



White Paper

Personalisation Preparation

The changing face of the Payment Environment

Introduction

In this paper:

- Introduction* 1
- The Changing Environment* 2
- Card Issuer Migration Strategy* 3
- Conclusions* 10
- The Thales e-Security Personalisation Preparation Process* 10

The magnetic stripe based bankcard is now familiar and widely used. It provides simple yet popular applications such as credit, debit, and cash withdrawal and cheque guarantee.

The production of cards has been very simple, and the degree of issuer and user information they hold only basic. For example a standard branded card (Europay, MasterCard, Visa, American Express etc.), has magnetic stripe, embossed data, indent data and (optionally) a hologram and a photograph.

In a conventional card issuing environment, the magnetic stripe and embossing data are normally produced by the card issuer; of this data only the PIN Verification Value (PVV) and the Card Verification Value (CVV) are cryptographically generated. This is normally carried out on the issuer's card production systems prior to the production and issuance of the actual plastic card.

Magnetic stripe cards provide limited functionality, supporting typically one or two functions. The issuer has dictated fixed functions rather than providing individual customer choice.

Another significant drawback with magnetic stripe bankcards is that they can be easily counterfeited and used fraudulently. This is a major problem for card issuing organisations worldwide, with millions of dollars being stolen, either by fraudulent use of the card in retailers or withdrawal of cash from Automatic Teller Machines (ATMs). The financial community has, for many years, been looking for an alternative to the magnetic stripe card to help the fight against ever-increasing levels of fraud.

The various global retail payment associations, of which all issuing organisations are members, have assessed many technologies, and the smart card has become the natural successor to the magnetic stripe card. The reasons for this are many and varied, falling into four main categories: -

Multiple Applications

With the issuance of smart cards, with memory storage capacity, it will be possible to provide support for multiple services, on one card, thus allowing the customer to have one or two cards instead of the multitude of cards they carry today. Additionally, cards can have applications loaded remotely at a later date at the customer's request.

Fraud Reduction

A microprocessor-based smartcard with secure memory storage is extremely difficult to copy and use fraudulently.

Offline Decision Making

As the smart card is microprocessor based, it has the ability to make decisions in line with the rules programmed into the chip, without having to go on-line to the issuer's host system. This allows cards to be used more securely in countries with poor telecommunication infrastructures.

Online Control

An issuer can control the usage of the smart card after it has been issued. For example, a person may become a bad credit risk so that when the card next goes online for verification, the issuer can send a command to the card to delete the credit application from the card, thereby removing the credit facility from the cardholder immediately. This allows the issuer to manage 'risk' with greater flexibility and control than was previously possible.

The Changing Environment

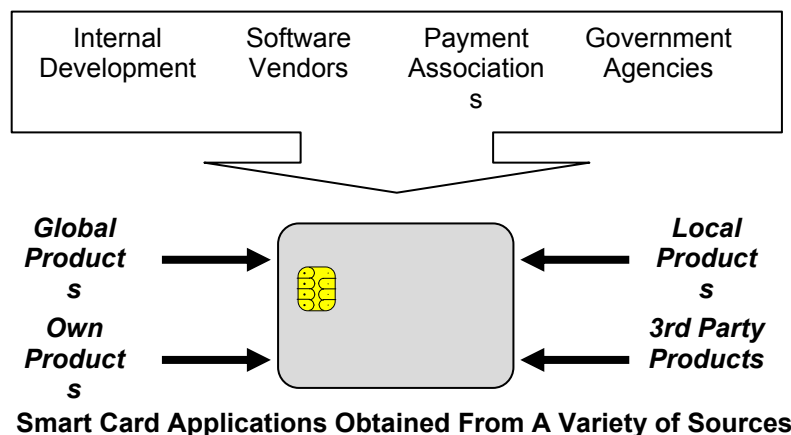
There are significant benefits to be made from the use of smart cards, including financial rewards, improved security and greater perceived benefits to the cardholder. Card issuers that are at the forefront in adopting smart card technology will reap the rewards.

Because of the flexibility and improved security of the smart card, it is attractive in many vertical market segments, for example: -

Financial Applications - Debit, Credit, Electronic Purse, Authentication etc.

Government Applications - National ID, Health Card, Driving Licence etc.

Telecommunication Applications – Stored Value Money, Value Added Applications etc.



As more organisations begin to realise and understand the benefits of smart cards and their potential applications, and with supporting technologies converging to become standardised, more are beginning to investigate the benefits of smart cards. This includes implementing trials and in certain circumstances full roll-out programmes.

Unfortunately, few card issuers yet appreciate how best to capitalise on the potential of smart cards. From a business perspective, issuing organisations can use personal customer data they already have in conjunction with the power of chip-based cards, to allow them to offer their customers a much better and more personalised service. In future customers will be able to have cards that reflect the individual's lifestyle as opposed to a standard card product type. This will enable the issuing organisation to capture and consolidate market share, as customers perceive greater personal benefit, and therefore value, promoting greater usage of the card. The smart card will also provide greater levels of security than are currently afforded with today's magnetic stripe technology. This will allow card issuers to provide customers with highly individual cards that can carry personal and private data, which can be used in a variety of applications.

Smart cards will have increasing memory and processing power. Unit costs will fall and acceptance will grow. All of these factors will contribute to an increasing role in everyday life. Gone will be the days when typically the cardholder possessed only payment cards (branded and private label). A new era is dawning where one can perceive users holding a reduced number of multiple application smart cards supporting a wide variety of applications that include payment applications, health details, social security information etc. There are many commercial issues to be addressed before this indeed can become reality, not least the issue of card branding. However the technology is here today to support such concepts.

Card Issuer Migration Strategy

When moving from magnetic stripe to smart card based implementations, there are many business and technical issues, which need to be addressed by the card-issuing organisation. Many issuers have fallen into the trap of believing that the issuance of smart cards is simply a more advanced version of the processes required for the magnetic stripe card. To do this is to both misunderstand and ignore the potential of smart card technology.

There are many complexities involved in moving to smart cards, from the initial issuance of the card to the on-going card management. This is especially important when an organisation wishes to offer their cardholders the ability to load and delete applications and data dynamically from remote locations. There are many factors that an issuer must consider before issuing smart cards, including: -

Migration Strategy

Even though organisations are moving towards smart cards, there will be still be a place for magnetic stripe cards for many years to come and no doubt also for specific applications.

Most organisations that wish to issue smart cards will have an existing magnetic stripe card management infrastructure. It is very unlikely that any organisation is going to completely replace the existing infrastructure, but will implement solutions that are complementary and will provide support for new product types. Therefore, a decision has to be taken whether to support smart card issuance and management on the existing host based card application suite, or implement a totally new approach.

Host Implementation

There are many advantages in implementing smart card management and personalisation preparation processes on existing mainframe card management systems, such as having a



single software suite for all card applications, control and management are harmonised onto a single hardware platform.

A card-issuing organisation must consider whether this is a pragmatic approach to smart card issuance, as it is very different from the processes employed today. Smart cards are rapidly evolving and this means that host applications will have to be continually developed to exploit the new advances in the technology.

Server Approach

Should the card issuer modify the existing card management system, especially when considering the ever-increasing number of smart card technologies and applications that will need to be supported?

Many organisations will start with a small volume of cards, probably for a pilot or trial scheme. This will allow the issuer to test and understand the technology, and it will provide the issuer with 'hands-on' experience and better understanding of the business benefits that can be achieved. However, when the trial moves to a full role-out phase, the issuer needs to ensure that the smart card management system is flexible and it can grow and meet the increasing business demands. A server-based approach can meet these requirements.

The server approach allows the issuer to develop additional support, as and when required, for new applications and technologies, in an environment that is isolated from the back office.

No matter which approach is adopted, the issuance system architecture must be flexible enough to support the new and emerging technologies and applications as and when they arrive and when the business or the market identifies a need.

Card Life Cycle Management

A major feature of any system must be card life cycle management. As multi-application cards become more common in the market with more variety and choice of applications, and as post-personalisation of applications onto issued cards becomes reality then issuers need to keep track of the applications that have been loaded onto cards. This is essential should the cardholder require a replacement/renewal card.

The management of multi-application smart cards is a complex process. The card management system will need to keep an account of the following information: -
Smart cards issued – Type/manufacture, memory capacity, applications loaded into ROM etc.
Card Application Profiles – Which products are to be supported on the card product types
Card Production Data – Data elements necessary to produce cryptograms for loading of applications and associated data for all supported card types
Application Parameters – EMV data parameters for financial product types (i.e. classic, gold, platinum cards) and non-brand data parameters

It will be the responsibility of the card life cycle management system to hold all information about the smart card types, details of issued cards, the data definitions for generation of smart card application data and full details of product types supported by the issuer. The card life cycle management system is a unique application. It is one of the few entities that needs to understand, not just the smart card profile and parameters, but also that of the business applications. It is one of the areas where the technology and business requirements have to work hand-in-hand.

The card life management system provides all the input details and data definitions that will be required by the personalisation preparation process to create the data to be loaded onto the target smart card.



Personalisation Preparation of Application and Cardholder Data

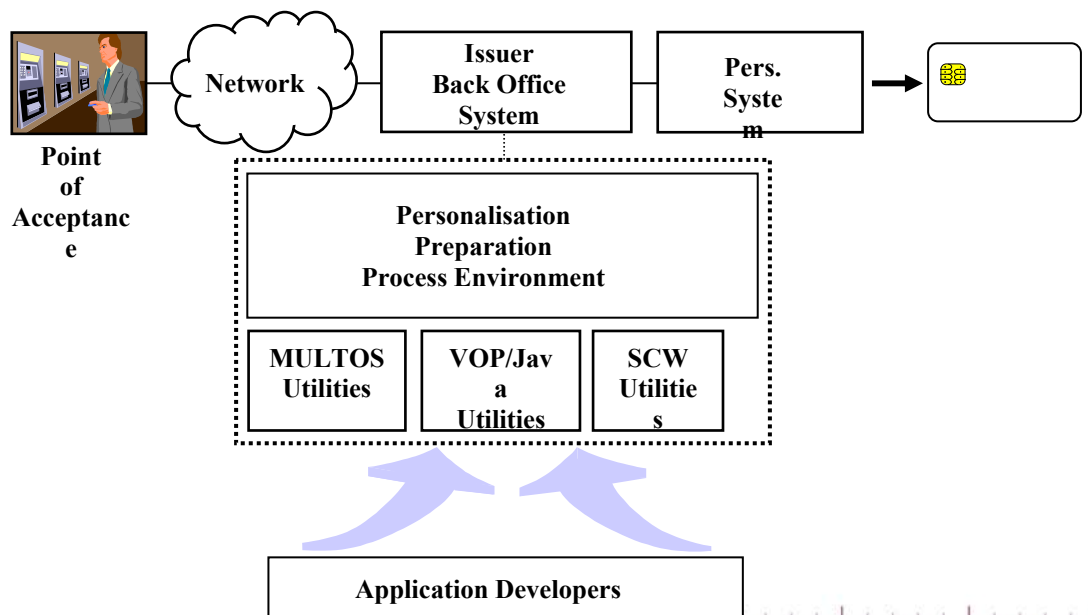
No matter which migration strategy is adopted, the creation and personalisation of the application and the cardholder data is a critical factor for smart card issuance. Unlike the traditional magnetic stripe card, there is a cryptographic framework for the generation and personalisation of the cardholder data, and this tends to be different for each global payment brand and smart card platform type.

The requirements for personalisation preparation are sometimes defined within the smart card issuance architecture being promoted by the brand/smart card developer. However, in the majority of circumstances this is not the case and the issuer is faced with assorted smart card platforms requiring different data generation and creation processes. This situation will become more complicated as more applications are offered to the market by different smart card application developers.

Each smart card, depending on which scheme it supports (i.e. MULTOS, Java, SmartCard for WINDOWS, Proprietary, etc.), requires that the data on it be formatted before the cryptographic security processes are applied, prior to the secure onward transmission to the personalisation system. Only when the data has been loaded onto the card will the issuer be in a position to test the card and its applications. If the personalised smart cards fail, potentially the issuer could end up with cards that are only good for the 'trash can'.

The type of personalisation data required for applications can be varied. On the one hand a smart card application may require basic information in order to initialise the application (e.g. anonymous loyalty), other applications, such as EMV financial applications, may require secure issuer and specific cardholder data. No matter what types of applications are required for the smart cards, it is important that an issuer implements standardised processes. An issuer must implement processes that support the various smart card product types that are commercially available and also provide for an integrated personalisation preparation framework. This must allow the issuer to acquire applications from any source (i.e. global payment brand, smart card application developers, in-house development etc.), and provide the means by which the issuer can standardise the personalisation preparation of the smart card application and cardholder data.

If an issuer does not adopt this approach, then potentially he will end up with multiple copies of personalisation preparation software for each application, application version and card product type that he intends to support. This may not be seen as an issue in the early stages, as few applications will be supported, but will become a major management issue as applications and card platform types increase.



When considering how to implement and support personalisation preparation there are many issues that a card-issuing organisation needs to consider, including: -

Personalisation Preparation Application Development

Every organisation that wishes to issue smart cards will have to decide whether to develop their own personalisation preparation application or purchase a commercially available solution. No matter which option the issuer chooses the following will have to be taken into consideration.

- If developed in-house, does the issuer have the resources to keep pace with the changes in smart card technology?
- Does the solution provide a generic personalisation preparation framework that will allow the issuer to obtain applications from a variety of other external sources?
- Does the issuer have the knowledge and understanding of the smart card platforms that will be issued and how to generate data for each platform and application type?
- Will the application/system support the immediate and long-term business requirements?
- How will the issuer cryptographic security requirements be supported, not just for the applications but for the overall key management?
- Is the personalisation preparation process able to support multi-applications and multiple smart card types?
- Does the system support centralised, distributed and post-issuance services?
- Is the personalisation process compatible with personalisation equipment manufacturer's systems?

Secure Issuer Key Management

An inherent part of the personalisation preparation is key management. The cryptographic framework for data generation and the issuance of smart cards is very different from that of the traditional magnetic stripe card. An issuer of financial branded applications will need to implement a hardware based key management system. Depending on the applications and smart card platforms being supported, the issuer will typically need to carry out the following key management functions and processes: -

- Generation of public key material and associated data for certification by the scheme/brand provider
- Public and private key generation for card applications
- Creation of card certificates
- Secure dissemination of keys to other entities within the scheme
- Import/export of key material

The key management system will need to provide the interface between the card issuer and the scheme/brand to allow the issuer to be certified to issue cards under the scheme rules. This is especially relevant for financial branded cards. Additionally, the issuer will need to generate all the cryptographic key material required for the various applications that are supported and, where necessary, share the key material securely with other entities within the scheme.

Smart cards offer a greater level of security than traditional magnetic stripe cards. The microprocessor-based card is more difficult and more costly to copy and counterfeit than today's card and therefore, provides an efficient tool to combat card fraud. It is important that the issuer implements a secure key management system that provides the right level of security, both physically as well as for the key generation/distribution. Ultimately, if cards can be copied, or key material exposed, the issuer, card brand and application will suffer not only from the fraudulent consequences, but will risk losing the confidence of their users.

Generic Smart Card Personalisation Preparation Framework

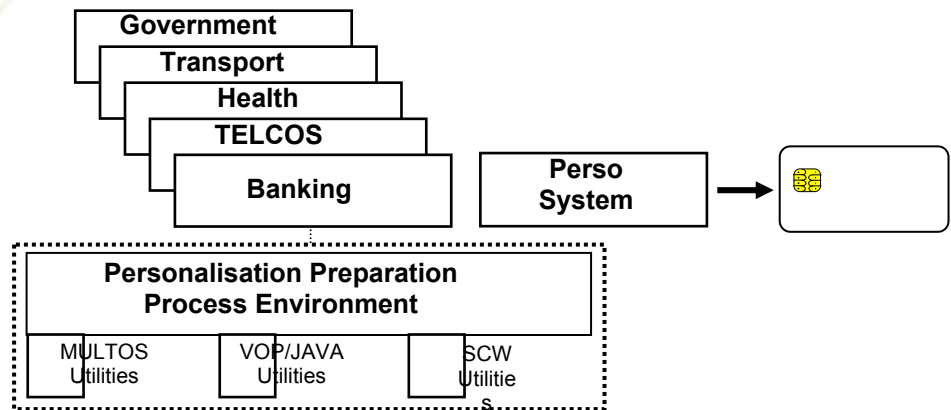
Although issuers currently talk about the issue of fixed functionality smart cards, the future is multi-application smart cards. They provide a better business case and allow the issuer to support, not only core applications but also additional value-added applications. This will



bring increased benefits both to the issuer and the cardholder. It will allow the issuer market differentiation for his products.

An issuer has to ensure that whatever solution is decided upon, it has the flexibility to support the business requirements today and in the future. This is not easy in a market that is in a continuous state of change, with new applications, key management schemes, personalisation processes and smart card platforms constantly being brought to market.

One step that an issuer can take to protect his investment in smart card technology is to implement a generic personalisation preparation framework, thus ensuring that whenever new applications or smart card platforms need to be supported, the framework has the flexibility and capacity to handle them.



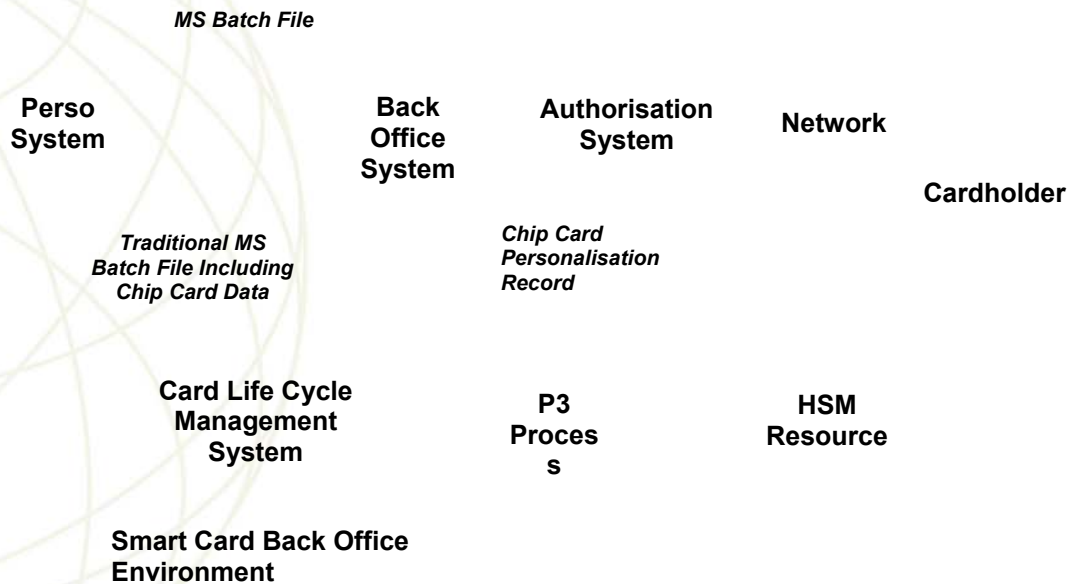
Personalisation Preparation Framework

Central, Distributed & Post Issuance

Until now the majority of cards have been centrally issued. However, with multi-application smart cards this model will change. Many issuers are talking about the ability to issue cards securely at remote sites and also provide post-personalisation services to the cardholder.

This means that the personalisation preparation process will need to be an integrated part of the back office environment, able to provide personalisation data in a real-time environment. When an issuer considers the implementation of a personalisation preparation process, he needs to ensure that it will support the issuance model that exists today, but also has the flexibility and capacity to offer new services to the business. The personalisation preparation process must have suitable interfaces for its integration with the back office environment.





Cost of Ownership

The similarity between the issuance process for smart cards and traditional magnetic stripe cards is limited, and this will become more marked with multi-application smart card platforms. When considering the issuance of chip cards for the first time, usually for a pilot implementation, an issuer will have two options available. Either they can contract with a third party bureau that will provide all the personalisation preparation and physical personalisation services for central issuance of the cards, or they can implement the personalisation preparation process in-house.

Third party bureaux offer total 'turn-key' personalisation services to issuers. This is an attractive option for an issuer who is about to issue smart cards for the first time. However, before embarking on this course of action, there are other factors that need to be taken into consideration. These include: -

Is the third party bureau offering the issuer service level guarantees for the issuance and replacement of smart card and, if so, are they acceptable and do they meet the business requirements?

Is the cost per card acceptable, especially for low volume issuance?

Will this option bring maximum benefit to the issuer or would greater benefit be gained from learning about the issuance and management of smart cards in a controlled environment (i.e. pilot) rather than in a full roll-out?

If the issuer is issuing cards with sensitive applications (i.e. financial), are they happy to have a third party organisation generate and manage the cardholder and issuer data (possibly including the cryptographic keys).

The second option, implementing an internal system, may seem unattractive, especially where a low volume of cards is going to be issued. However, as well as considering the above, the following need to be taken into consideration: -

If only a low volume of cards is to be issued, is it justifiable to implement in-house processes?

Is there a business case that supports waiting until a larger volume of cards is to be issued?

Can the issuer gain valuable experience by implementing the processes himself during a pilot scheme?

Organisations need to understand all the issues surrounding the management of card stock, key management, issuance processes and the card life cycle management quickly, for them to succeed with this new technology.



Smart Card Personalisation

Card personalisation for traditional magnetic stripe cards has been well understood by issuers for many years. The personalisation system accepts a batch file from the issuer, which contains all the individual card records, typically comprising magnetic stripe information, embossing data, carrier information (cardholder name and address) and, optionally, other information (photograph etc.). When producing magnetic stripe cards, the security requirements are dependent on the management and control of the card stock. There is no cryptographic security processing required during the personalisation stages as the cryptographic security data (PVV, CVV etc.) has already been pre-calculated by the issuer prior to sending the card data.

However, this picture changes when smart cards need to be personalised. Existing personalisation equipment will need to be upgraded to support the personalisation of chip cards. In most cases this means the addition of a smart card programming module which is installed, in line, into the personalisation system. Smart card personalisation is a secure process. Unlike traditional magnetic stripe card personalisation, there is a final round of cryptographic processing required to load the application, and issuer and cardholder data onto a smart card. When smart card information is received at the personalisation system from the personalisation preparation process, the data has been encrypted and contains a Message Authentication Code (MAC), to provide data integrity.

Cards held at the personalisation system, have been 'locked' using a transport key(s) during the manufacture and initialisation processes. Smart cards will only accept encrypted data for loading data, which has been encrypted using the card transport key. As with the personalisation preparation process, the cryptographic processing should only be carried out within the confines of a secure tamper-resistant security module.

Most cards issued today, especially by financial institutions, are issued via a central bureau, whether it is an internal facility of the issuer or provided by a third party organisation. This traditional approach to card issuance will be challenged in the future as new delivery mechanisms for cards and applications emerge. Typical examples may include the following:

-

Distributed Issuance

Many organisations in future will wish to offer customers new products and services. Today it can take time to personalise and issue a new card to the customer and so rapid delivery will become an important marketing tool of most organisations in the future. One important feature will be the ability to issue a card to the user at the time he or she applies for new products and services. In order to achieve this, whether it is from a bank branch, kiosk or any other remote issuance point, cost-effective secure card issuance systems will be required.

Some of the issues that need to be considered include: -

Physical security of the remote equipment

Management and control of remote equipment

Security, management and control of card stock at the remote location

Operational status of remote issuance system (i.e. can the remote site operate off-line, or are all card issuance requests sent to a central site for processing).

Post Personalisation

A smart card has the ability to have new applications loaded onto it once it has been issued. This provides the issuer with the unique ability of supplying a card product that can better reflect the lifestyle of the cardholder, as opposed to the traditional model of a fixed card product type being offered to the client. It will help promote greater usage of the card, and will allow the issuer or the cardholder to change the applications that are on the card on an on-going basis, thereby providing the cardholder with greater benefit and perceived value.



In order to support this business model, issuers will need to build an infrastructure that allows for the generation and delivery of secure personalisation data, in the correct format for the target card, to remote devices in a real time mode. Many issues need to be considered when adopting this business model, including: -

Central or remote generation of the personalisation data (see comments above)

Service delivery level - the time to generate the personalisation data and write it to the target card

On-line authorisation and validation of an application load request

Acknowledgement of successful load or failure of an application and the updating of the front and back office systems

Conclusions

Smart cards provide an effective mechanism to issue multiple applications to cardholders that better reflect the individual's lifestyle. Multiple application smart cards have proven that they lend themselves to different vertical markets, and at the same time allow for crossover into new market areas. This will become common place as issuers start to sell 'real estate' on their cards.

Many organisations have delayed the issuance of smart cards, but the business case for smart cards is growing, especially in the financial market, with counterfeit fraud continuing to escalate. As technology advances the cost for the supply and issuance of smart cards is dramatically falling, making them much more of a commodity item.

In order for an organisation to gain the maximum benefit associated with this new technology, to deliver ever increasing value to the cardholder and to maximise the business revenues, careful and due consideration has to be given to current and future card management and issuance processes. The smart card offers many value-added benefits over the traditional magnetic stripe card and it is only the issuer's inhibitions and lack of creativity that will hold the organisation back. The longer traditional issuers wait to deploy smart cards, the greater the opportunity for other organisations to enter the market.

The THALES e-SECURITY Personalisation Preparation Process

Overview

The Thales e-Security Personalisation Preparation Process (P3) system has been designed and developed to allow card issuers to move into smart card schemes by reducing or eliminating the need to change back office issuing processes. The P3 system receives the files generated from the existing card management system, if so required, and adds the appropriate data for the smart card applications to produce a composite file in a format ready for physical card personalisation.

The Thales e-Security P3 system provides card issuers, whether they be financial, government or commercial organisations, with a generic card personalisation preparation architecture to meet their current business needs and their future card issuance requirements. P3 provides a personalisation preparation architecture that allows the issuer to support personalisation and customization of applications and cardholder data onto a variety of smart card technologies (Visa Open Platform, Javacard, MULTOS, Proprietary etc.). The Thales e-Security P3 system provides the following features: -



Multiple Application Support

The P3 system provides for the generation of the EMV data elements. Specific functionality has been included into P3 to provide full support for 'Early & Full Option' card data requirements. The following EMV compliant applications are supported: -

Debit Credit Applications

- Europay Pay Now Pay Later
- MasterCard MCPA
- Visa Smart Debit Credit
- JCB Debit Credit

Dedicated Funding Source Application Data

Electronic Purse Applications

Visa Cash DES

Visa Cash RSA

With the advent of open platform smart cards, many organisations are looking to issue applications for a variety of purposes. Today the most common form of applications are financial (i.e. debit, credit, electronic purse etc.), however, many issuers are also looking to offer non-financial, non-branded value added applications.

The P3 system is supplied with smart card platform software utilities. These software utilities provide the issuer with an architecture that allows them to source smart card applications from any vendor, and convert the application and associated positional information, into a standardised format for personalisation preparation. The P3 architecture provides a standardised approach that allows an issuer to perform this task through a common process (P3) with a set of software utilities for data formatting, irrespective of the applications and card type.

P3 provides a personalisation preparation framework that supports the issuers immediate business needs, but has the capability to support new applications, as and when the business requirements dictate, thereby protecting the organisation's investment in smart card issuance systems in the future.

Secure Key Management Functions and Processes

Many applications and smart cards require secure information to be programmed on the card. The Thales e-Security P3 system provides for the secure generation, storage and distribution of all sensitive key material and data. All cryptographic security processes are carried out in the Thales e-Security Host Security Modules (HSM). No sensitive information is ever presented outside the HSM in a clear text format.

The HSM is a tamper resistant, hardware cryptographic processor that is extensively used by financial institutions worldwide. It provides a secure means to generate all the sensitive information required for smart cards. The HSM can commonly be found attached to banks' front-end systems, providing the cryptographic support for the authorisation of online cardholder transactions.

P3 provides the card issuer with the necessary public key support to allow for the generation of the issuer public key pair and the certification of the issuer's public key by the card brand.

Security is of paramount importance when trying to combat fraud. As such, the Thales e-Security P3 system provides the card issuer with a cryptographic key management system that will allow them to generate and control all the keys required by the applications, cards and associated systems. In many instances, issuers have used P3 to generate the transport keys required for the silicon manufacturing and initialisation stages of production, thereby giving them complete control of the cryptographic key management architecture.



Secure Card & Data File Processing

The Thales e-Security P3 system has been designed so that it can accept a traditional card record file from an existing card issuing system. Issuers generate the traditional cardholder data and pass either individual card records or a batch file to P3. The P3 system interrogates each individual card record and reads the magnetic stripe information. From this information P3 can then generate the required chip card data, this being dependent on the applications to be supported on the smart card.

P3 supports data file formats that are widely used in the card industry. Much of the development of P3 was conducted in co-operation with the personalisation equipment manufacturers to ensure compatibility. Unlike traditional magnetic stripe card data, smart card data is sensitive. Therefore, P3 secures the output files (encrypted and authenticated) for transportation to the personalisation system.

Scaleable Architecture

P3 is a fully scaleable system. As and when the issuers business grows, either through growth in card volume, support for additional applications or new smart card technologies, P3 can be expanded to meet the business needs.

P3 has been developed to provide a scaleable solution to issuers of smart card products. No matter whether an issuer wishes to issue a small or large volume of cards, either for a pilot or roll-out scenario, P3 has been designed to cope with these requirements.

P3 can grow from being a single application on a Windows NT server with an attached HSM, through to multiple copies of P3 on a single, or multiple Windows NT servers, in a networked environment. Also the Thales e-Security Ethernet attached HSMs can be connected to the network to provide cryptographic resources to multiple P3 applications.

Centralised & Post Issuance

Card issuers may wish to generate and construct smart card application and cardholder data in different ways. For the centralised issuance of cards, typically, the issuer will construct a batch file of cardholder data and send it to P3 for processing. However, some issuers may wish to process individual cardholder records in a real time environment.

The P3 system supports generation of application and cardholder data in the following modes of operation.

Batch Processing

Issuers wish to create the personalisation files in a serial process, therefore, they generate all the magnetic stripe data on their host and pass the file to the P3 system. P3 then reads each individual card record, generates the chip card data and populates the relevant data fields of the application.

Transaction Processing

An issuer may wish to generate the smart card personalisation data files at the same time as the magnetic stripe information. P3, acting as a server to the host issuing system, will allow the card management application to call the P3 system in real time environment to generate and create the smart card personalisation data records. The individual card record will then be passed back to the card management application, which will in turn construct the batch file to be sent to the personalisation system(s).

However, as the world moves towards post personalisation of applications and cardholder data, the issuer will need to be able to generate all necessary information in a secure, real time environment. The issuer will need to generate a smart card application and personalisation load unit for the target card in real time environment, in an acceptable period of time, as and when requested by the card holder. In order to support this new feature, there



will be many changes required to the issuer's computing environment. Front and back office systems will have to be enhanced to support new message structures. Additionally, issuers will need to implement card life cycle management systems to meet these new business needs.

The card life cycle management system will hold all the permissions and parameters required to generate the relevant card data and this will provide the input for P3. The Thales e-Security P3 system, with its real time, online interface, will provide the mechanism for the secure generation of the application and cardholder data. P3 will also be capable of generating the correct application and cardholder load unit required for the target card to be personalised. Thales e-Security has been working closely with the card life cycle management system vendors to ensure compatibility with the back office systems.

Audit & Event Management

The P3 system, using the features of the Windows NT operating system, will provide access control of all operators and processes. All operator actions, processes and events in P3 are written to an internal log, which can be either viewed locally or consolidated at a central level for interrogation.

Utilising the standard tools and facilities of Windows NT, all event logging, reporting and performance information can be centralised at a single point for merging with other relevant system data, prior to viewing.

P3 is a fully configurable system. P3 can be configured, via the management interface, to provide the maximum processing throughput, dependent on batch/transaction processing, applications and smart card platforms supported.

THALES

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](mailto: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](mailto: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](mailto:asia.sales@thales-
esecurity.com)