



White Paper

Smart Cards for Payment Systems

An Introductory Paper describing how Thales e-Security can help banks migrate to Smart Card Technology

Background

In this paper:

- Background* 1
- The Solution* 2
- How Thales e-Security can help banks move to Smart Cards* 3

The payment card has been in existence for many years. It started in the form of a card embossed with details of the cardholder (account number, name, expiration date) which could be used at a point of sale to purchase goods or services. The magnetic stripe was soon introduced as a means of holding more data than was possible by embossing alone. The magnetic stripe also allowed cardholder details to be read electronically in a suitable terminal so that checks could be made with little or no human intervention about the cardholder's credit-worthiness or whether the card had been reported lost or stolen.

Card technology has advanced over the years to keep ahead of the worldwide increase in card related crime. As the criminal fraternity found ways of producing sufficiently good counterfeit cards, so the card companies introduced new ways of combating the problem. A succession of anti-fraud measures have been introduced over the years such as the hologram, the Card Verification Value (CVV, a value stored on the magnetic stripe which can be used to determine if a card has been produced illicitly), and in some cases, photographs of the cardholder.

Magnetic stripe cards have now been developed to the point where there is little or no further scope for introducing more anti-crime measures. This has caused the card associations to look at new technologies to take the plastic card into the 21st century. One technology which offers many benefits is the smart card; essentially a small computer chip embedded into a plastic card with the same dimensions as the magnetic stripe card. The only difference the cardholder sees is a small metal area on the face of the card which contains a set of electrical contacts through which the chip can be accessed.

From the anti-crime perspective there are a number of benefits in adopting the smart card. The card itself (or in conjunction with the terminal) can make decisions about whether or not a transaction can take place. Secret values can be stored on the card which are not accessible to the outside world allowing for example, the card to check the cardholder's PIN without having to go online to the card issuer's host system. Also there is the possibility of modifying the way the card works while it is inserted in a point of sale terminal even to the point of blocking the card from further transactions if it has been reported lost or stolen.

As well as these anti-fraud measures, the smart card is seen as offering a number of other benefits to the card issuer and cardholder. These additional benefits are an integral part of building the business case for introducing smart card technology. Some of the other benefits of introducing smart cards are:

The ability to have more than one payment application resident on the card. For example a card could contain an “electronic purse” to provide the equivalent of cash, usually for lower value transactions such as parking, tickets, newspapers etc.

The ability to have other applications such as loyalty schemes and access to information facilities (e.g. libraries) co-resident on the card.

The possibility of reducing on-line validation costs by allowing the card to operate off-line more of the time.

In the future there may be the possibility of storing personal details such as driving license and medical records on the card.

There are many issues to be resolved before such all-embracing cards become common place, the most obvious ones being who owns the card and who controls which applications can be loaded or deleted.

Today, the banks are interested mainly in providing payment related services to their customers and most of the current activity surrounds the provision of smart card based credit/debit services sometimes with an additional electronic purse facility.

The Solution

EMV Specifications

In the early 90's the major card associations (Europay, MasterCard and Visa) recognized that for smart cards to become acceptable, it was necessary to standardize the way they work, at least for banking applications. Considerable work was undertaken to reach agreement on a standard culminating in the so-called Europay MasterCard Visa (EMV) specifications. These specifications define the physical characteristics (size, shape, thickness, position of contacts), the electrical characteristics (signals to be fed to each contact), command set (how to access data and functions on the card), overall card security methodologies (static data authentication, dynamic data authentication) and the data to be stored on cards for payment systems. The EMV specifications do not fully describe particular payment applications, that being left to individual card associations to define. They do describe the basic framework under which all payment applications will work.

It is important to appreciate that while the EMV specifications describe how cards, terminals and host systems interact, they do not describe how cards will be personalized, since different card manufacturers use different methodologies. This is one area where Thales e-Security and its partners can offer products to assist issuing Banks.

Visa Specifications

Smart Debit/Credit

Visa has produced a specification which deals with the details of how a credit /debit application will operate in a Visa world. This is known as the Visa Integrated circuit card (ICC) Specification (VIS) and is currently at version 1.3.1. This specification refers to an application called Chip Card Payment Service (CCPS). This name is gradually being replaced by the term Visa Smart Debit/Credit. There are plans to introduce Visa Smart Debit/Credit into a significant number of countries over the next few years.

Visa Cash

The Visa electronic purse product is called Visa Cash. It is available in two basic forms; disposable and reloadable. There are two types of reloadable Visa Cash cards; the DES-based version and the public key version. The public key variant offers improvements in security since the public key algorithm is implemented on the card itself. Visa Cash is in use in many different countries around the world.



MasterCard Specification

MasterCard has released a set of specifications describing their product which they call Debit and Credit on Chip. These are functionally equivalent to the Visa VIS specification although there are small variations.

MasterCard plan to implement Debit and Credit on Chip on the Multos open platform card.

The MasterCard electronic cash product is the Mondex purse. This can co-reside on the same Multos card as Debit and Credit on Chip.

Other Specifications

In the UK the Association for Payment Clearing Services (APACS) has developed a specification detailing the chip credit and debit features which will be implemented in the UK. This is known as the UK ICC Specification (UKIS) and is effectively a subset of the Visa VIS specification. UKIS does not implement the PIN on the card feature since PINs at point of sale are not used in the UK.

It is understood that Europay is developing a credit/debit smart card scheme.

How Thales e-Security can Help banks move to smart cards

In order to migrate to smart card based payment systems, Banks will have to make a number of changes to their existing systems. Among these are:

Enhancements to the card issuing process. Existing systems were developed, often many years ago, to handle the types of data needed for magnetic stripe cards. Smart cards require considerably more data to be generated including cryptographic keys for the cards themselves. In most instances changing existing systems represents a major investment of resources. Thales e-Security can offer a product to enable Banks to achieve this migration with the minimum of change and in some cases, no change at all. The product is called the Personalization Preparation Process or P3 and is described in detail later in this document.

Enhancements to the card personalization process. Banks generally personalize their cards in one of two ways; either using an in-house facility, or using an external personalization bureau. The choice will usually be based on the size of the cardholder base, since setting up an in-house facility is an expensive exercise. Thales e-Security has been working closely with the DataCard Corporation in the USA who produces a range of personalization machines for smart cards. Thales e-Security's products form an integral part of the smart card enabled DataCard systems.

Enhancements to the systems, which handle card transactions. Systems are in place today for handling a number of magnetic stripe based transactions such as ATM cash dispensing, on-line card and PIN verification, and offline bulk transaction processing. Using smart cards there is a need to extend these systems to handle the transaction verification mechanism used in smart debit and credit cards, or in the case of electronic purse schemes like Visa Cash to handle the secure loading of e-cash onto the card. Thales e-Security has developed the required functionality into its range of Host Security Modules to allow this processing to take place securely. This functionality is described in more detail below.

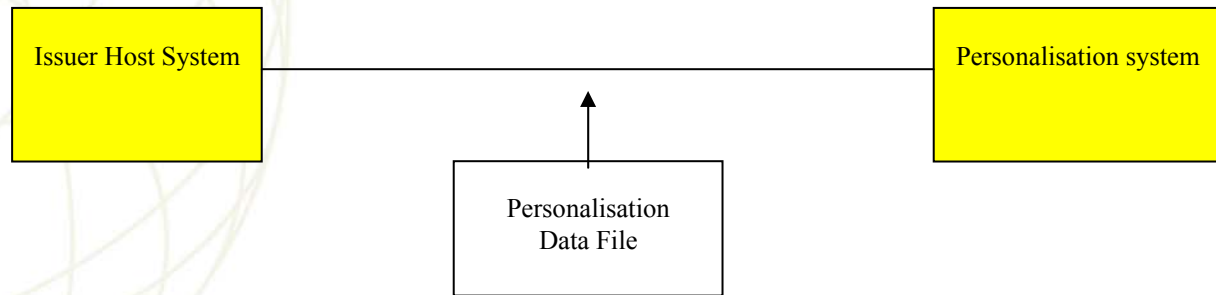
The Personalisation Preparation Process (P3)

The existing Magnetic Stripe Process

Today's magnetic stripe cards are generally produced as depicted in the diagram below. The Issuer Host System embodies the database of all cardholder details and provides facilities to generate data to produce a new card. Often cards are produced in batches and it is the



responsibility of the host system to assemble all data for a given batch of cards. A batch might be generated as a result of the normal re-placement cycle (2 or 3 years) or possibly to replace those cards which have been reported lost or stolen during the day. The host system produces the data in a series of records, one record per cardholder. The data is known as the Personalization Data File.



Each record of the Personalization Data File comprises a number of modules. These would normally include:

- i) Data to be embossed onto the card.
 - ii) Data to be encoded onto the magnetic stripe of the card.
- Data to be printed on a “paper carrier”. This carrier is used to hold the card whilst in its delivery envelope and would be printed, for example, with the cardholder’s name and address.
- Another possible module might be:

- iv) Data for an ID photograph

Most of the information for these modules is held in the cardholder database. Some items in the magnetic stripe module need to be generated using a security module. These include the PIN Verification Value (PVV) or equivalent, and the Card Verification Value (CVV). Both these items are derived using a cryptographic process which involves the use of secret keys. Thales e-Security produces a range of Host Security Modules (HSMs) which are suitable for this purpose and are in use by many card issuers worldwide in their existing magnetic stripe systems.

It is worth noting that while the data in the Personalization Data File is normally handled carefully, there is nothing inherently secret about it and for that reason it is not normally encrypted. It only becomes a useful commodity when it is combined with a real plastic card which happens in the personalization bureau. Such facilities are highly secure establishments with tight access control procedures and many internal mechanisms to guard against finished cards being lost or stolen. Normally cards in their paper carriers are inserted directly into envelopes and passed straight to the postal system. The PIN mailer for a card is normally produced in a separate establishment from the cards themselves often as a separate output from the Issuer host system. This separation of PIN mailer and finished card is normally an essential part of the card issuance process. Often PIN mailers are not posted until the cardholder acknowledges receipt of the card.

With the arrival of the smart card the Issuer needs to produce an extra “module” of data; that which is intended to be programmed into the chip itself. Of course there will be many items of information in this chip data which are common to the magnetic stripe and the embossing data. Examples of this are the Primary Account Number (PAN) and the cardholder name. However there are some new items which are specific to smart cards. Some examples of these are:

- a) Upper Consecutive Off-line Limit. This is a value held by the card which determines its spending limit. Once this limit has been exceeded, the card forces the transaction to be completed on-line. This is part of the inherent risk management features of a chip card.



- b) Signature of static card data. This is a value calculated using a public key cryptographic algorithm at the time the card data is generated. It can be validated by each terminal accepting the card and is used to give some confidence that the card is genuine.
- c) Issuer Certificate. This data is set up by the Issuer in conjunction with the card association to which the Issuer belongs (e.g. Visa or MasterCard). It is placed onto every card issued and contains the public key of the Issuer. It is used by the terminal as part of the process to validate the signature in item b above.
- d) Unique Derived Keys (UDKs). These are DES keys, unique to each card, which are placed on the chip and used as part of the transaction validation process. Basically the transaction details are passed to the card, which uses the UDK to generate a cryptogram (similar to a MAC) which is passed back to the Issuer for validation. Using this technique, the Issuer can be sure that the transaction was handled by a valid card.

The various credit and debit specifications define in excess of 40 such data items which need to be generated and placed on smart cards. It is the Issuer's responsibility to generate these items, something which existing card systems were never designed to handle.

Note that the advent of chip cards has meant that for the first time, some of the data passing from Issuer to Personalizer is now secret and must be only be sent in encrypted form. The UDKs described above are an example of such secret data.

The Thales P3 System

Thales e-Security has recognized that there is a need for a product which is able to generate the new data required by the various smart card schemes. This means that a Card Issuer can migrate to smart cards without having to make changes to an existing cardholder database host system. As noted before this can be a costly and time-consuming exercise and often proves to be a major barrier for a Bank in moving to smart cards.

P3 is a compact name for Personalization Preparation Process which goes some way to describing what the system achieves. Its main objectives are:

To take an existing Personalization Data File in an industry-accepted format and adds to it the extra data required for the smart card scheme concerned. Currently P3 supports the Visa Cash scheme (Public Key or DES-based variants), the Visa "Easy Entry" scheme, the Visa Smart Debit/Credit scheme and the UKIS scheme. P3 will be enhanced to support other schemes in the future.

To achieve the above it stores securely all the cryptographic keys and certificates required by the above schemes. It uses a Thales Host Security Module to provide a secure cryptographic processing environment for these keys.

To generate Issuer Public and Private Key sets (RSA public key algorithm) and to get the public key into a form where it can be sent to the scheme's Certification Authority (CA) so that it can produce the Issuer Certificate. The certificate so produced can be imported back into the P3 system and stored for use in the personalization preparation process.

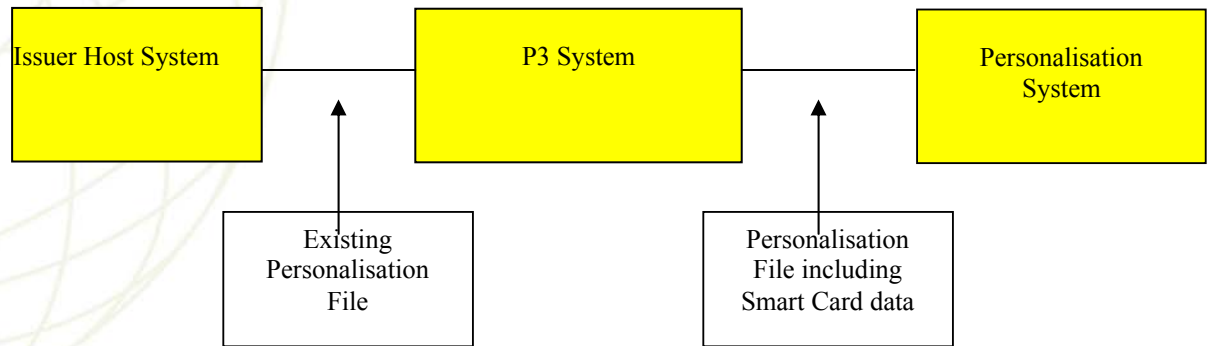
To produce the output data in a format which can be used by the DataCard 9000 system used by most card personalization bureaus around the world. Sensitive card data such as keys are encrypted in the output stream.

To store details about regularly performed jobs so that record processing can be performed with the minimum of user intervention.

To provide a security environment with controlled access which aligns with the operating procedures found in many personalization bureaus. Using the security features of Windows NT, a P3 user can set up system managers, administrators and operators to perform the required tasks for normal operation.

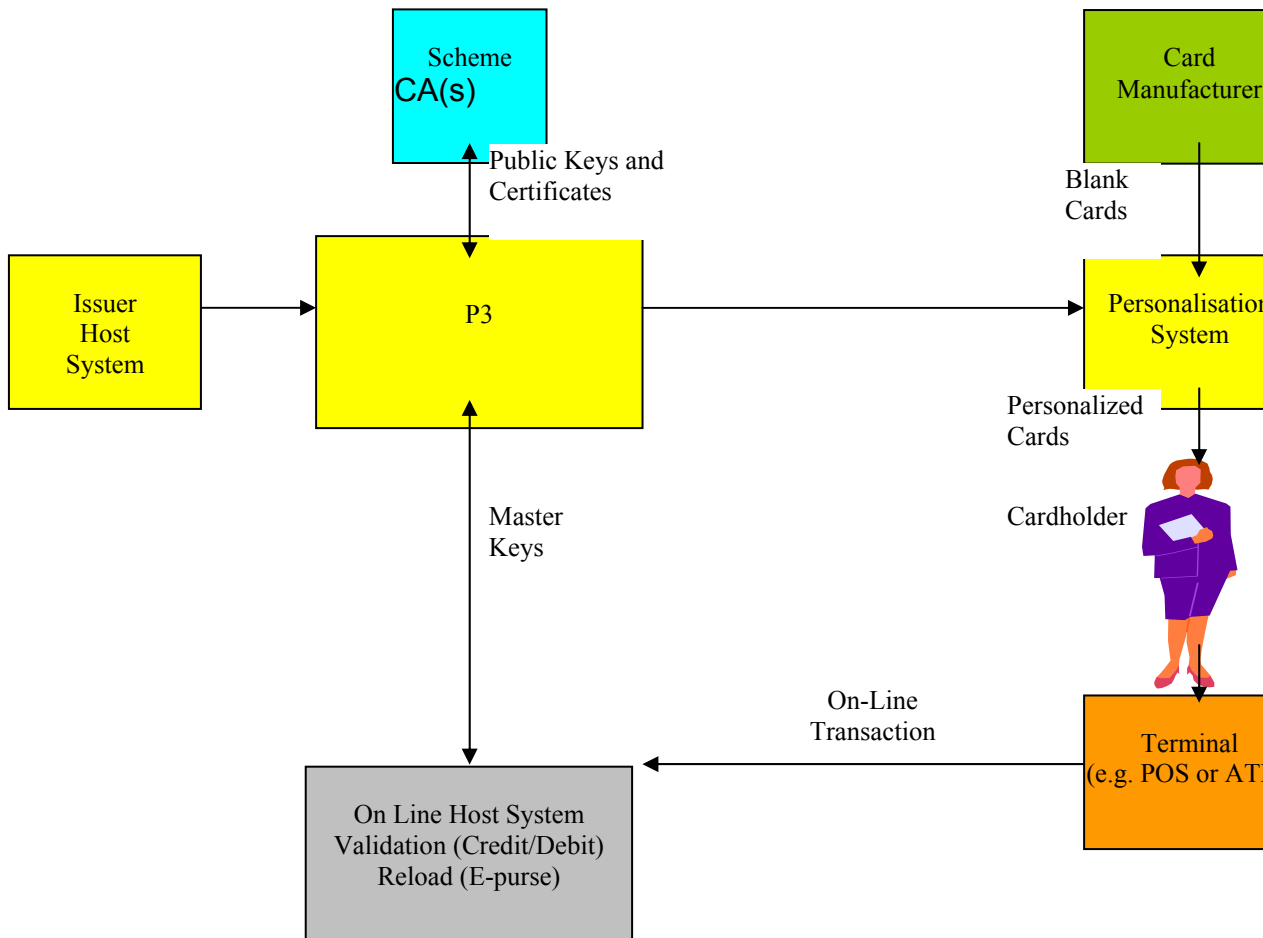


The P3 system fits into an existing card issuing process as shown in the diagram below.



There are two possible configurations of P3. It could belong to, and be co-sited with the Issuer Host system. Alternatively P3 could be operated by a Personalization Bureau who may act on behalf of several Issuers.

In order to perform its job, P3 needs to be able to interface with a number of external parties. These interfaces are shown in the diagram below.



The parties that P3 shares information with are:

Scheme Certification Authorities (CA). Part of the security of the various smart card schemes includes the need for an Issuer to generate an RSA public/private key pair. The private key is

retained securely in a Host Security Module and used to “sign” card data to produce a signature which is placed on the card. The public key is transmitted to the scheme provider (e.g. Visa, Europay or MasterCard) where it is certified using the “scheme private key” to produce the Issuer Certificate. This is transmitted back to the Issuer where it is stored so that it can be placed on every card. The certification process is slightly different for each of the Scheme Providers but the principle is the same.

Issuer Host System. P3 receives personalization data from the existing Issuer Host System as described in other parts of this document

Personalization System. P3 adds the appropriate smart card data to the cardholder record before passing the combined data to the Personalization system.

Once cards have been Issued, they may be used to obtain goods or services. If the card is a Credit or Debit card, it is generally used at a point of sale or at an ATM. As part of the transaction, the card generates an Authorization Request Cryptogram (ARQC) using unique keys held on the card. This is passed back as part of the transaction message to be validated by the bank’s host validation system. The host system is able to validate the ARQC and produce an Authorization Response Cryptogram (ARPC) which is sent back to the card. The card can validate this ARPC. This mutual authentication process gives a very high assurance that the card is genuine, and that the bank with which it is in communication is the one which issued the card originally.

If the card is an electronic purse card, normal purchases are carried out as off-line transactions. However there is a need to go on-line when the card is to be re-loaded with funds. In the case of Visa Cash, a card generates a Load Request which involves a cryptographic signature known as S1. This is validated by the host system which then generates the Load Authorization signature (S2). The card validates this and finally produces a Load Completion Signature (S3) which is send back to the host system to confirm that funds have been loaded.

Both the above on-line transaction processes involve cryptographic keys. These keys have to be shared between the on-line host system and P3. Facilities are provided in P3 to allow this.

At the time of writing, the Thales P3 system is able to support the following applications. Work is in progress on others applications which will be announced in due course.

Visa Cash (DES-based)

Visa Cash (Public Key)

Visa Easy Entry

Visa Smart Credit Debit

APACS UKIS application

The P3 system uses a Thales Host Security Module equipped with the RSA public key algorithm to provide security for all keys.





Smart Card Credit and Debit processing HSM Functions

As outlined above, an on-line host system handling credit and debit transactions from smart cards needs to be able to process the ARQC/ARPC values. Thales e-Security has implemented these algorithms in its RG7000 series Host Security Modules. These are available today.

Visa Cash Load and Unload processing HSM Functions

To be able to handle the Visa Cash Load (and Unload) functions, the on-line host system must be able to handle the S1, S2, and S3 signatures as described above. Thales e-Security has implemented these algorithms in its RG7000 series Host Security Modules. These are available today.



EUROPE, MIDDLE EAST, AFRICA THALES e-SECURITY LTD.

Meadow View House
Long Crendon, Aylesbury
Buckinghamshire, HP18 9EQ, UK
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
e-mail: emea.sales@thales-esecurity.com

AMERICAS

THALES e-SECURITY, INC.
2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
e-mail: americas.sales@thales-esecurity.com

ASIA PACIFIC

THALES e-SECURITY (ASIA) LTD.
Asia Pacific
Units 2205-06, 22/F Vicwood Plaza,
199 Des Voeux Road
Central, Hong Kong, PRC
Tel: +852 2815 8633
Fax: +852 2815 8141
e-mail: asia.sales@thales-esecurity.com