PayPass – M/Chip

Security Architecture

Version 1.2 – November 2007
Copyright

The information contained in this manual is proprietary and confidential to MasterCard International Incorporated or one of its affiliated entities (collectively “MasterCard”) and its customer financial institutions.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Media

This document is available in both electronic and printed format.

MasterCard Worldwide - Chip Center of Excellence
Chaussée de Tervuren, 198A
B-1410 Waterloo
Belgium

E-mail: specifications@paypass.com
# Table of Contents

**Using this Manual** ................................................................. 5  
- Scope ......................................................................................... 5  
- Audience .................................................................................... 5  
- Contents ..................................................................................... 5  
- Related Publications .................................................................. 6  
- Abbreviations ............................................................................ 7  

**1 PayPass Payments** .............................................................. 9  
1.1 Magnetic Stripe and Contact Chip Technology ......................... 9  
  1.1.1 Traditional face-to-face Environments ........................................ 9  
  1.1.2 Virtual Environment ................................................................... 10  
1.2 PayPass Technology .................................................................. 10  
  1.2.1 Environment .............................................................................. 10  
  1.2.2 Business requirements ................................................................. 11  
  1.2.3 Security Requirements ................................................................. 12  

**2 Security Analysis** ............................................................... 13  
2.1 Fraud ....................................................................................... 13  
  2.1.1 Guessing Attacks ....................................................................... 13  
  2.1.2 Passive Attacks ........................................................................... 14  
  2.1.3 Active Attacks ............................................................................. 14  
  2.1.4 Real-time Active Attacks ............................................................... 15  
2.2 Denial of Service ........................................................................ 15  
2.3 Privacy Invasion ......................................................................... 16  

**3 Two EMV-based techniques** ................................................. 17  
3.1 Introduction .............................................................................. 17  
3.2 Use of an Online EMV-based Cryptogram .................................... 17  
  3.2.1 Purpose of mechanism ................................................................. 17  
  3.2.2 Flow description ........................................................................... 18  
3.3 Use of an EMV-based CDA approach .......................................... 19  
  3.3.1 Purpose of mechanism ................................................................. 19  
  3.3.2 Flow description ........................................................................... 19  

**4 Assessment of EMV-based techniques** ............................... 21  
4.1 Computation process and choice of algorithm ......................... 21  
4.2 Security Considerations .......................................................... 21  
  4.2.1 Fraud Attacks .............................................................................. 21
# Table of Contents

4.2.2 Denial of Service Attacks .................................................................................. 22
4.3 Use of an Online EMV-based Cryptogram ...................................................... 22
4.3.1 Guessing Attacks............................................................................................... 22
4.3.2 Replay Attacks .................................................................................................. 22
4.3.3 Preplay attacks .................................................................................................. 23
4.3.4 Relay Attacks .................................................................................................... 23
4.3.5 DoS Attacks on the Card................................................................................... 23
4.3.6 Recommendations............................................................................................. 23
4.4 Use of an EMV-based CDA approach ............................................................. 24
4.4.1 Guessing Attacks............................................................................................... 24
4.4.2 Replay Attacks .................................................................................................. 24
4.4.3 Preplay attacks .................................................................................................. 24
4.4.4 Relay Attacks .................................................................................................... 24
4.4.5 DoS Attacks on the Card................................................................................... 24
4.4.6 Recommendations............................................................................................. 25

5 PayPass – M/Chip Risk Model ................................................................................. 27
5.1 Guessing, Replay and Preplay Attacks ............................................................ 27
5.2 Relay Attacks ....................................................................................................... 27
5.3 Risks to Other Environments ............................................................................ 27
5.3.1 Use of PayPass-specific PANs ......................................................................... 27
5.3.2 Use of SecureCode .......................................................................................... 28
5.3.3 Use of CVC2 for MO/TO .................................................................................. 28
5.4 Lack of Cardholder Approval .......................................................................... 28
5.5 Lack of Cardholder Authentication .................................................................... 29
5.6 Lack of Terminal Authentication ...................................................................... 29
5.7 Data Privacy ........................................................................................................ 30
5.8 Denial of Service ................................................................................................. 30

6 Conclusions ........................................................................................................... 31
Using this Manual

This chapter contains information that helps you understand and use this document.

Scope

MasterCard PayPass™ technology enables fast, easy and globally accepted payments through the use of contactless chip technology on the traditional MasterCard card platform. PayPass – M/Chip is designed specifically for offline environments and authorization networks that presently support EMV chip card authorizations for credit or debit applications.

This document provides a threat and risk analysis of credit and debit PayPass – M/Chip payments. It uses the results of that analysis as the basis of an analysis of the PayPass – M/Chip security features, mainly those based on the use of EMV functions. The following steps are performed to conduct this analysis:

- Identification and analysis of security threats related to PayPass environment and of the vulnerabilities specific to PayPass.
- Description and analysis of two PayPass security features based on EMV online and offline card authentication mechanisms.
- Analysis of the overall PayPass – M/Chip risk model.

Audience

This document is intended for use by acquirers acquiring PayPass – M/Chip transactions and issuers issuing PayPass – M/Chip cards.

It is assumed that the audience already has an understanding of chip card technology in general.

Contents

A brief introduction to PayPass is provided, which forms the basis of the review of high-level threats to PayPass payments.

The security-relevant parts of the EMV online and offline card authentication techniques, which are the main focus of this document, are described. This includes descriptions of the data elements, the main data flows, the cryptographic computations, and the processing by the card, the terminal and the issuer.
The next part of the document provides a view of PayPass – M/Chip risk model, including a risk assessment and a description of other PayPass security measures. The last part of the document provides some conclusions.

Related Publications

The following publications contain information directly related to the contents of this specification.


# Abbreviations

The following abbreviations are used in this specification:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>Triple-DES</td>
</tr>
<tr>
<td>ARQC</td>
<td>Authorization Request Cryptogram</td>
</tr>
<tr>
<td>ATC</td>
<td>Application Transaction Counter</td>
</tr>
<tr>
<td>CDA</td>
<td>Combined Dynamic Data Authentication</td>
</tr>
<tr>
<td>CSK</td>
<td>Common Session Key Derivation Algorithm</td>
</tr>
<tr>
<td>CVC</td>
<td>Card Verification Code</td>
</tr>
<tr>
<td>DDA</td>
<td>Dynamic Data Authentication</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DPA</td>
<td>Differential Power Analysis</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay MasterCard Visa</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Circuit Card</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MO/TO</td>
<td>Mail Order / Telephone Order</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary Account Number</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>SDA</td>
<td>Static Data Authentication</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>UN</td>
<td>Unpredictable Number</td>
</tr>
</tbody>
</table>
1 PayPass Payments

A PayPass payment is a payment made using a chip card that does not need to be in physical contact with a card reader. That is, the card communicates with a merchant terminal via wireless means, instead of via chip card electrical contacts or via the reading of a magnetic stripe. Clearly, the wireless nature of the communication between the card and the terminal may introduce new threats to the system security. These new threats have to be tackled adequately by the PayPass security architecture.

The purpose of PayPass – M/Chip is to allow contactless chip payments to use offline terminals or authorization networks (proprietary and shared) that support contact chip authorizations for credit or debit applications.

In the text below, a number of assumptions are stated regarding the nature of the environments in which various types of payment are conducted. In particular the environmental conditions for traditional and virtual payments are contrasted with those arising for the PayPass environment. This enables the security vulnerability analysis to distinguish the different vulnerabilities arising from the PayPass environment, based on the types of authentication performed and on the data exchanged.

1.1 Magnetic Stripe and Contact Chip Technology

1.1.1 Traditional Face-to-face Environments

1.1.1.1 Authentication

In the traditional face-to-face environment both the card (credit or debit) and the cardholder are present at the merchant premises. The authentication process has the following characteristics.

- **Card authentication:** with magnetic stripe technology, the physical characteristics of the card – such as embossing, hologram and/or brand logo – may be checked by the merchant if present. In the case of an online transaction, mechanisms like the Card Verification Code (CVC1) give some level of assurance that the card is genuine. In practice, the possession of a valid card, i.e., a card containing the necessary data to conduct a payment, is often enough to complete a successful transaction. With EMV technology the terminal may perform either online card authentication (by submitting to the issuer a card-generated Authorization Request Cryptogram – ARQC) or offline card authentication (including SDA, DDA or CDA).

- **Cardholder authentication:** this may be achieved through entry of a Personal Identification Number (PIN) or a signature by the cardholder. Some merchants require the cardholder to provide other evidence, e.g. the cardholder’s passport, to demonstrate that the cardholder is the genuine owner of the card. However, in many cases where signature is used, merchants do not even compare the signature provided by the cardholder with the one on the back of the card. Hence, in practice, the authentication
process is minimal when PIN is not used, and the possession of a valid card, i.e., a card containing the necessary data to conduct a payment, is often enough to complete a successful transaction.

- **Terminal authentication**: no mechanism exists to allow the cardholder to authenticate the terminal. Cardholders build a trust relationship with the merchant, and as a result trust that the merchant terminal is legitimate and has not been modified. If terminals are unattended, cardholders should verify by some means that the terminal is legitimate.

1.1.1.2 Payment Data

The card provides a means of payment. With magnetic stripe technology, the necessary data to conduct a transaction include the Primary Account Number (PAN), the card expiry date, and the CVC1 of the card. These data are all contained in the card’s magnetic stripe. With EMV technology, the data listed above may not be sufficient to perform a transaction, since the card may, for example, also be asked to perform offline authentication, which requires signed static data in the card (for SDA).

1.1.2 Virtual Environment

In the virtual environment, neither the card (typically a credit card) nor the cardholder are present at the merchant site. The lack of human involvement in the transaction is one of the greatest benefits of e-commerce, as it allows the merchant to handle more transactions, more quickly and more cheaply. However, this benefit is also a source of security vulnerabilities.

1.1.2.1 Authentication

In many cases there is neither card authentication nor cardholder authentication. Cardholder authentication is only available when security mechanisms like SecureCode are used, and is usually provided through password provision. The equivalent of terminal authentication is typically poor, although it can be supported by technical mechanisms like Secure Socket Layer (SSL) server authentication.

1.1.2.2 Payment Data

Today’s payments in the virtual world (including those made via the Internet as well as MO/TO transactions) usually require only the PAN and expiry date of the card, and optionally require the merchant to get the CVC2 of the card. The payment instructions are often transmitted over the Internet without any real protection, and card and payment data stored in merchant databases are often poorly protected.

1.2 PayPass Technology

1.2.1 Environment

The environment where PayPass technology is used can be regarded as a special case of the traditional face-to-face environment, but has different characteristics, as follows.
- **PayPass card**: a card into which integrated circuit(s) and coupling means have been placed that allow communication with a PayPass coupling device (i.e., terminal) through inductive coupling.

- **PayPass coupling device**: a reader/writer device that uses inductive coupling to provide power to the PayPass card, and also to control the data exchange with the PayPass card. The device produces an energizing radio frequency field which couples to the card to transfer power and which is modulated for communication. A PayPass coupling device has typically an operating range of less than 10 cm (4 inch). A PayPass coupling device may be part of a merchant terminal.

- **Over-the-air transfer of data**: card and payment data are transmitted over-the-air between a PayPass card and a PayPass coupling device integrated into a terminal.

PayPass payments are designed with the following business drivers in mind:

- **User convenience**: PayPass payments are intended to be simple and fast, the ‘tap and go’ description captures the ease and speed benefits to both cardholder and merchant. Merchants in particular may win significant process improvements as a result of increased transaction speed.

- **Backwards compatibility**: support of PayPass payments does not require significant modifications to acquirer, issuer or payment system infrastructure.

- **Support of new form factors**: PayPass payments allow for form factors that cannot be used with traditional cards, for instance key fobs or watches.

PayPass design intends to fully deliver these benefits. However, this may cause some limitations to the PayPass security architecture, as the above business drivers may conflict with some potential security measures. Whenever required, the PayPass security architecture must accommodate appropriate trade-offs between security and functionality as is usual in any service.

### 1.2.2 Business requirements

The choice of a particular security architecture for PayPass payments is driven by the following business requirements:

- The overall fraud in the system relating to the PayPass should not damage consumers trust in brand.

- **PayPass** should re-use and/or converge with existing and developing MasterCard programs.

- **PayPass** technology components must conform to international standards. These standards refer to ISO/IEC 14443 but also to security standards, e.g. for cryptographic algorithms.

- Risks levels should not be higher for PayPass transactions than for conventional magnetic stripe card based transactions.

- **PayPass** security architecture should be designed such as to minimize changes to acquirer’s and issuer’s operational processes and infrastructure.

- **PayPass** payment process must be quicker than cash, cheque and existing credit or debit card payment processes. This is an important requirement that implies that the
processing time for each cryptographic operation and the number of computations required must be carefully considered.

1.2.3 Security Requirements

The security requirements are the starting point for the design of the security architecture. These requirements determine the security measures that have to be implemented to remove or reduce the vulnerabilities arising from the particular properties of the PayPass technology. In order for PayPass to provide a security level similar to or higher than the security level of magnetic stripe, it is mandatory to:

- Introduce an efficient anti-replay mechanism for PayPass transactions, and
- Limit the impact of fraudulent capture of PayPass data by fraudsters, both in the face-to-face environment and in other environments.
2 Security Analysis

The threats and attacks that are identified and analyzed in this document are only the ones that derive from the particular nature of the PayPass technology. The analysis does not include threats that may already be found in other technologies.

It is not the intention of this document to try to address all the threats applicable to a payment technology, magnetic stripe, contact chip, PayPass or other. The intention is instead to identify the new threats specific to the PayPass technology, and to analyze possible countermeasures.

The characteristics of the PayPass technology and of its business drivers may result in potential vulnerabilities that may be exploited by fraudsters and lead to the following threats:

- Fraud
- Denial of service (DoS)
- Privacy invasion.

2.1 Fraud

Fraudsters may attempt to conduct fraud, that is, generating fraudulent payment transactions, by using the following potential vulnerabilities:

- It may be possible to generate data as transmitted between card and terminal. Such a possibility might be exploited by fraudsters in guessing attacks.

- It may be possible to capture data transmitted between card and legitimate terminal during a genuine transaction. Such a possibility might be exploited by fraudsters in passive attacks.

- It may be possible to capture data transmitted between card and illegitimate terminal during an attacker-forced transaction. Such a possibility might be exploited by fraudsters in active attacks.

- It may be possible to use an illegitimate terminal in proximity of a card to force fraudulent transaction without cardholder’s consent. Such a possibility might be exploited by fraudsters in real-time active attacks.

2.1.1 Guessing Attacks

It is feasible to guess or predict data to be transmitted between a card and legitimate terminal during a genuine transaction, without the need for eavesdropping actual transactions.

This vulnerability may enable a fraudster to conduct fraudulent PayPass transactions.
2.1.2 Passive Attacks

It is feasible to capture data transmitted over-the-air between a PayPass card and a legitimate terminal during a genuine transaction. This could, for example, be through the use of an illicit antenna and reader device that is either:

- Mobile and carried by the fraudster (e.g., in a rucksack) in the proximity of the genuine card and cardholder, such as in the queue of a fast food restaurant, or
- Fixed and placed in the proximity of the legitimate terminal, such as under an unattended terminal in a petrol station.

This vulnerability may enable a fraudster to capture data that could be re-used to conduct either fraudulent PayPass transactions or fraudulent magnetic stripe card, contact chip card or electronic commerce transactions. Such attacks are also known as replay attacks.

PayPass cards could be read from distances larger than the ranges supported by off-the-shelf readers. However, long-distance receivers would require specific development, and their actual operating range would depend on receiver cost and antenna size.

Reports indicate that receivers costing around $10K and featuring fairly large antennas and a large and heavy power supply may capture card data within a range of 1-2 meters. Smaller, "suitcase" readers would be limited to a range of half a meter.

While in theory it is feasible to build a mobile antenna and for the fraudster to carry it, in practice this imposes severe constraints on the operational distance and on the dimensions of the antenna, since otherwise the noise received by the antenna is likely to be too great to enable data capture.

A fixed antenna may be placed by the fraudster in the direct proximity of a legitimate terminal, but the success of this operation probably relies on there being poor physical protection for the legitimate terminal, since otherwise the noise received by the antenna is again likely to be too great to enable data capture. When installed at merchant locations, such fixed antennas are likely to be detected by classical fraud forensic mechanisms already in place.

2.1.3 Active Attacks

It is possible that a legitimate or illegitimate terminal and/or reader device in the possession of a fraudster could be used to force the PayPass card to produce data, without the cardholder’s consent (e.g., by placing a fraudulent terminal in proximity to a genuine card, e.g. in a crowded train or bus). The captured data could be used subsequently to conduct a fraudulent transaction. This vulnerability would enable the fraudster to capture data that could be re-used to conduct either a fraudulent PayPass transaction or a fraudulent magnetic stripe, contact chip or electronic commerce transaction. Such attacks are also known as preplay attacks.

Clearly, to exploit this vulnerability, the only requirement for the fraudster is to possess a legitimate terminal or to build an illegitimate one. Note that such an illegitimate device may conduct PayPass transactions at greater operating distances than a legitimate device can, since it does not have to comply with [ISO/IEC 14443 PAYPASS] power requirements.
In addition to simply reading data from the card, the fraudster could attempt to force the conduct of a full fraudulent transaction by the PayPass card, without the cardholder’s consent. The fraudster would then need to be able to submit the transaction to a legitimate terminal, using for instance a rogue PayPass card. This vulnerability could enable the conduct of a fraudulent PayPass transaction.

The feasibility of active attacks depends largely on whether terminal authentication by the card takes place during a transaction. This is typically not the case because of backwards compatibility reasons, as the magnetic stripe technology does not provide support for terminal authentication.

### 2.1.4 Real-time Active Attacks

When there are two fraudsters, one possessing a rogue card in the proximity of a legitimate terminal and the other possessing an illegitimate reader device in the proximity of a genuine card, and where a real-time communication link exists between the two fraudsters, so-called relay attacks may be set up. When the legitimate terminal initiates the transaction, the first fraudster forwards the commands sent to his rogue card to the second fraudster who makes the genuine card generate the necessary response. These data are forwarded to the first fraudster, who finalizes the transaction.

In order to perform relay attacks, fraudsters need:
- A rogue card
- An illicit reader
- A real-time communication means between the rogue card and the illegitimate reader. The data exchanges on that link have to comply with the PayPass timing requirements for the card-terminal communication.

If the fraudster is him/herself a fraudulent merchant, this vulnerability is neither new nor specific to the PayPass technology. Such a merchant is likely to be identified by today’s fraud detection mechanisms, as many complaints will be received from cardholders for a particular terminal and merchant.

If the fraudster is not a merchant, this vulnerability may be harder to fix. However, exploiting it requires significant technical expertise, and a number of technological barriers (e.g., timing requirements) would have to be overcome.

Note that the rollout of non-card form factor devices (especially those equipped with integrated communication capabilities, e.g., NFC-capable mobile phones) may make relay attacks easier to mount. However, they may also provide support for protection mechanisms.

### 2.2 Denial of Service

It is possible that a legitimate or illegitimate terminal and/or reader device in the possession of a fraudster could be used to conduct DoS attacks, in which the fraudster seeks preventing a genuine card from being used to conduct (genuine) transactions.
2.3 Privacy Invasion

It is feasible to capture data transmitted over-the-air between a PayPass card and a legitimate terminal during a genuine transaction, or it may be possible to force a PayPass card to produce data, without the cardholder’s consent. As such data carry cardholder-related information, their capture may cause a threat to the cardholder’s privacy.
3 Two EMV-based Techniques

3.1 Introduction

The security requirements listed in section 1.2 are the starting point for the design of the PayPass – M/Chip security architecture. This section describes in detail the resulting mechanisms, which are essential components of that architecture. The detailed technical specification can be found in [PAYPASS CHIP].

These mechanisms are designed to meet the following security requirements:

- Introduce an efficient anti-replay mechanism for PayPass transactions, and
- Limit the impact of fraudulent capture of PayPass data by fraudsters, both in the PayPass face-to-face environment and other environments.

This objective can be achieved with the PayPass technology by proving the legitimacy of the data transmitted over-the-air. This can be done through mechanisms requiring the card to authenticate itself dynamically. Hence for each transaction the card performs a unique dynamic action such that only the genuine card could perform this action and any replay of this action would be detected.

3.2 Use of an Online EMV-based Cryptogram

3.2.1 Purpose of mechanism

The online EMV-based cryptogram technique is a possible approach to make the card authenticate by performing a unique dynamic action for each transaction. It assumes online transactions and is based on an existing EMV infrastructure.

In this mechanism, the PayPass card computes a cryptogram - a Message Authentication Code (MAC) - on data supplied by the terminal and data specific to the card, including transaction details, unpredictable number (UN) generated by the terminal and a card-stored Application Transaction Counter (ATC), using a session key shared with the issuer. The MAC, unique for each transaction, is sent to the issuer for verification. The ATC is incremented by the card at each transaction.

The approach is hence similar to the online dynamic CVC3 technique described in [PAYPASS MAGSEC]. The most important differences are the following:

- The data that are input to the MAC computation,
- The use of a session key, and
- The size of the cryptogram.
Two EMV-based Techniques
Use of an Online EMV-based Cryptogram

This increases the security of this protocol compared to the above-mentioned online dynamic CVC3 technique.

3.2.2 Flow description

A number of EMV commands are exchanged between the card and the terminal so that the card has the necessary elements to perform the cryptogram computation (see Table 1). The process is the same as an EMV exchange today, except for the fact that it involves an over-the-air transmission.

Table 1: Recommended data elements for cryptogram computation

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Supplied by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount, Authorized (numeric)</td>
<td>Terminal</td>
</tr>
<tr>
<td>Amount, Other (numeric)</td>
<td>ICC</td>
</tr>
<tr>
<td>Terminal Country Code</td>
<td>Terminal</td>
</tr>
<tr>
<td>Terminal Verification Results</td>
<td>ICC</td>
</tr>
<tr>
<td>Transaction Currency Code</td>
<td>Terminal</td>
</tr>
<tr>
<td>Transaction Date</td>
<td>ICC</td>
</tr>
<tr>
<td>Transaction Type</td>
<td>Terminal</td>
</tr>
<tr>
<td>Unpredictable Number</td>
<td>ICC</td>
</tr>
<tr>
<td>Application Interchange Profile</td>
<td>Terminal</td>
</tr>
<tr>
<td>ATC</td>
<td>ICC</td>
</tr>
<tr>
<td>Card Verification Results</td>
<td>Terminal</td>
</tr>
</tbody>
</table>

As a second step, the card derives a 16-byte session key for a card-stored master key, using, for example, the EMV Common Session Key Derivation Algorithm (CSK) approach. The card then concatenates the data specified in Table 1 in the order specified to create a block of data. The card formats this block of data into 8-byte blocks and pads this block according to method 2 of ISO/IEC 9798-1. Finally the card performs the MAC algorithm described in section A1.2 from [EMV41] using the derived session key.

The cryptogram is the 8-byte result that is then transmitted to the issuer via the terminal, as in EMV contact transactions.
3.3 Use of an EMV-based CDA approach

3.3.1 Purpose of mechanism

The EMV-based CDA technique makes the card authenticate dynamically by performing a unique dynamic action for each transaction. It is one of the offline card authentication methods specified as part of EMV, and requires the presence of an EMV infrastructure.

In this mechanism, the PayPass card first generates a cryptogram. Then, using its private key, it generates a signature on a combination of data supplied by the terminal and specific to the card (including transaction details, UN and ATC), and the cryptogram (approve, decline, go online). The terminal verifies the signed data using the card’s public key, checks the UN and observes the card’s decision.

This approach is less useful than the one described in 3.2 if the card or the terminal asks to go online, as the signature is an additional step in the generation of a cryptogram. However, the advantage of this method is that it can be used for both online and offline decisions.

3.3.2 Flow description

The EMV Combined DDA/Application Cryptogram (CDA) approach is described in detail in [EMV41], pp.2-12 to 2-18.
Two EMV-based Techniques
Use of an EMV-based CDA approach
4 Assessment of EMV-based techniques

4.1 Computation process and choice of algorithm

The algorithm used for the computation of cryptograms makes use of 5 cycles of DES and one of 3DES, where DES (Data Encryption Standard) corresponds to the ISO 8731-1 and ISO 8372 standards. Other algorithms may be faster but both their security and complexity of implementation are still under consideration.

Key derivation for the computation of the cryptogram can be performed using the EMV CSK method. Using key derivation limits the number of pairs cleartext/ciphertext pairs that may be available to an attacker. This allows for the use of two-key 3DES, which in the EMV context is believed to be secure until 2030.

The algorithm used for the signature generation and verification is RSA. RSA key sizes are as per MasterCard policy for contact EMV transactions.

4.2 Security Considerations

Possible attacks on the EMV-based techniques are divided into two main categories:

- **Fraud attacks**, in which a third party seeks to use a ‘bogus card’ to conduct a fraudulent transaction, and
- **DoS attacks**, in which a third party seeks preventing a genuine card from being used to conduct (genuine) transactions.

Other possible attacks (e.g. those involving use of a stolen or borrowed card) are not considered since these are not directly related to the security techniques described. Similarly, threats to privacy are not considered as they are not addressed by these techniques.

4.2.1 Fraud Attacks

The four types of fraud attacks identified in section 2.1 and their relation to the online EMV-based cryptogram technique are analyzed separately. The four types are:

- **Cryptogram guessing attacks**, in which the fraudulent card supplies a random cryptogram value in response to a ‘Generate AC’ command.
- **Replay attacks**, in which the fraudulent card uses a (valid) cryptogram value intercepted (using a passive attack) from a previous valid transaction between a card and a terminal.
- **Preplay attacks**, in which the fraudulent card uses a (valid) cryptogram value obtained from a valid card using a fraudulent terminal (using an active attack).
• Relay attacks, in which an active attack is mounted in real-time.

4.2.2 Denial of Service Attacks

We consider the two following types of DoS attack:
• Attacks on the (genuine) card, and
• Attacks on the card issuer.

4.3 Use of an Online EMV-based Cryptogram

4.3.1 Guessing Attacks

The cryptogram generated by the card is 8 bytes long. The EMV infrastructure allows these 8 bytes to be transmitted, whereas a magnetic-stripe based infrastructure limits the transmission to a few digits.

It thus gives the fraudster only one chance out of $2^{64}$ to guess the correct cryptogram, which is easily sufficient to prevent him from sending cryptograms until a valid one is found. The issuer may, if desired, set up a fraud detection system whereby he will stop accepting transactions from a particular card once too many invalid cryptograms have been received. However this risk is minor, and the additional protection provided by such a fraud detection system can be therefore deemed optional.

4.3.2 Replay Attacks

The 4-byte UN is transmitted in full to the issuer. Hence the replay attacks described in [PAYPASS MAGSEC] for the online dynamic CVC3 are almost infeasible (including the construction of a table or the request of a particular UN to the terminal) and the security recommendations can be less stringent.

The replay of a valid cryptogram that was accepted in a previous transaction implies that all elements in Table 1 input to the cryptogram computation process are the same as for the genuine transaction, which may occur only if:
• The 4-byte UN is the same,
• The ATC is the same, and
• All transaction details are the same (including the transaction time).

The probability that all these hold is very small, since on its own the probability of getting a particular UN in real time from the terminal is one in $2^{32}$. The optional check by the issuer that the ATC has not been used before may prevent fraudulent merchants from replaying the cryptogram with the same UN and transaction details, although it may be easier for them to use a coupling device in the proximity of the card to make it generate a new cryptogram for a particular UN.
4.3.3 Preplay attacks

When the fraudster may both make the card generate cryptograms for several UNs and get several UNs from the terminal, generation of $2^{16}$ different UNs by both terminal and card is needed in order to have a probability of success of about 0.5. Therefore, such an attack is unrealistic.

4.3.4 Relay Attacks

The online EMV-based cryptogram technique does not protect against relay attacks. However, conducting such attacks would require significant technical expertise, and a number of technological barriers (e.g., timing requirements) would have to be overcome by the fraudster.

4.3.5 DoS Attacks on the Card

Here a malicious third party seeks to render a card invalid by using an illicit terminal in the proximity of a valid card. One obvious attack is to cause the card to keep incrementing its ATC until it reaches its upper limit of $2^{16}$.

4.3.6 Recommendations

The following checks are not necessary in this approach, but may be implemented. They include:

- The issuer checks that the ATC is valid, if the cryptogram received is valid.
- The issuer blocks the card after a certain number of invalid cryptograms have been received.
- The terminal monitors the number of aborted transactions and takes appropriate measures if an excessive number of aborted transactions is detected; for example the terminal could introduce wait times after three aborted transactions.
- The terminal imposes short card response time, e.g. a few seconds.
4.4 Use of an EMV-based CDA approach

4.4.1 Guessing Attacks

The generation of a valid signed message is infeasible for a fraudster, as he does not know the card’s private key.

4.4.2 Replay Attacks

The replay of a valid signed message that was accepted in a previous transaction implies that all elements of the message are the same as for the genuine transaction, which may occur only if:

- The 4-byte UN is the same,
- The ATC is the same, and
- All transaction details are the same (including the transaction time).

The probability that all these hold is very small, since on its own the probability of getting a particular UN in real time from the terminal is one in $2^{32}$.

4.4.3 Preplay attacks

When the fraudster may both make the card generate signed message for several UNs, and get then several UNs from the terminal, generation of $2^{16}$ different UNs by both terminal and card is needed in order to have a probability of success of about 0.5. Therefore, such an attack such an attack is unrealistic.

4.4.4 Relay Attacks

The offline EMV-based CDA technique does not protect against relay attacks. However, conducting such attacks would require significant technical expertise, and a number of technological barriers (e.g., timing requirements) would have to be overcome by the fraudster.

4.4.5 DoS Attacks on the Card

Here a malicious third party seeks to render a card invalid by using an illicit terminal in the proximity of a valid card. One obvious attack is to cause the card to keep incrementing its ATC until it reaches its upper limit of $2^{16}$.
4.4.6 Recommendations

The following checks are not necessary in this approach, but may be implemented. They include:

- The terminal monitors the number of aborted transactions and takes appropriate measures if an excessive number of aborted transactions is detected; for example the terminal could introduce wait times after three aborted transactions.

- The terminal imposes short card response time, e.g. less than a second.
Assessment of EMV-based techniques
Use of an EMV-based CDA approach
5 PayPass – M/Chip Risk Model

5.1 Guessing, Replay and Preplay Attacks

The level of risk associated with this type of attack is extremely low.

5.2 Relay Attacks

Relay attacks are not a new vulnerability or one specific to the PayPass technology. However, this vulnerability has a bigger impact in PayPass, as access to the card can potentially happen at any time, without the cardholder's knowledge and consent. With the classical chip payment technology, only legitimate yet fraudulent merchants may commit relay attacks. Such fraudulent merchants are easily identified and shut down.

The risk of relay attacks can be mitigated in two ways:

- By cardholder approval or authentication: if the cardholder must approve each transaction or authenticate himself/herself at each transaction, then it is very unlikely, although not infeasible, to synchronize the rogue payment transaction with what the cardholder would see as a genuine payment. One way of enforcing cardholder approval could be the use of on/off switches on the PayPass card or on the PayPass-carrying device when other form factors than cards are used.

- By using an anti-relay transaction protocol validating strict timing constraints.

The former technique is not supported for reasons listed above. The latter would have a major impact on the card and terminal infrastructures. Hence, it is not supported in the current version of PayPass.

5.3 Risks to Other Environments

A number of countermeasures may be used to avoid that data captured from PayPass cards is used for conducting fraudulent magnetic stripe transactions or e-commerce transactions.

5.3.1 Use of PayPass-specific PANs

It is recommended that issuers use specific PAN ranges for their PayPass cards. Using such PANs ensures that PayPass sensitive data transmitted over-the-air are useless for the fraudster planning to perform fraudulent transactions in MO/TO or magnetic stripe acceptance environments.
5.3.2 Use of SecureCode

SecureCode implements a cardholder authentication mechanism. Hence, the capture of data from PayPass cards does not affect issuers using SecureCode.

5.3.3 Use of CVC2 for MO/TO

For a MO/TO transaction, as long as the merchant insists on CVC2 entry and uses the address verification service, the information obtained from eavesdropped or preplayed transactions is not sufficient for a fraudster to perform a transaction.

5.4 Lack of Cardholder Approval

Typically, cardholder approval may not be required to complete a PayPass payment.

The absence of a cardholder approval mechanism in the PayPass technology may result in:
- The conduct of fraudulent transactions without the cardholder’s consent,
- The capture of data without the cardholder’s consent, and
- DoS attacks on the card.

Note that, even when a cardholder approval mechanism is used, the cardholder has no means of verifying that he is approving the expected transaction. This is essentially linked to the absence of terminal authentication.

Without a cardholder approval mechanism, any reader device in proximity of the card may activate the card. The card may then perform certain actions, e.g. produce transaction data, increment its ATC, etc.

The absence of cardholder approval is therefore a vulnerability that needs to be taken into account. Note that if terminal authentication is performed, only legitimate merchants may use a reader device, and hence only fraudulent merchants may benefit from the absence of a cardholder approval mechanism unless sophisticated relay attacks take place.

There exist several methods of implementing cardholder approval:
- The use of on/off switches on the PayPass card or on the PayPass-carrying device when other form factors than cards are used
- The protection of the card from any energizing radio frequency field unless the cardholder removes this protection, e.g. an envelope around the card, a mechanism present in the wallet, etc.

While the former method would make the cards more expensive and less reliable, the latter method may efficiently be used to reduce the risks of data capture during mailing, while the card is in transit to the cardholder.
5.5 Lack of Cardholder Authentication

In the traditional face-to-face payment environment, a signature (or in some cases a PIN) is required for credit transactions and a PIN is (typically) required, for debit transactions. When PayPass technology is used, authentication of the cardholder is not required in order not to compromise the transaction speed and cardholder convenience. Cardholder authentication would considerably reduce the risk of the conduct of fraudulent transactions, as it would also prevent an illegitimate cardholder from conducting a transaction. However, this still does not ensure that the cardholder is really approving the transaction he thinks he is approving (this could partly be achieved through terminal authentication).

Several technical methods could be used to achieve cardholder authentication, for instance:

- The use of a PIN by the cardholder,
- The use of a biometric (e.g., fingerprint) verification mechanism at the card level, and
- The use of a biometric (e.g., retina) verification mechanism at the terminal level.

The implementation of such mechanisms in PayPass would make the cards more expensive, more complex to manufacture and less reliable, or it would increase the transaction time. Therefore, they are not explicitly supported in the current version of PayPass. However, with other form factors, the activation of the PayPass functionality may be subject to local cardholder authentication, based on the capabilities of the PayPass-carrying device.

5.6 Lack of Terminal Authentication

Terminal authentication may prevent the use of illegitimate coupling devices\(^1\) and ensure the confidentiality of data transmitted over-the-air. PayPass does not use terminal authentication, which is not a new vulnerability, or one specific to the PayPass technology. However, the vulnerability cannot be ignored since the introduction of this new technology may induce cardholder confusion. This vulnerability may have a greater impact when using PayPass technology than when using magstripe or chip technology.

A terminal authentication mechanism would be complementary to the two EMV-based techniques described in Chapter 3. The use of public key cryptography would obviously be the only practical solution for terminal authentication. This has a number of impacts:

- First, the need to store the terminal private keys would require all terminals to feature a tamper-responsive security module
- Second, a layered key management system would have to be implemented and managed, similarly to what is currently in place for the support of EMV offline card authentication method. In addition, while card revocation is relatively easy to support (by use of blacklists or certificate revocation lists at terminal level), a suitable terminal revocation mechanism is far more difficult to implement. Hence the issue of stolen terminals would have to be tackled by heavy logical and physical security measures, whose efficiency may be questioned.

---

\(^1\) At least, outside of relay attacks.
Using such a technique would have major impacts on the terminal infrastructures, and could have adverse impact on the card performance. Hence, it is not supported in the current version of PayPass.

5.7 Data Privacy

Because of the over-the-air nature of their interface to the payment terminals and because of the lack of terminal authentication, PayPass cards may expose cardholder identification data such as the card PAN or the cardholder's name. Such an exposure may raise privacy concerns, as separate purchases made with the same card can be linked, and potentially linked to individuals.

The protection of the card from any energizing radio frequency field unless the cardholder removes this protection, e.g. through a mechanism present in the wallet, etc may mitigate that risk. Similar measures, e.g. a special protective envelope around the card, might be used to protect the cards when in transit to the cardholder during the card distribution phase.

In addition, it is mandated that PayPass – M/Chip ‘Cardholder Name’ data element tag (‘5F20’) data do not include the cardholder's name.

5.8 Denial of Service

Measures aiming at protecting cards from any energizing radio frequency field when not in use (similar to the ones described in section 5.7) may be used to mitigate DoS risks.
6 Conclusions

When properly implemented, PayPass M/Chip offers a suitable and ‘fit-for-purpose’ trade-off between functionality and security. It delivers the full convenience of tap-and-go payments without any significant impact to acquirer or issuer infrastructure, while providing adequate security. This is achieved through the use of EMV-based card authentication mechanisms, designed to comply with chip transactions requirements. The possible attack scenarios that then remain are generic for transactions that are without cardholder authentication.

The EMV-based card authentication techniques ensure an appropriate level of security for the PayPass technology. The following recommendations are good practices to mitigate risks in general:

• The PAN range for PayPass should be separate from the PAN range for magnetic stripe and contact chip
• SecureCode should be used for electronic commerce transactions

The following additional recommendations are good practices to mitigate risks in general:

• The PAN range for PayPass should be separate from the PAN range for magnetic stripe and contact chip, and
• SecureCode should be used for electronic commerce transactions.

**** End of Document ****