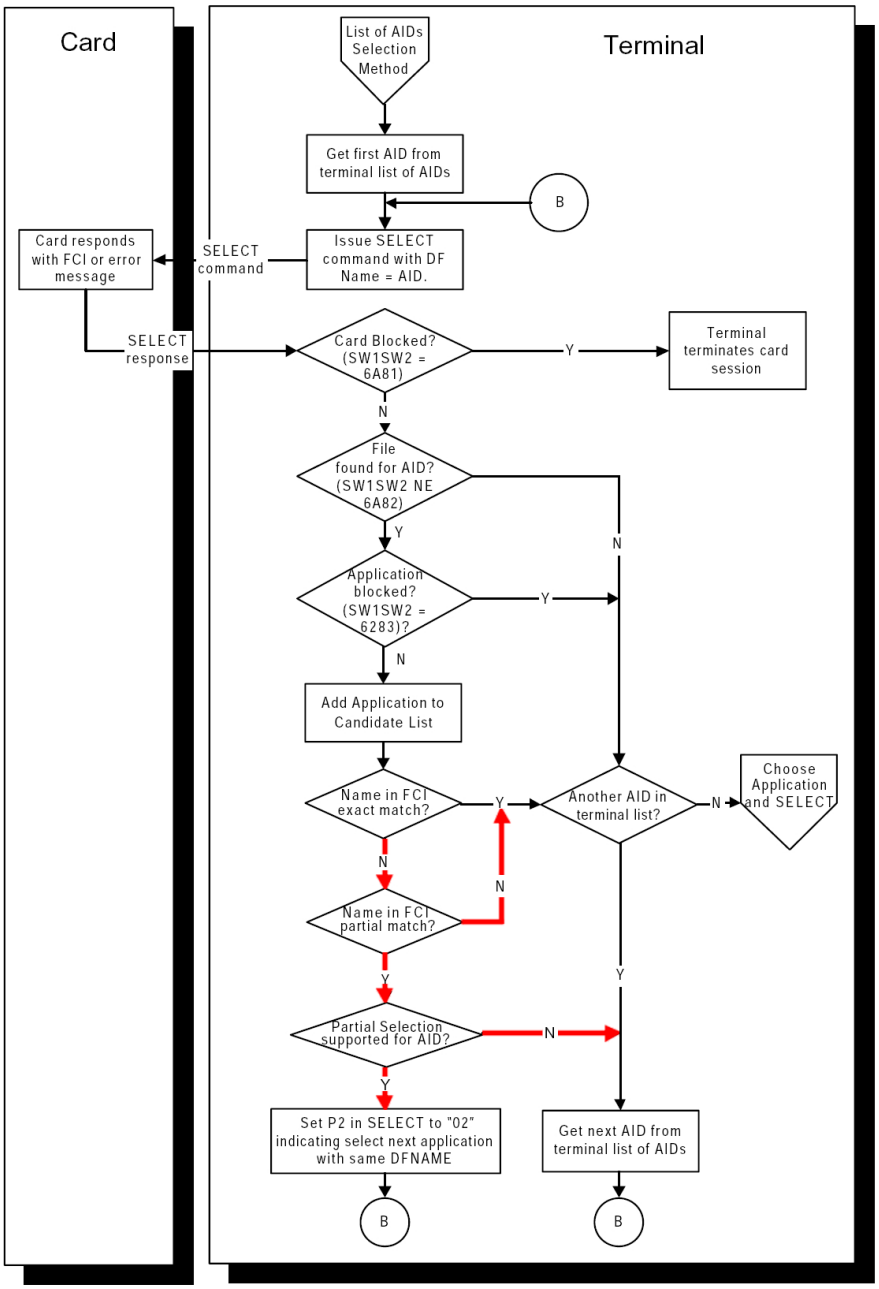


Figure F.2: Step 1: Application Selection Processing Flow (2 of 3)

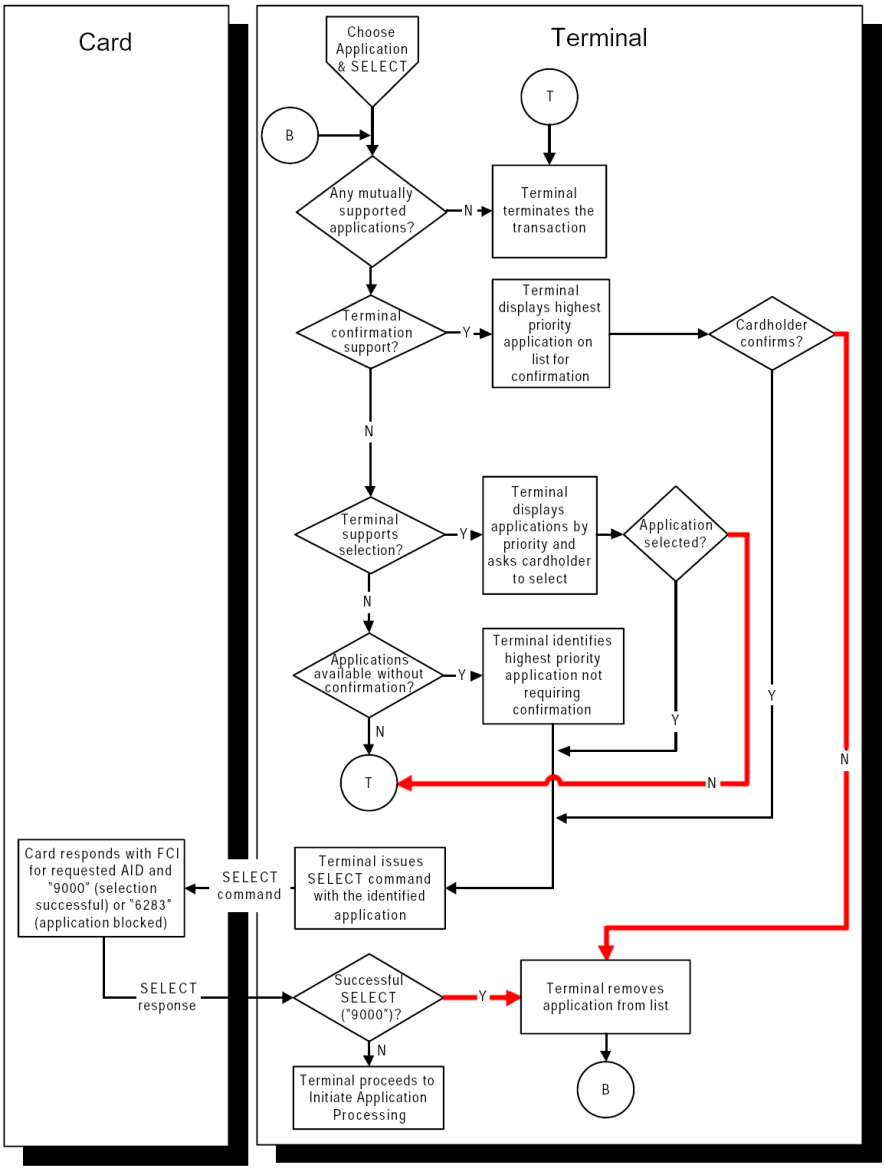


Figure F.3: Step 1: Application Selection Processing Flow (3 of 3)

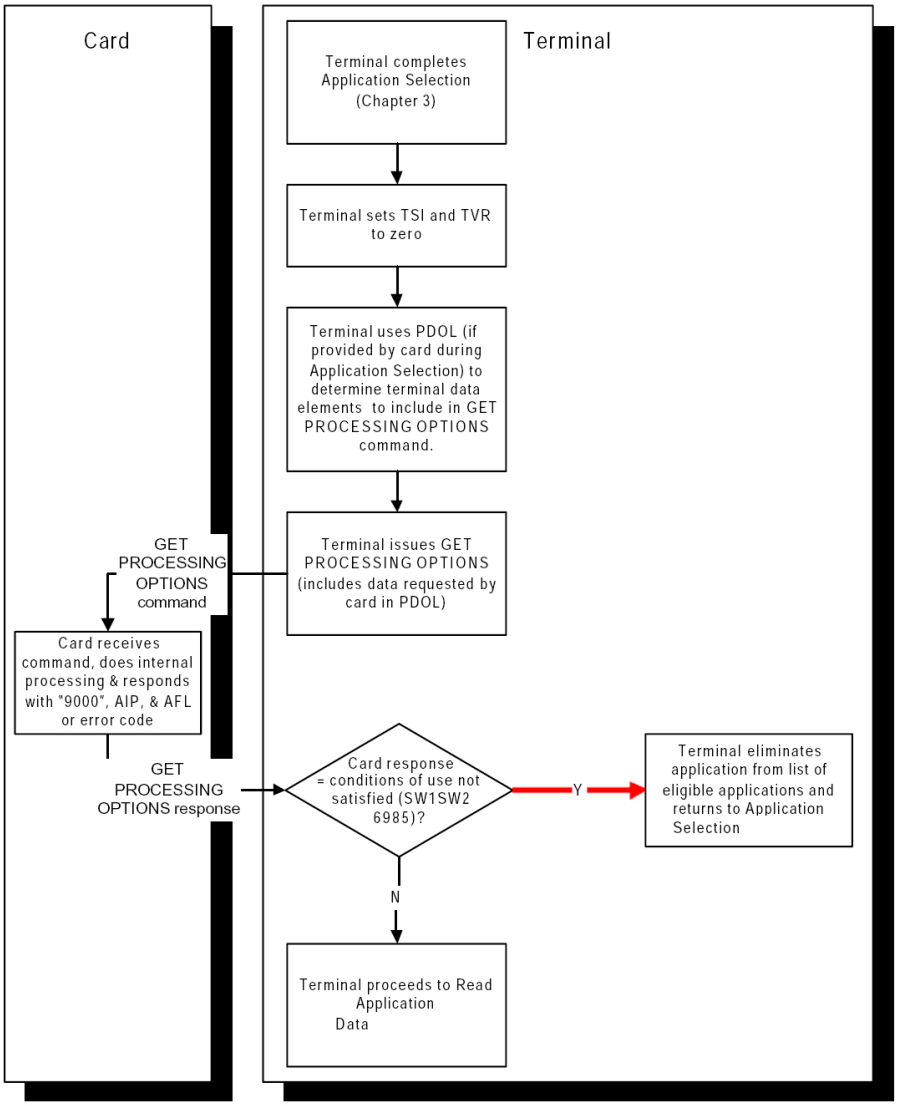


Figure F.4: Step 2: Initiate Application Processing Flow

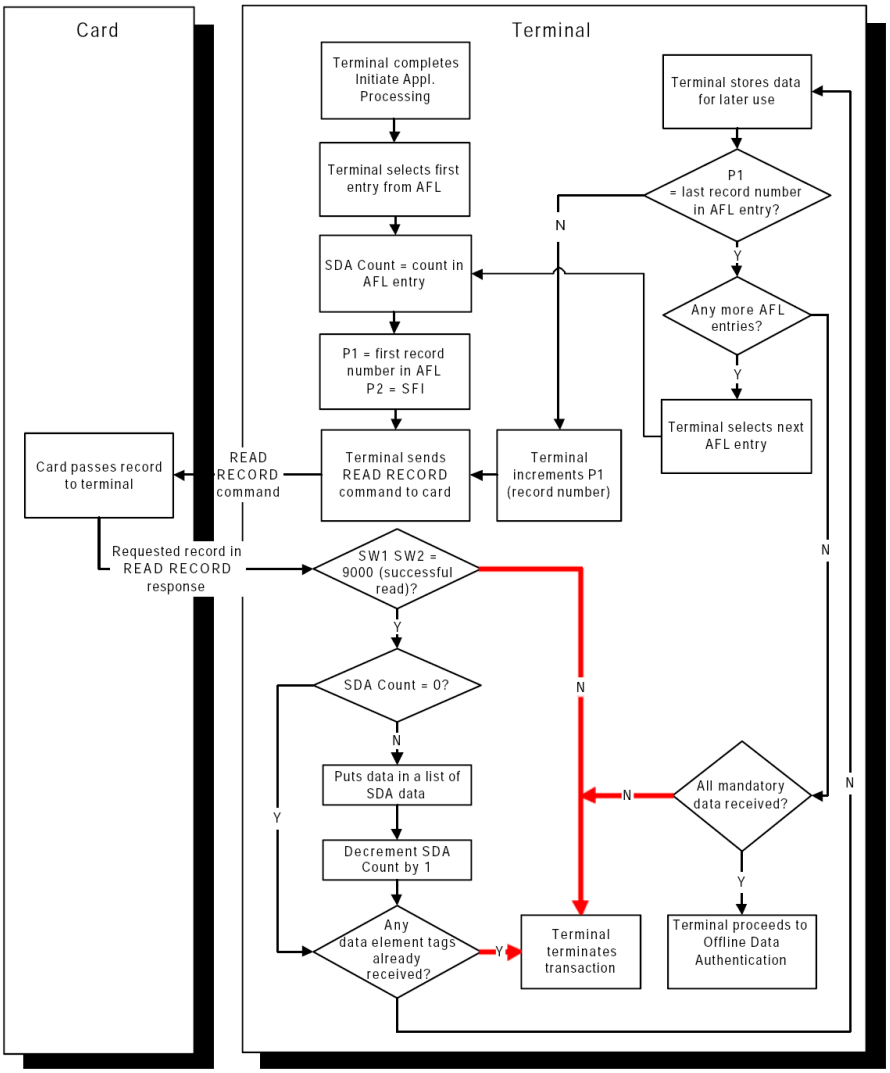


Figure F.5: Step 2: Read Application Data Processing Flow

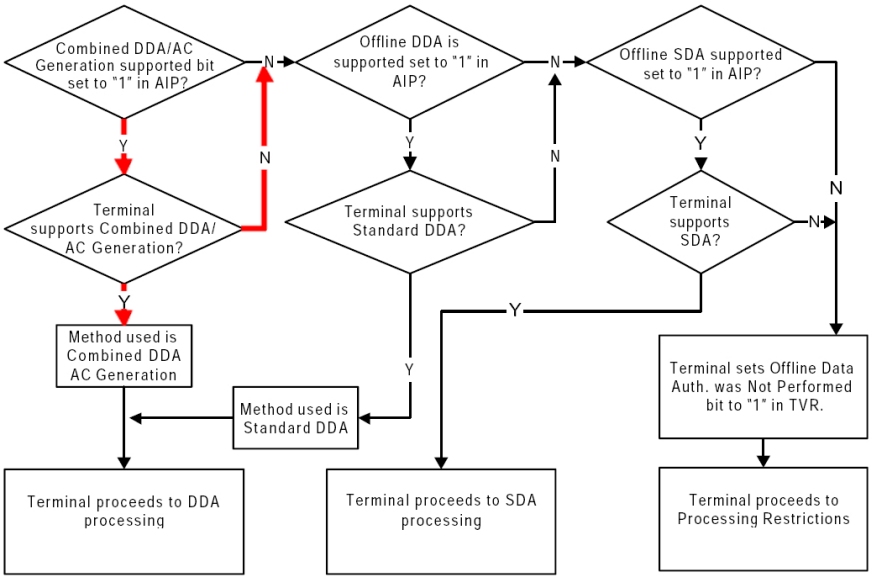


Figure F.6: Step 3: SDA or DDA Determination

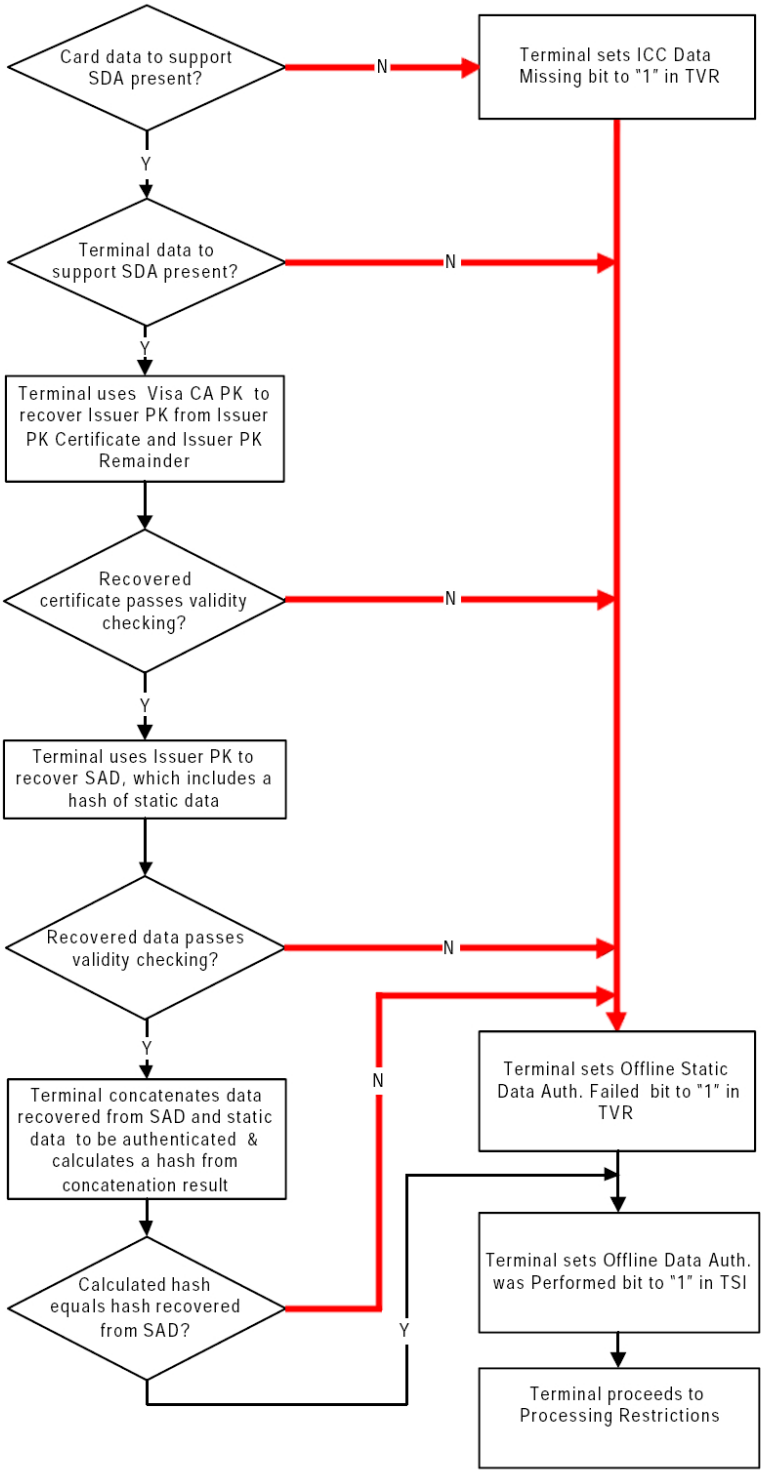


Figure F.7: Step 3: SDA Flow

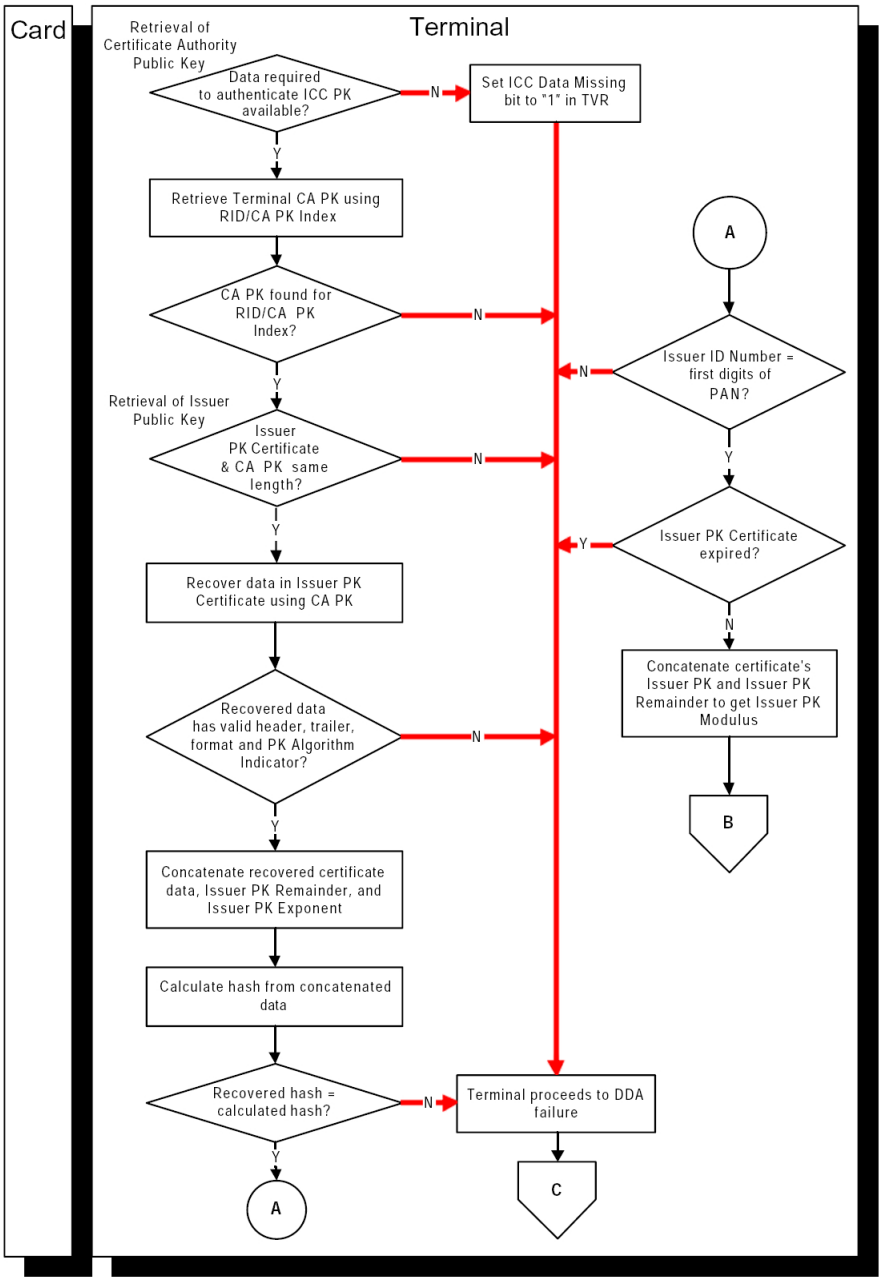


Figure F.8: Step 3: DDA Flow (1 of 3)

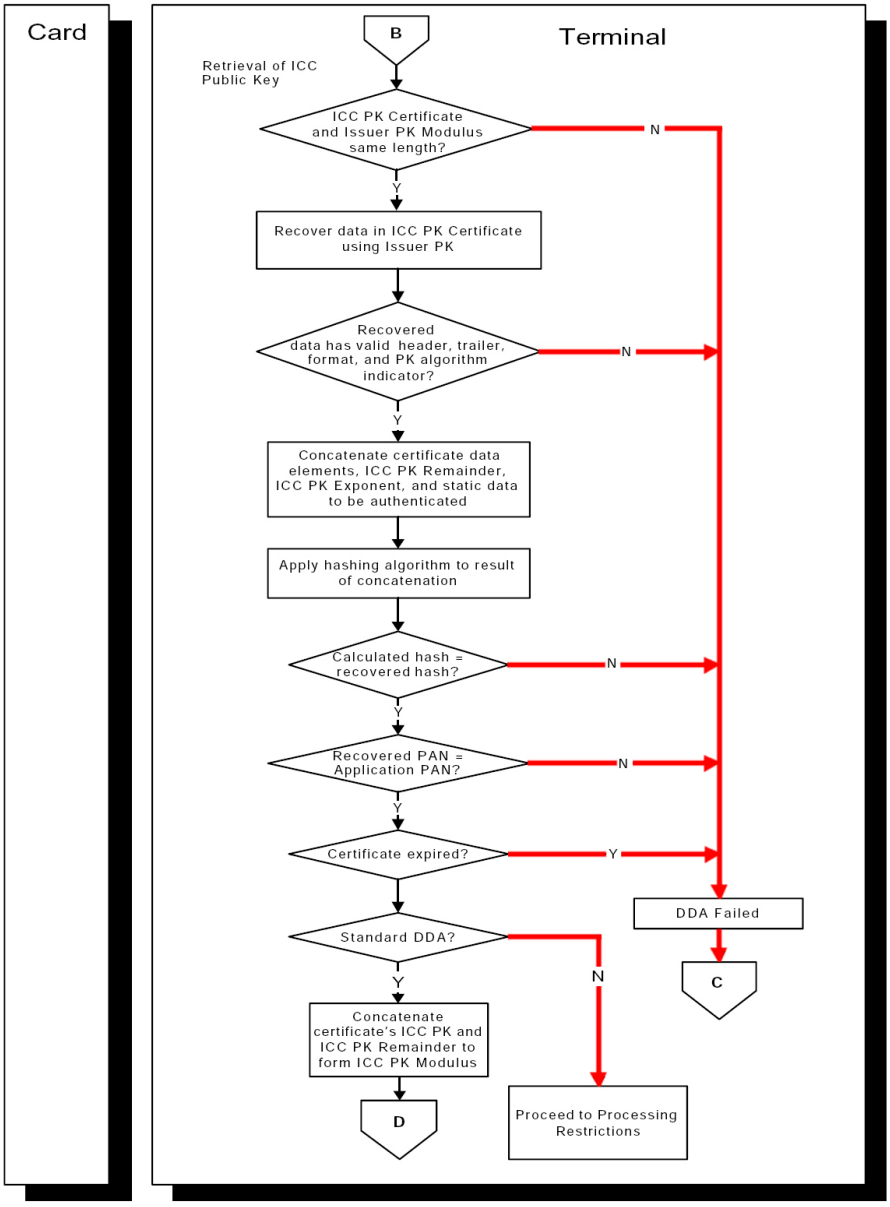


Figure F.9: Step 3: DDA Flow (2 of 3)

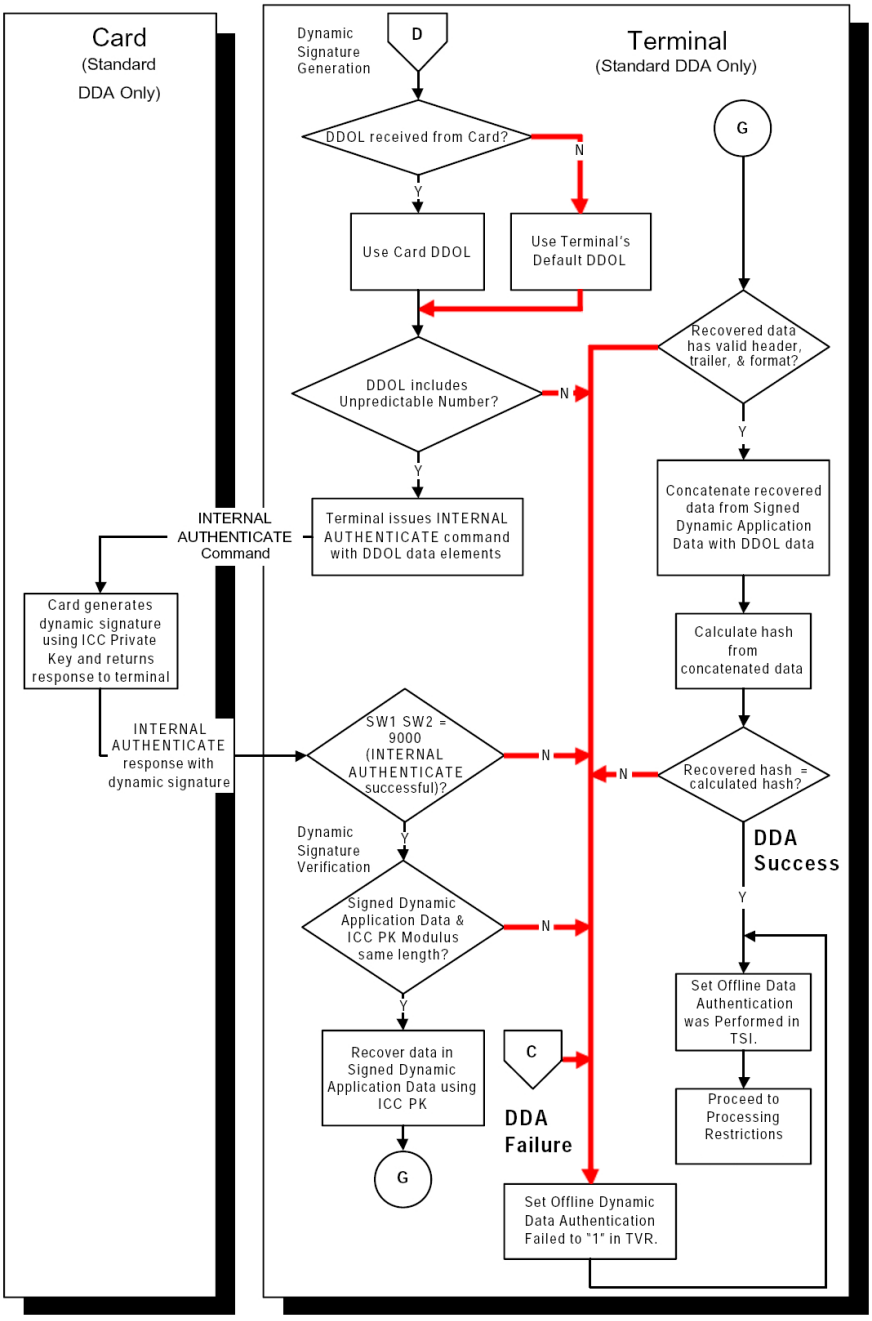


Figure F.10: Step 3: DDA Flow (3 of 3)

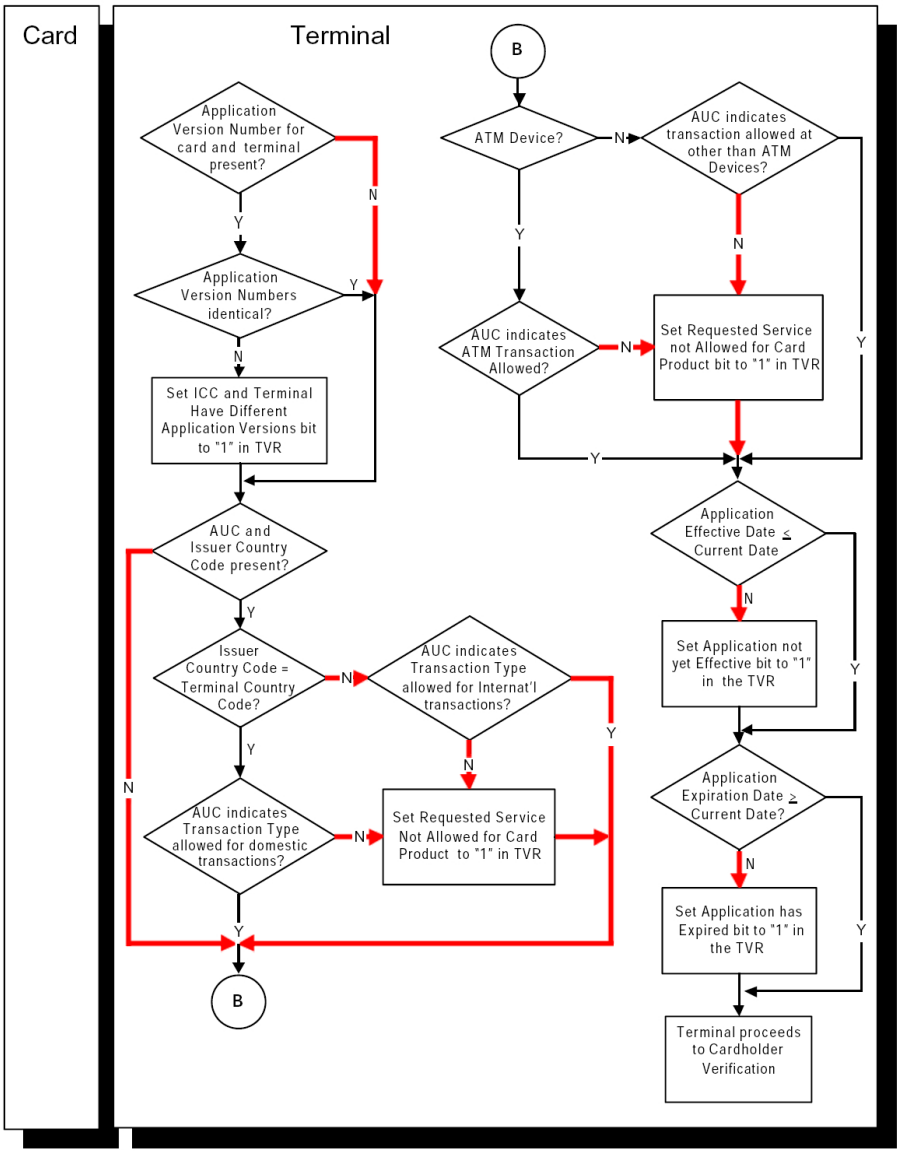


Figure F.11: Step 4: Processing Restrictions Flow

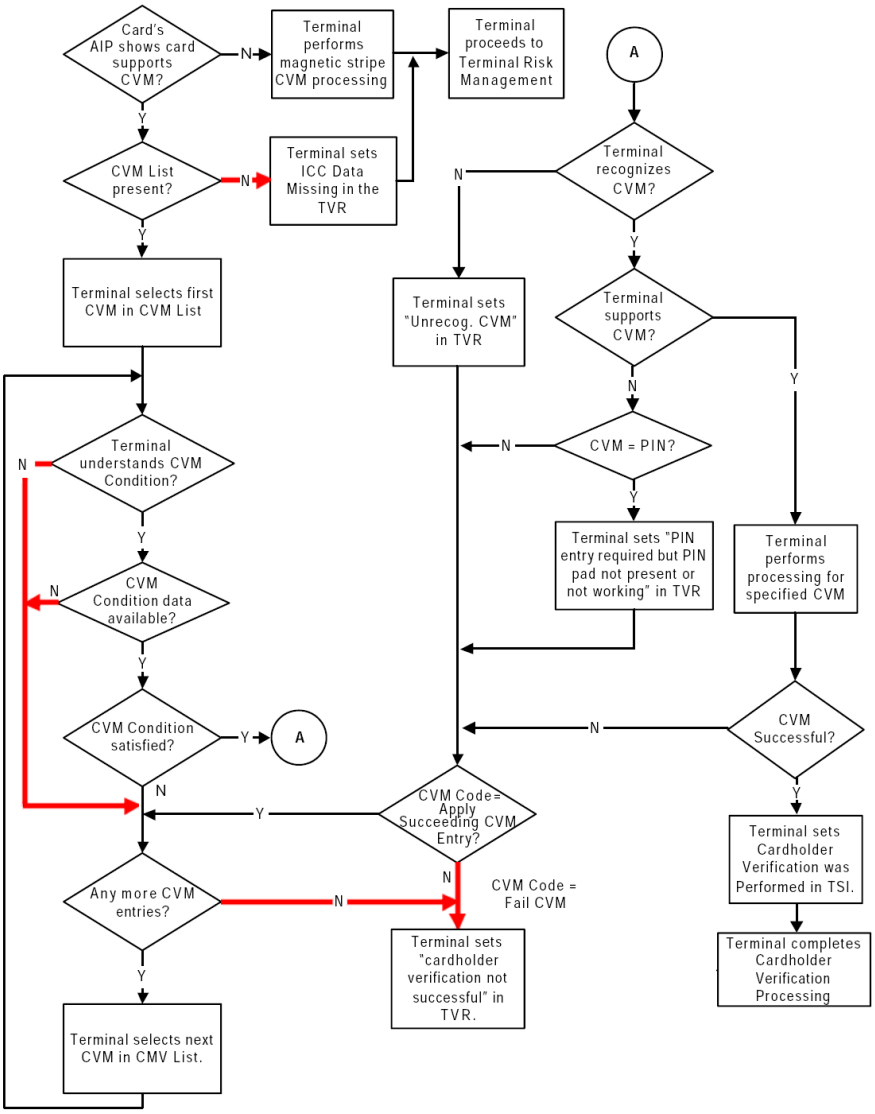


Figure F.12: Step 5: CVM List Processing Flow

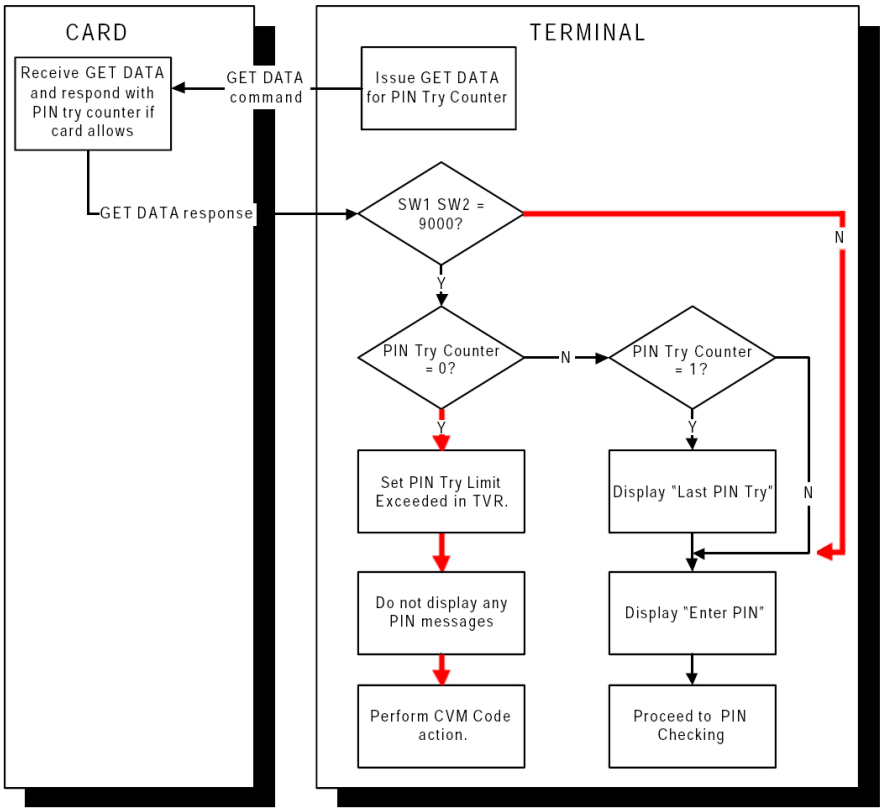


Figure F.13: Step 5: PIN Try Counter Checking Flow

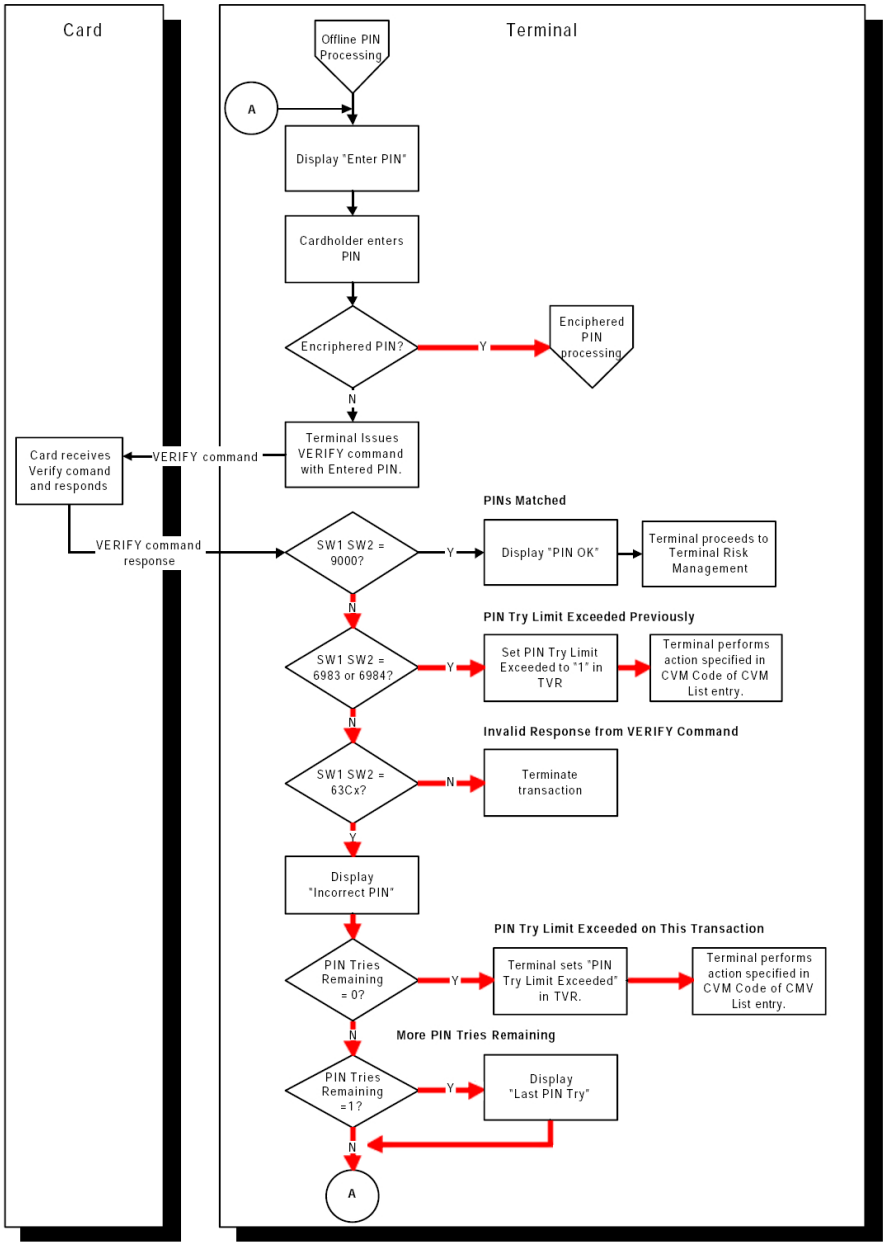


Figure F.14: Step 5: Offline PIN Processing Flow

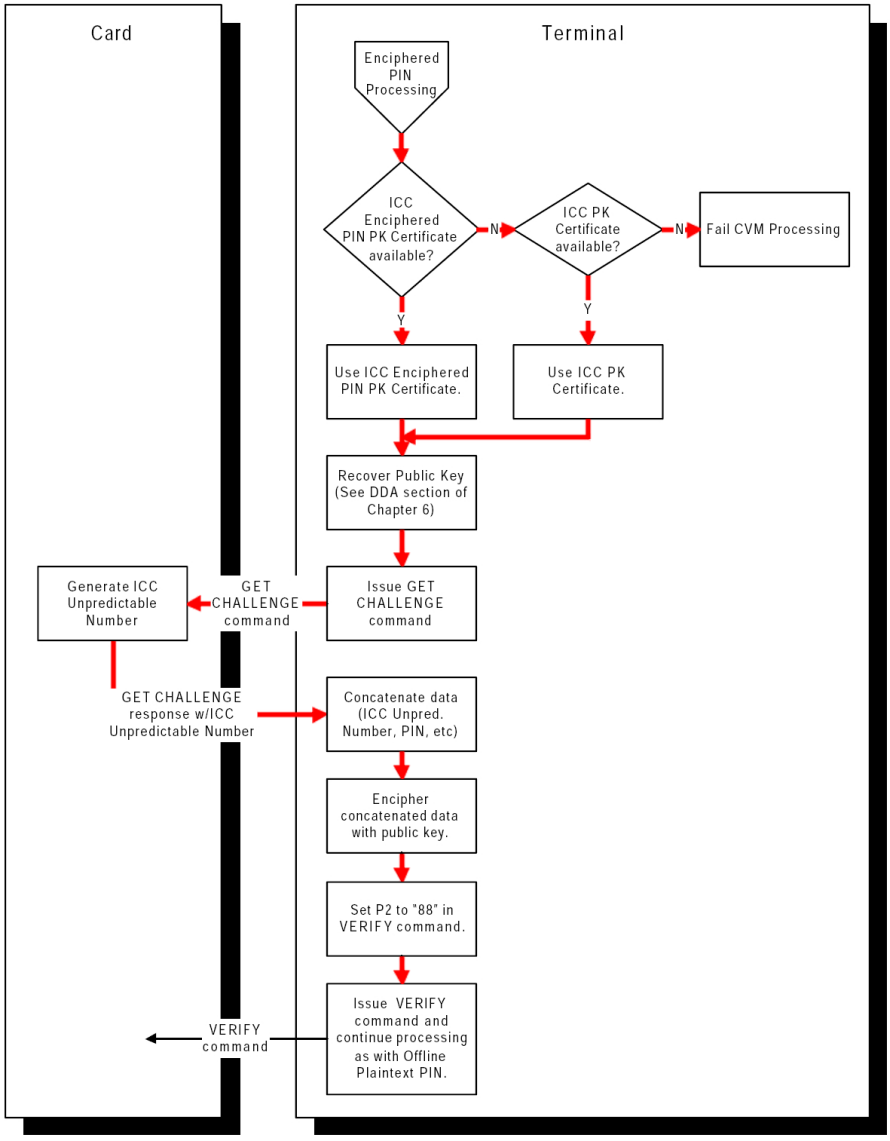


Figure F.15: Step 5: Offline Enciphered PIN Processing Flow

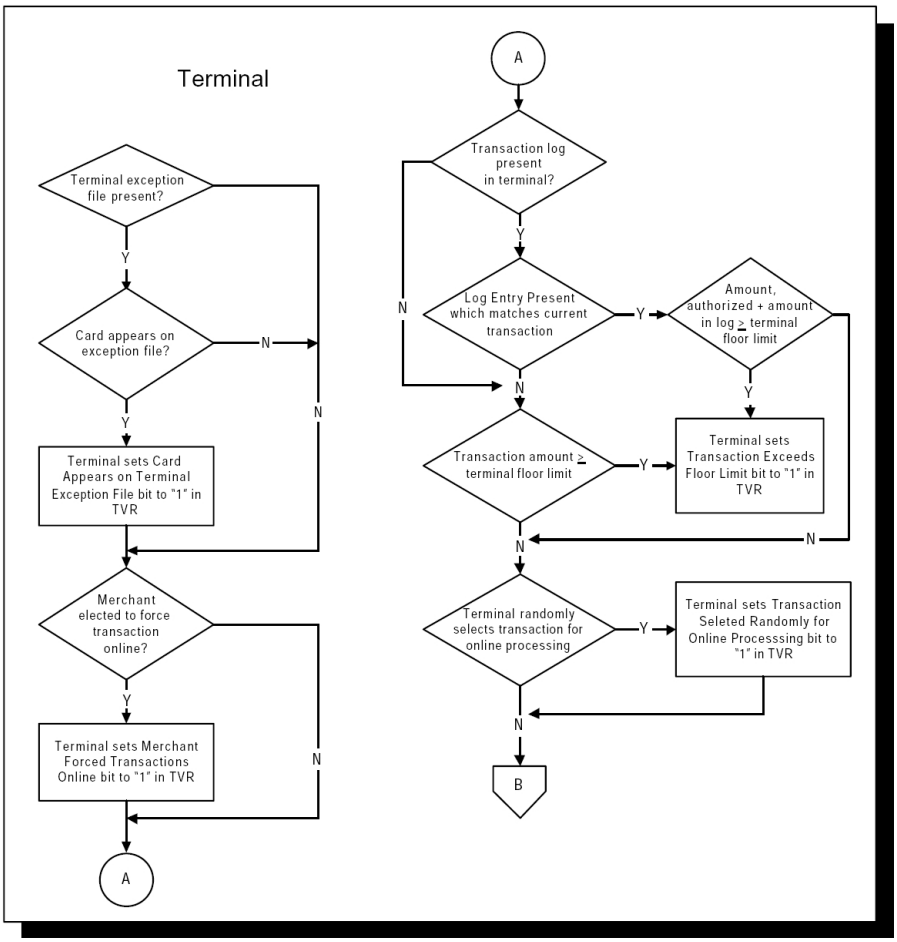


Figure F.16: Step 6: Terminal Risk Management Processing Flow (1 of 2)

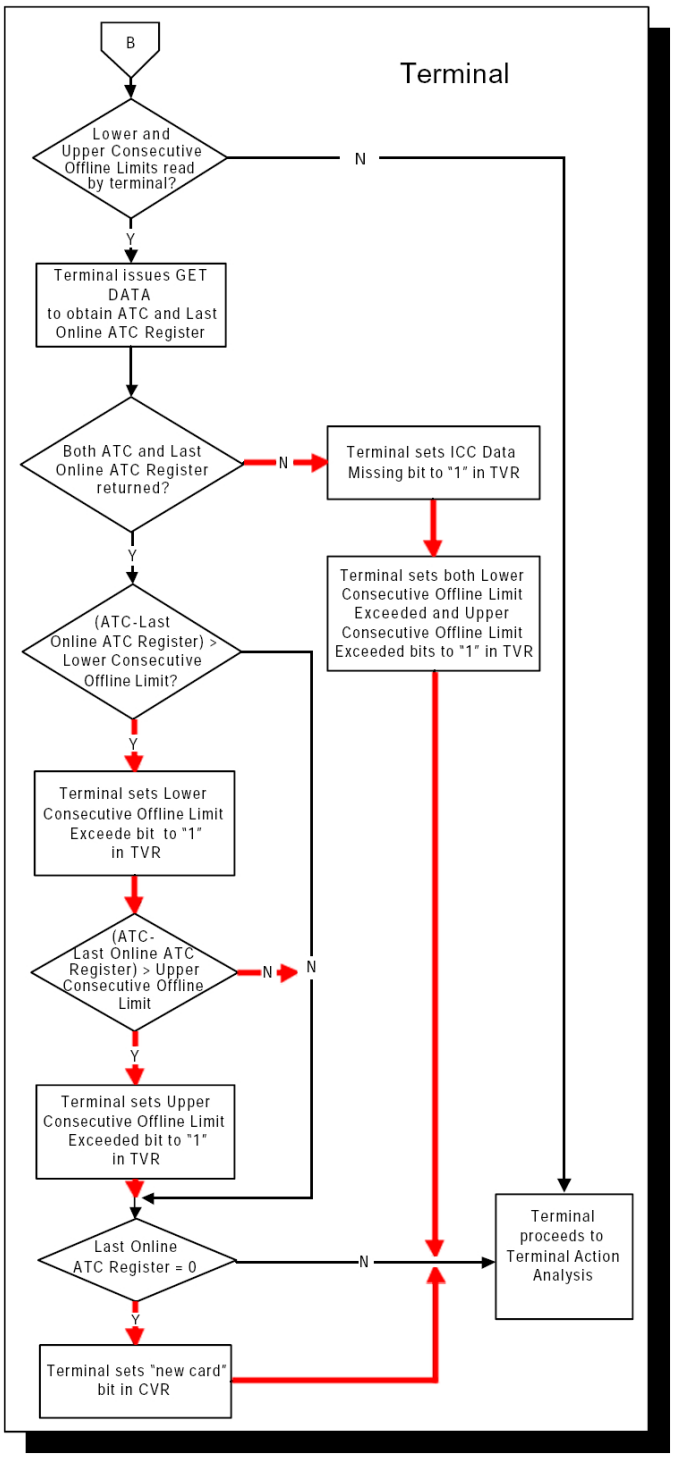


Figure F.17: Step 6: Terminal Risk Management Processing Flow (2 of 2)

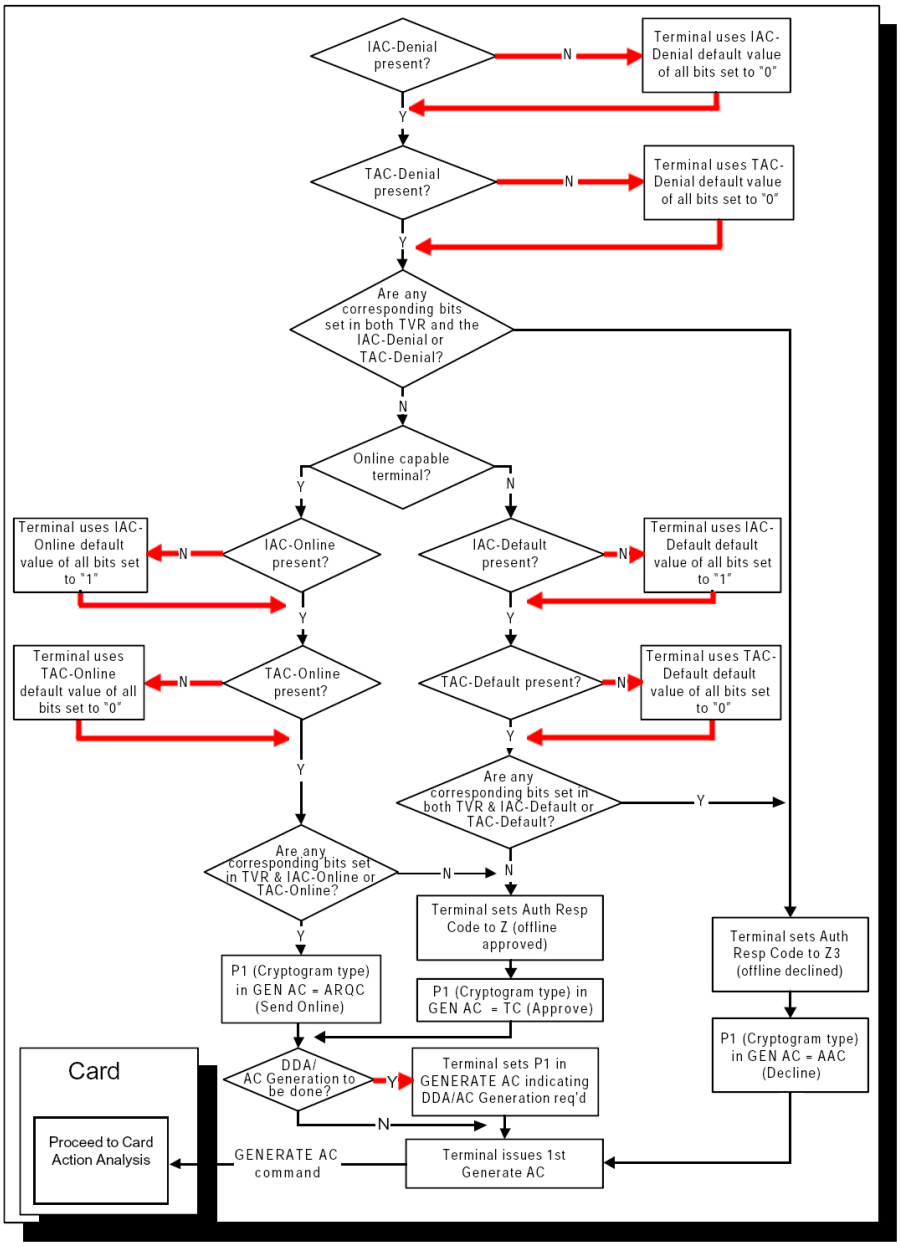


Figure F.18: Step 7: Terminal Action Analysis Flow

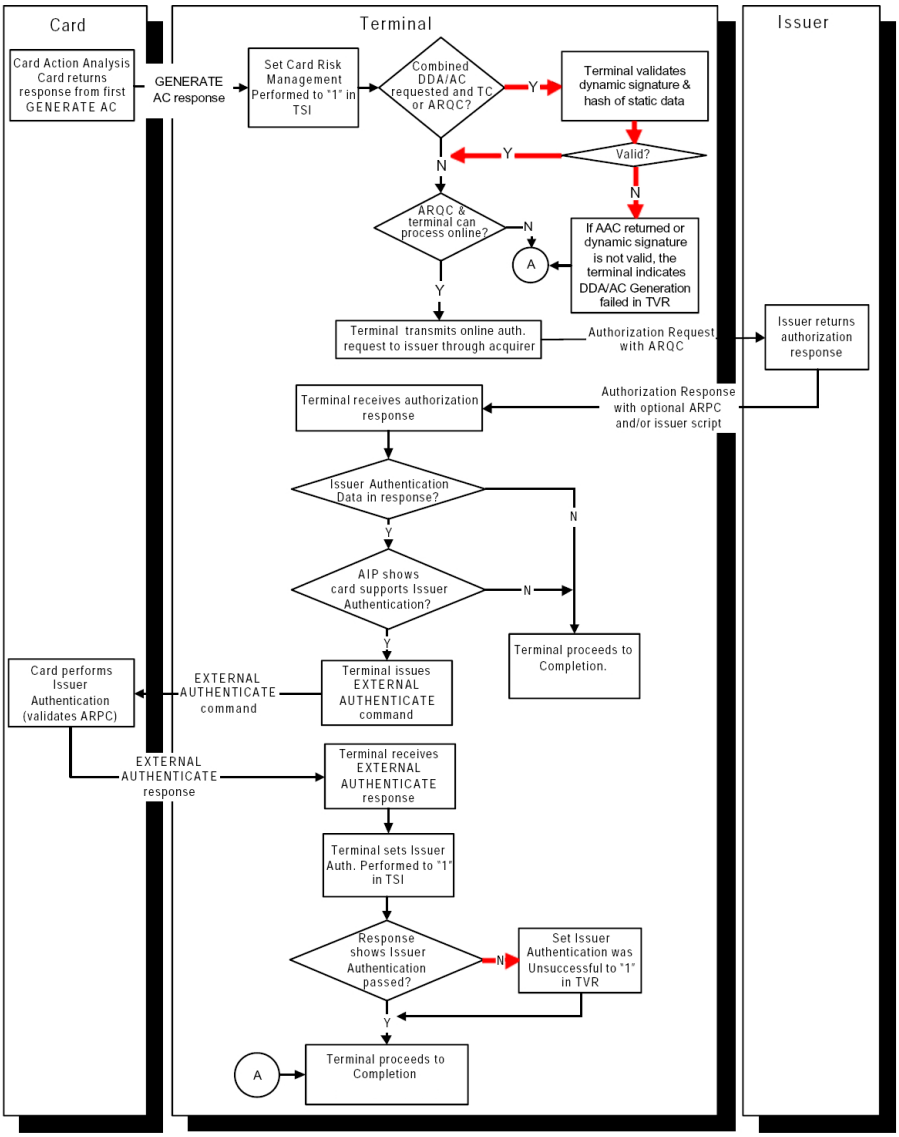


Figure F.19: Step 9: Online Processing Flow

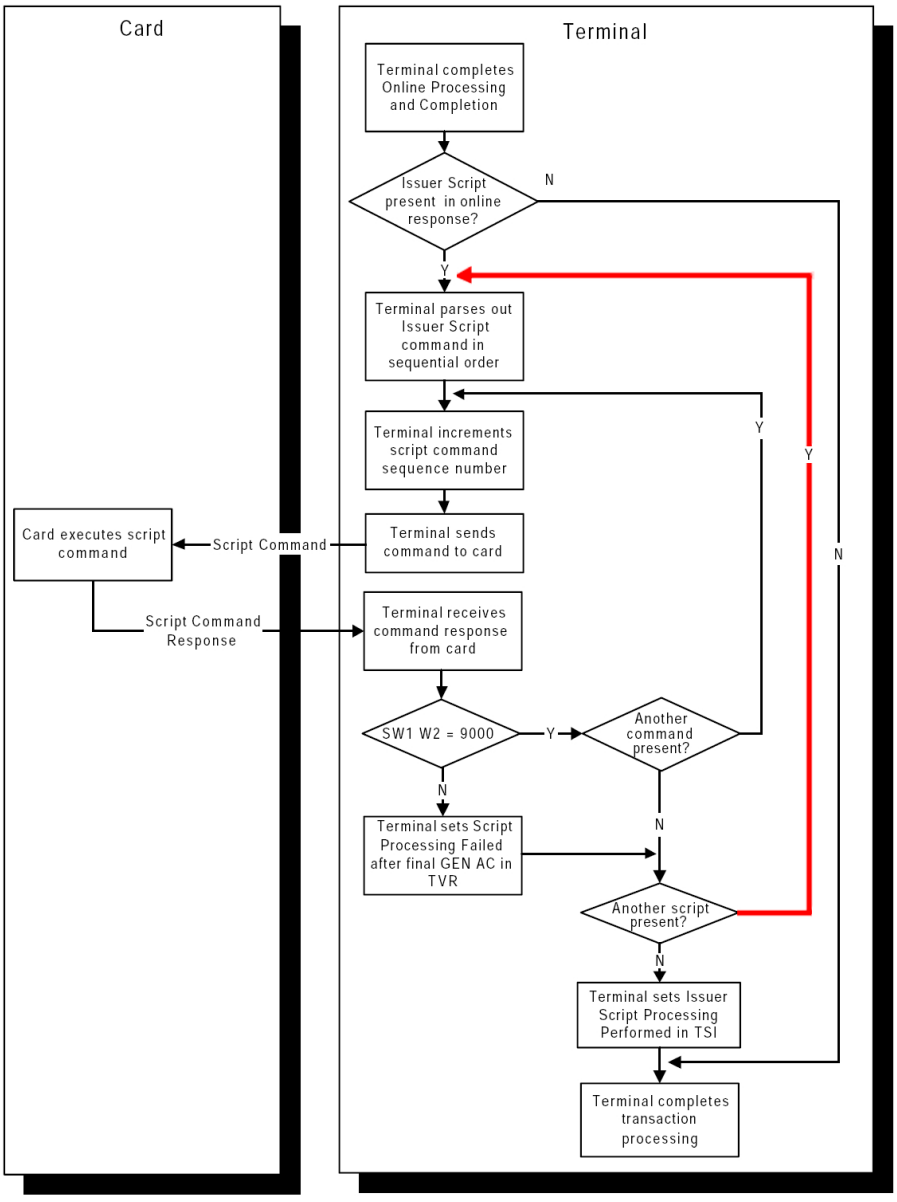


Figure F.20: Step 10: Issuer Script Processing Flow

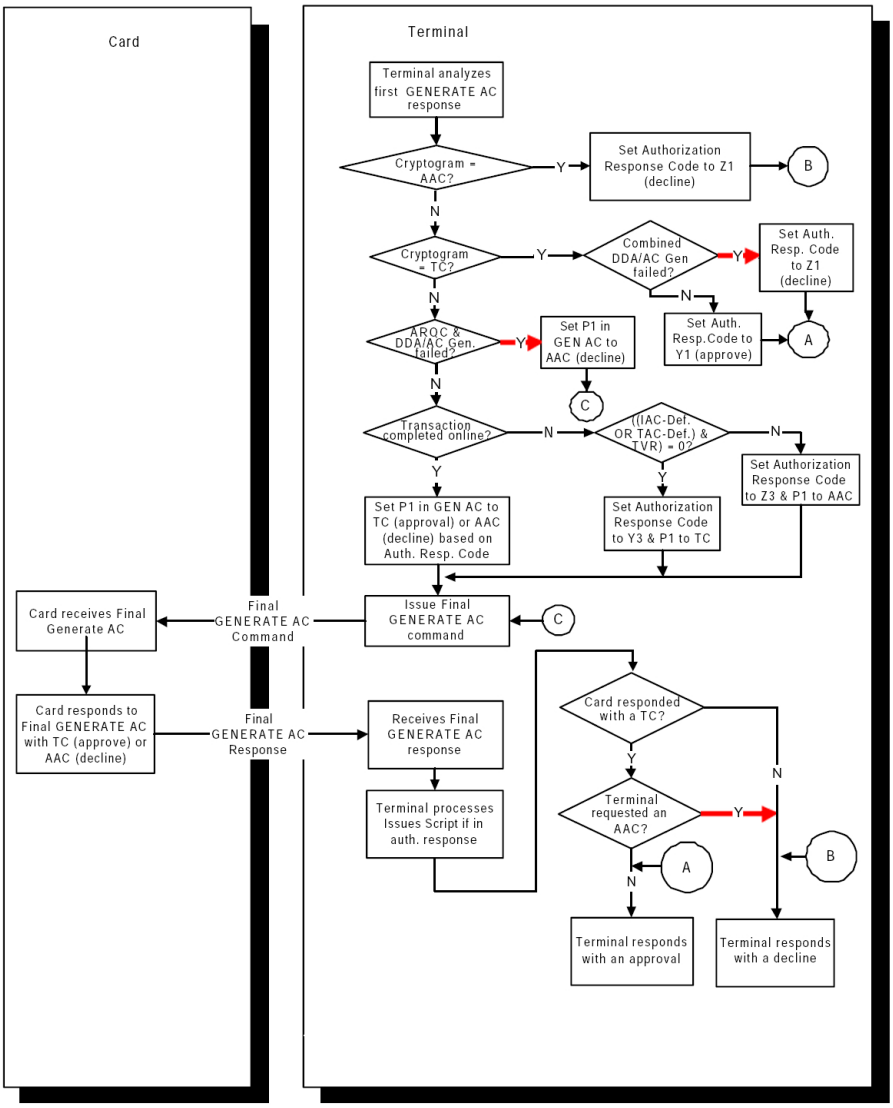


Figure F.21: Step 11: Completion Flow

Appendix G

Communication Messages in the Chain of Components

In this appendix each protocol between the components is discussed, and illustrated by an example request and response. All the requests and responses are from the same transaction flow. All readable credit card numbers are obfuscated so that they are not readable/ usable, according to Payment Card Industry (PCI) compliance [24].

G.1 Card and Terminal

The first part of the communication is between the card and the terminal. This communication can be followed through sniffer logs. With a sniffer device that must be put between the card and the terminal all requests that are sent from the terminal to the card, and all the responses, are stored. This data can be retrieved from the sniffer device by connection it to a computer. Below an example of a part of a sniffer log:

```
+ICC: 70 37 5F 25 03 04 01 01 5F 24 03 09 12 31 9F 07
      02 FF 00 5A 08 ** ** ** ** ** ** 00 20 5F 34 01
      00 9F 0D 05 FC 50 A0 00 00 9F 0E 05 00 00 00 00
      00 9F 0F 05 F8 70 A4 98 00
  +Data Analysis
    Tag  : Application Elementary File (AEF) Data Template
    Length 37
    Value 5F 25 03 04 01 01 5F 24 03 09 12 31 9F 07 02 FF
          00 5A 08 ** ** ** ** ** ** 00 20 5F 34 01 00 9F
          0D 05 FC 50 A0 00 00 9F 0E 05 00 00 00 00 00 9F
          0F 05 F8 70 A4 98 00
      Tag 25 : Application Effective Date
      Length 03
      Value 04 01 01
      Tag 24 : Application Expiration Date
      Length 03
```

```
      Value 09 12 31
      Tag 07 : Application Usage Control
      Length 02
      Value FF 00
      Tag  : Application Primary Account Number (PAN)
      Length 08
      Value ** ** ** ** ** ** 00 20
      Tag 34 : Application PAN Sequence Number
      Length 01
      Value 00
      Tag 0D : Issuer Action Code - Default
      Length 05
      Value FC 50 A0 00 00
      Tag 0E : Issuer Action Code - Denial
      Length 05
      Value 00 00 00 00 00
      Tag 0F : Issuer Action Code - Online
      Length 05
      Value F8 70 A4 98 00
  ICC: SW1 SW2 = 90 00 => Successful
```

This part of the sniffer log indicates the response of some data tags. Tag *GF 25* (or in short *25*) is the Application Effective Date of the application. This is set to the first of January, 2004. The PAN tag is the credit card number, which is *** ** ** ** ** ** 00 20*.

With this detailed information the communication from the card to terminal can be investigated comparing it with the sniffer logs of, for example, an other terminal.

G.2 Terminal and POS Application

As stated in Section 3.5 the terminal uses his own protocol. The message that must be send to the terminal is a binary message. All the messages that are sent between the terminal and the POS application are stored in a separate log file of POS application. Below an example is given of the command 06 request message that is sent from the POS application to the terminal:

```
CMD_06_Req_BinaryMessage:
 0000 - 06 14 06 10 06 09 40 36   00 00 00 00 00 10 00 00
 0010 - 00 00 00 10 00 00 00 00   00 00 00 00 00 00 00 00
 0020 - 03 00 00 03 E8 08 26 02   30 34 31 39 30 30 36 30
 0030 - 00 00 00 00 00 03 30 30   30 31 00 00 01 F4 00 00
 0040 - 30 30 30 30 30 30 30 38   39 34 35 36 30 32 32 52
 0050 - 01
CMD_06_Req_POSTimeout                  : 20
CMD_06_Req_Date                        : 061006
```

```
CMD_06_Req_Time                          : 094036
CMD_06_Req_TransactionType               : 0
CMD_06_Req_TransactionAmount             : 1000
CMD_06_Req_AmountAuthorised              : 1000
CMD_06_Req_AmountOther                   : 0
CMD_06_Req_AcquirerDefault               : 000003
CMD_06_Req_AmountReferenceCurrency       : 1000
CMD_06_Req_TransactionCurrencyCode       : 826
CMD_06_Req_TransactionCurrencyExponent   : 50
CMD_06_Req_TerminalIdentification        : 04190060
CMD_06_Req_AcquirerActual                : 000003
CMD_06_Req_TransactionSeqNum             : 1
CMD_06_Req_TerminalFloorLimit            : 500
CMD_06_Req_HotCardStatus                 : 0
CMD_06_Req_MerchantForcedOnline          : 64
CMD_06_Req_MerchantNumber                : 000000089456022
CMD_06_Req_VLPControl                    : 0
CMD_06_Req_TransactionCategoryCode       : 82
```

The response that the terminal sends back to this request is:

```
CMD_06_Resp_BinaryMessage:
 0000 - 20 00 ** ** ** ** ** **   00 20 FF FF ** ** ** **
 0010 - ** ** 00 20 D0 18 22 01   04 30 AC 66 6F FF FF 09
 0020 - 78 00 46 46 30 30 38 32   36
CMD_06_Resp_Code                         : 0
CMD_06_Resp_PAN                          : ************0020
CMD_06_Resp_Track2                       :
  ************0020=0912201048980666
CMD_06_Resp_ApplicationCurrencyCode      : 978
CMD_06_Resp_ApplicationCurrencyExponent  : 0
CMD_06_Resp_ApplicationUsageControl      : FF00
CMD_06_Resp_TerminalCountryCode          : 826
```

The request and the response consist of binary data. Below the messages the explanation of the message is displayed. As can be seen, the 06 command retrieves also the PAN from the card. The request from the terminal to the card to retrieve this can be seen in the previous section.

G.3 POS Application and PSP

The POS application has an other log file where all the messages that are exchanged with the PSP are stored. Also the PSP logging was extended so that this data could also be retrieved from the PSP. Below a part of the XML request that is sent from the POS application to the PSP:

```
<application>
  <ICCCryptogramInformation>
    80
  </ICCCryptogramInformation>
  <ICCCryptogramType>
    0
  </ICCCryptogramType>
  <ICCAppUsageControl>
    FF00
  </ICCAppUsageControl>
  <ICCAppId>
    A0000000041010
  </ICCAppId>
  <cryptogram>
    F110583240379A17
  </cryptogram>
  <interchangeProfile>
    5800
  </interchangeProfile>
  <transactionCounter>
    015E
  </transactionCounter>
</application>
<issuerCardData>
  <ICCIssuerActionCode>
    0000000000F870A49800FC50A00000
  </ICCIssuerActionCode>
  <applicationData>
    0212A5000F040000DAC000000000000000FF
  </applicationData>
  <track number="2">
    ************0020=0912201048980666
  </track>
</issuerCardData>
```

For example, the retrieved track2 data is sent in the XML to the PSP. A part of the response from the PSP to this request looks like this:

```
<EMV_Response>
  <authenticationData>
    <ARPC>
      539673BE3BCDD95B
    </ARPC>
    <authorisationResponseCode>
```

```
      0012
    </authorisationResponseCode>
  </authenticationData>
  <script>
    FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  </script>
</EMV_Response>
```

In the response is an certificate from the issuer (the *ARPC* tag), and also an issuer script (the *script* tag). These are values that the PSP received after the request is sent to the acquirer (see the next section).

G.4 PSP and Acquirer

The protocol that is used for the communication with the acquirer is APACS30 [5, 4]. Below an example of the authorisation request that the POS application has send to the PSP (see previous section), that is sent from the PSP to the acquirer:

```
<stx>
4 04190060 0000 3182 20 89456022
<fs>
************0020=0912201048980666
<fs>
1000
<fs>
<us>
<us>
<fs>
<fs>
<fs>
<fs>
0803070941
<fs>
22
<fs>
826
<fs>
826
<fs>
10
<fs>
F110583240379A17 5800 015E C1FF2886
0000008000 00 0212A5000F040000DAC000000000000000FF
<us>
```

```
A0000000041010
<us>
0002
<us>
80
<us>
410302
<fs>
<etx>
```

The <*stx*> tag indicates the start of the message and <*etx*> the beginning of a message. The tags <*fs*>, and <*us*> are used to split up values. For example, the first *4* is a message sort indicator, the next value is the terminal indicator (each terminal has his own unique number), and the value after the first <*fs*> is the track2 data. Most of the values that the POS application has sent to the PSP are just forwarded to the acquirer, but in a different format.

The response of the acquirer to this request looks like this:

```
<stx>
4 04190060 0000 12 00 0
<fs>
<fs>
AUTH CODE:075462
<fs>
<fs>
5
<fs>
0703
<fs>
539673BE3BCDD95B 0012
<us>
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
<fs>
000800
<fs>
<etx>
```

The value *12* in the first line after the <*stx*> tag is the message type and indicates that the authorisation is approved. After the second <*fs*> tag the value of the authorisation code can be found. The value after the <*us*> tag is the issuer script. This value (only Fs) indicates that there is no issuer script that needs to be processed by the card.