# In-Branch Card Issuance

Personalisation of smart cards is the last step in a smart card issuance process relating to the loading of cardholder specific data into the applications on the card.

Traditionally cards are personalised in batches, in a central and well-secured environment; however, it would be beneficial in certain circumstances if this personalisation step could be carried out locally at the different branches of a bank or government institution. For example, it would enable a bank to re-issue a card for a customer on-demand: the customer enters the bank's branch, reports problems with his current card, enters his preferred PIN, and leaves the branch with a new, fully functional card within 10 minutes. Below you will find details on how in-branch card issuance can bring substantial time, cost and ease of use benefits.

The concept of in-branch card issuance

The principal concept of in-branch card issuance is that a customer enters a local office to apply for a new card, and actually leaves that office in possession of the new card.

Typically, the process for in-branch card issuance from enrolment onwards is managed as follows: A customer enters a branch office to apply for a particular card product. Examples are an EMV credit and/or debit card, or ID card. The customer details
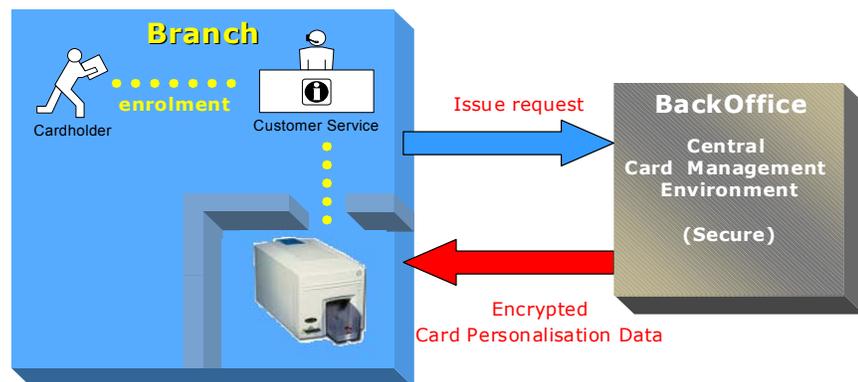
are recorded and validated, and a card issue request is sent to the central office. After further data validation and verification at the central office, encrypted personalisation data (unique to the request in question) is produced in a highly secure manner by the back office system inside the central office. The encrypted data is sent to the branch's personalisation environment, where the data is loaded onto the chip and details printed/embossed on the front and back of the card. The branch employee requests the customer to sign a delivery form and hands over the fully personalised card, which can be used with immediate effect.

The idea behind in-branch card issuance is that card management and any cryptographic functions are deployed centrally, as always, but that each branch has its own stock of non-personalised cards and simple personalisation equipment. This offers several benefits above the classic solution of central personalisation.

The benefits of in-branch card issuance

Reduction of distribution costs

Often, personalised cards are distributed to cardholders by mail. With in-branch card issuance, non-personalised cards are sent in batches to the different branches. An immediate saving of the distribution costs is achieved due to the elimination of PIN mailers.

Secure and reliable card distribution

While saving on the costs of distribution, the distribution also is more secure. When a batch of cards is transported from the central office to a branch, the cards are protected against abuse by non-authorised parties by means of a strong security scheme. The cardholder's personal information is merged with the EMV or ID application in a central secure location, and is then downloaded as an encrypted package to the smart card in the branch, so personal information is never exposed. At the same time, the distribution of cards to cardholders is more reliable in the sense that the card is handed over to the physical cardholder, and not sent to his address. This introduces the possibility to have the cardholder sign for acceptance, and thus avoid any disputes.

Enhanced customer service

In addition, in-branch card issuance enhances customer service in many ways. Most profoundly, customers don't need to wait for days for their new card, but leave the branch with the new fully functional card. Moreover, in-branch card issuance opens up the possibility that a customer chooses his PIN during enrolment. This way, a customer will always have a card with his preferred PIN without having to go through a PIN change operation and avoids the requirement for PIN mailers.
As a natural consequence, in-branch card issuance makes customers less dependent on their "home" branch. A customer could apply for a card at any branch. This is particularly appealing for customers "on the road". Replacement of a lost or stolen card only needs a visit to the nearest branch. It is clear that this particular service option is available only in cases where branches make use of a central smart card management system at the central office.

The challenges of in-branch card issuance

Classic personalisation requires a secured environment, either secured, reliable networking to a centralised Smart Card Management System, or in-branch security modules providing security locally. Such security infrastructures can make in-branch card issuance of smart cards expensive to implement on a large scale. The solution is to use MULTOS smart cards, which are unique in allowing applications such as EMV or ID to be personalised and encrypted for each cardholder's MULTOS chip using MULTOS' high security Public Key based-scheme in a centralised, secure environment. Each fully encrypted package is then delivered in a single message over any network, including the Internet, to the branch. It is then loaded to and decrypted inside the targeted (and not any other) MULTOS chip. Thus high-security in-branch card issuance is achieved without the need for reliable, secured networking or the extra expense of in-branch hardware security modules.

Who will benefit from this solution?

Government

Worldwide, governments are introducing smart card based ID cards. It is to be expected that, just like passports that are handed out by local government institutions in many countries, ID cards will be handed out decentralised and therefore would benefit from the in-branch card issuance model.

Banking

Within the banking world a huge demand for in-branch card issuance exists. Of the benefits mentioned above, typically, almost all are applicable to banks.

ACI and Thales deploying MULTOS technology for the In-Branch Card Issuance Solution

Recognising the market requirement for in-branch card issuance of EMV smart cards, ACI, MAOSCO and Thales created a working demonstration system for various exhibitions in the Middle East and Asia Pacific. Each company contributed one or more components to the solution closely based on their existing product portfolios.
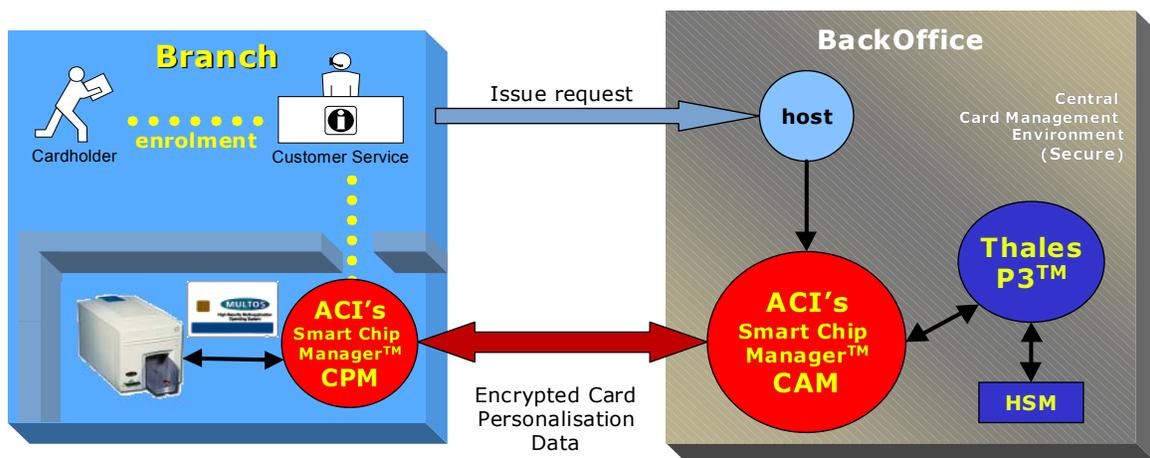
The ACI, Thales and MULTOS solution for In-Branch Card Issuance

In the case of ACI, the centrally-located Card and Application Management (CAM) system from ACI's Smart Chip Manager™ product suite is used for the smart card and application management which will 'smart card enable' the legacy host system. Each branch employs an instance of the Card Personalisation for in-branch personalisation (CPM-branch) system from ACI.

Thales provides the secure data preparation functionality required at the central site through the use of the P3™ application software in conjunction with the Thales Hardware Security Modules (HSMs).

MULTOS is the chosen card operating system platform and application loading mechanism, which is managed as an open standard by the MAOSCO organisation.

The solution is also particularly well suited for banks that currently issue magnetic-stripe cards locally. They can upgrade to EMV without changing the service response to customers.

After enrolment at the branch, and the necessary validations and approvals by the issuer's host system, ACI's CAM system receives a card issue request. The message is linked to the originating branch, which enables CAM to set-up a request-response communication with ACI's CPM-branch implementation at the regional office. During this communication CAM receives the public key of the actual MULTOS card in order to prepare encrypted personalisation data that can only be loaded to that specific card. In order to perform these required cryptographic functions CAM integrates with P3 to generate the required Application Load Unit (ALU) for the specific MULTOS smart card in question.

About ACI

Every second, every day, more then 500 organisations around the world rely on ACI solutions to power online payment and smart card processing systems in both emerging and traditional channels. More customers use our software to manage higher payment volumes, of greater diversity, across more platforms and geographies, than any other provider in our field.

In the emerging smart card market, ACI has become a major player by providing large-scale EMV solutions and participating in multi-application smart card projects in a variety of markets. Since 1975, ACI has provided software solutions to the world's innovators.

Successful smart card migrations demand more than just implementing the right product solutions. To this end, ACI offers a comprehensive programme of guidance, education and support to help organisations through their migration.

ACI's Smart Chip Manager^{TM} modular design and parallel processing capabilities allow the solution to grow as an organisation's business grows. And because the system operates independent of card technology, it enables the management of mixed card populations to protect infrastructure investments.

Visit ACI Worldwide on the Web at www.aciworldwide.com

About Thales

Thales is an international electronics and systems group, serving defence, aerospace and security markets. The group employs 62,000 people worldwide and generated revenues of €10.6 billion in 2003. Operating in three main markets covering e-security, card payment and network security, Thales e-Security addresses the business, government and finance industries' need for cryptographic security products and solutions. Over half of the world's banks, together with the majority of the busiest exchanges, currently use Thales technology.

The Thales P3 system is designed to provide card issuers with a ready-made way of migrating from magnetic stripe cards to smart cards. Aimed primarily at the payments card industry, it offers the ability to generate data for credit/debit and electronic purse payment cards. Using P3 reduces or eliminates the need to make changes to the issuer's host system thereby reducing implementation costs and timescales.

Ideal for use in both personalisation bureaux or in-house card issuers such as banks and similar institutions, P3 generates and maintains the cryptographic keys required for the secure personalisation of cards. This includes the exchange of public key certificates with the scheme Certification Authorities (CA) operated by associations such as Visa and MasterCard.

Visit Thales e-Security on the Web at www.thales-esecurity.com

About MULTOS & MAOSCO

MULTOS is a highly secure multi-application smart card operating system specification supporting a wide range of applications including EMV, ID and other value-added applications. This open standard is managed and developed by MAOSCO - a consortium of the worlds leading smart card companies - and is the only commercial operating system to attain the security requirements of ITSEC E6-high. (ITSEC is an independent and rigorous security evaluation scheme supported by more than 14 countries worldwide, whose results are openly published.) Third party software developers provide a broad catalogue of MULTOS applications and value-added services for card users and issuers that can be deployed consistently across all implementations of MULTOS. Over 25 million MULTOS smart cards had been shipped in 27 countries at Q4 2003, in projects ranging from banking, National Identity, Campus, Secure ID and Transit.

For more information about MULTOS, visit www.multos.com