

Chapter 2

Smart Card Production Environment

Claus Ebner

Abstract This chapter gives an introduction to the production steps in the lifecycle of a (smart) card. After a short introduction the manufacturing of the card body will be described. The next paragraphs give information on the personalization process chain from data processing and on to card personalization and additional services such as packaging and shipment. A separate paragraph focuses on quality and security issues. At the end there are a few thoughts on current trends and challenges for the smart card industry.

Key words: Data Preparation, Services, Card Body Production, Smart Card Personalization, Personalization, Security

2.1 Introduction

There are two main ways to distinguish card types. On the one hand it is based on the related application/Issuer type, on the other it is the technical features and/or physical characteristics. As there is a close relation between the two - e.g. an ID card for government bearing security features in the card body - this chapter will focus on the “application view”:

In banking there are the standard debit and credit cards in ID-1 format (see Table. 2.1) - both with similar characteristics: A multi-layer (usually 4 to 5 layers of individual plastic foils) card body with printed design, some optional printed security features, a magnetic stripe, a signature panel, a hologram and (more and more) with a chip. The optical personalization of the card is either done by embossing or by laser engraving.

New variations include non-standard ISO/IEC7810 cards in smaller sizes (e.g. VISA mini) or different shapes (e.g. MasterCard MC²) [2]. With the evolving trend

Claus Ebner, Giesecke & Devrient, Germany,
e-mail: claus.ebner@gi-de.com

to contactless payment even other form factors have shown up like key fobs or modules embedded in the shell of a mobile phone.

In telecoms there are prepaid telephone memory cards and microprocessor cards for mobile telephones. The card body may be either multilayer or injection moulded - with a decreasing trend for multilayer. For cards either with a short life cycle, or only serving as carrier for the plug-in module until mounted in the mobile, usually the cheaper variant is chosen.

For a card body which has no security elements, optical personalization is either done by inkjet and thermal transfer printing or by laser engraving.

Mobile phones which take a complete ID-1 card are long gone, but even the ISO/IEC 7810 ID-000 plug-in size has already a smaller successor: The Mini-UICC or 3rd FormFactor (3FF) (see Fig. 2.1).



Fig. 2.1 A G&D UniverSIM Card

Table 2.1 Smart Card Sizes

Card Type	Explanation	Size
ID-1	Usual smart card	54,0 x 85,6 mm
Plug-In	for GSM	15,0 x 25,0 mm
Mini-UICC	for GSM (3FF)	12,0 x 15,0 mm
Visa Mini	for Credit/Debit	40,0 x 65,6 mm

The highest requirements for the card body can be found for government cards and here of course especially for ID cards. The card body is usually of multilayer type (up to 9), containing security features such as mentioned for payment cards plus even more sophisticated ones, e.g. a multiple laser image, micro line print,

guilloches, invisible fluorescent ink print. Health care cards usually have a contact based chip and most new ID cards use contactless technology.

For optical personalization all techniques can be used - preferably laser engraving due to security reasons. For photos also colour dye sublimation or retransfer technology is used.

2.2 Smart Card Production Steps

2.2.1 Overview

On the way to the final product for the customer there are several steps in card production. First there is the manufacturing of the card body - which includes making of the plastic, printing, and adding additional elements, such as the magnetic stripe. This is followed by embedding the smart card module, which itself went through the steps of test and probably completion and initialization.

An optical and electrical personalization transforms the smart card to an individual one. This often is accompanied by related services, such as card carrier personalization, mail fulfilment and packaging. The following paragraphs describe these steps in more detail.

2.2.2 Card Body Manufacturing

The card body production itself may be divided into several steps again - depending on the technologies used and the features of the card (see Fig. 2.2).

2.2.2.1 Materials

The basic material used for cards is either supplied as foil for laminating or as granulate in case of injection moulding. The classical material used is PVC, but due to environmental discussions and higher lifetime requirements as well, other materials gain importance. Table. 2.2 gives a short overview, summarized from [1].

2.2.2.2 Printing Technologies

The offset printing technique is the most common one used today in industry. It starts with the making of offset printing plates for each printing colour, usually directly from a digital source made with the computer ("Computer to plate" - CTP).

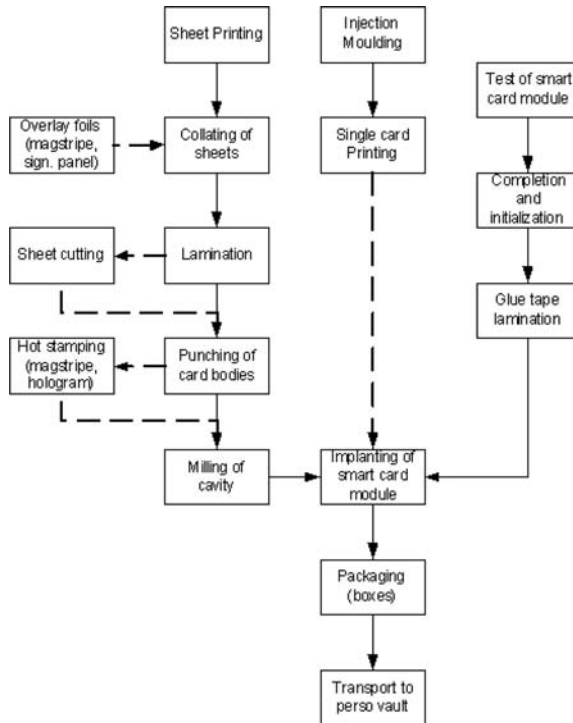


Fig. 2.2 Card Body Manufacturing Flowchart.

The image is exposed to the light sensitive plates with a laser beam. After development of the plate and chemical treatment there are zones which attract ink and others which attract water.

The plates are mounted to printing cylinders which during their rotation run against water rollers and ink rollers. The water rollers dampen the non-image parts of the plate, the ink rollers dampen the image area of the plate with ink.

The plate then transfers the ink to the rubber blanket of a second cylinder, which in turn offsets the image onto the foil running between it and an impression cylinder.

There is also a waterless variant of offset printing using special inks and UV technology. This technique is used in machines for single card printing, where the design is applied to white cards - mostly coming from an injection moulding process.

Screen Printing

The other technique used for card printing works with a porous woven fabric which is stretched over an aluminium frame. A stencil is created on the screen by filling its mesh for the negative parts of an image.

Table 2.2 Card Materials

Material	Advantages (+) / Disadvantages (-)
PVC	(+) Low price, many years of experience, recycling possible (-) Environmental compatibility, limited thermal stability
PC	(+) high temperature stability and mechanical strength, recycling possible (-) high price, low scratch resistance
ABS	(+) injection moulding suitable, temperature stability, recycling possible (-) does not comply with ISO standard, not classified as environmentally friendly
PETG	(+) best material regarding environmental compatibility, middle price, recycling possible (-) process not as easy and well-known as for PVC

The common method to do this is the photo emulsion technique. A positive film of the image is made and placed over the screen, which is coated with a light sensitive emulsion. Exposed to ultraviolet light, the emulsion will harden in the parts of the screen, where the UV light passes through the transparent areas of the film. The non-hardened emulsion will be washed away afterwards from the screen and a negative stencil of the image will be left.

In the press the screen is placed over the foil to be printed and filled with ink. A rubber blade (called squeegee) then is pulled across the screen which fills the holes of the mesh with ink. In a second step a squeegee will press the ink through the mesh onto the foil which is pressed against it.

The printed foil must now dry before the next colour can be applied.

Digital Printing

For high volume printing today there is no alternative to the techniques described above. But as there is a trend to address card Issuers more and more individual, small editions (even “lot size 1”) are topics for the card industry.

Digital printers working with thermal sublimation dye or retransfer printing are used to print individual designs onto white cards. Though the quality of this technique has so far not reached the level of Offset or Screen Printing, the results are already very well accepted by card Issuers.

2.2.2.3 Lamination

Card bodies manufactured with the lamination technique consist of two or more foils, which are pressed together under high temperatures. As the foils are of thermoplastic material they will establish a connection under heat when their softening temperature is reached.

The most common compositions are four- and five-layer cards, for contactless and ID cards even up to nine layers are put together. No matter how many layers are used, as the physical parameters of a card are defined in ISO, the sum of the foil thicknesses has to be less than 840 microns.

To protect the design printing there are two ways: If there is external printing on the outer layers of a card the surface will be covered by a transparent varnish. In the most common case of internal printing, transparent overlay foils will be laminated over the design which provides a better resistance against scratching and abrasion.

Besides design and overlay foils there are other components which can be applied in the lamination process. Magnetic stripes and signature panels brought onto a foil before are often added in this process step already. For contactless cards a “pre-lam” inlay containing the chip module and antenna is one of the layers in the lamination process.

Before entering the lamination press the layers have to be collated in such a way that the images for front and back side match exactly and the location of additional elements, such as magnetic stripes or contactless inlays, is within given tolerances. This may either be done by hand or using a sheet collating machine. The simplest way is to align the sheets using their ledges or using adjustment holes in the sheets. If more precision is needed, printed crosses on the foils are brought together using a special table with two cameras - one for the front and one for the back design. In any case the foils will be stapled together by a heated spot stamp in the rim.

These pre-mounted sheets are stacked together with thin, highly polished metal plates. This stack is put between one of the several heating plate pairs in the laminator. Depending on the necessary process parameters - which are specific for each product (regarding the type of materials etc.) - the layers are heated for a certain time and under certain pressures. After cooling down under pressure of the laminated sheet, the card bodies will be punched out in the next process step. If necessary, the sheets will be cut to fit the punching machine.

2.2.2.4 Injection Moulding

For GSM cards which mainly serve as carrier for the plug-in module, the trend is to choose the cheaper process of injection moulding. The cavity needed for the chip module is already created in this process, so that no milling is necessary afterwards.

The preferred material for injection moulding is ABS. The plastic granulate is pressed under high pressures into the pre-heated mould form. The material melted by heat and shearing forces fills the shape of the mould and solidifies. The form is opened and the work piece ejected.

The two main challenges for injection moulded cards are to find the right process parameters to cope with the shrinkage of the material and to ensure the quality of the relatively thin part under the module cavity.

Another important attribute of injection moulded cards is their printability, as the card design will be applied afterwards in a single card printing process before the chip module is implanted.

2.2.2.5 Adding other Card Elements

Signature Panel

Everybody who has a payment card in his wallet, knows that he has to sign his card before he may use it. In order to do so with a customary ballpoint pen, a special signature panel is necessary.

Signature panels are applied with two different techniques: Laminating or hot-stamping.

Paper signature panels are mounted to the outside overlay foil of a card and will connect to the card surface during the lamination process. Another option is to create overlay foils with a printed signature panel by the use of special colours in a screen printing process. Again, this overlay will be applied in a lamination process.

The hot-stamping technique works with prefabricated elements which are transferred from a carrier tape to the card body by the usage of a heated stamp. The elements - such as signature panels - are covered with an adhesive which activates under heat and pressure. Under the hot stamp the element will bond to the card surface and in turn lose its connection to the carrier tape.

Magnetic Stripe

The magnetic stripe which is a main element for all payment cards, needs to be put onto the card at a certain position. The techniques used to apply it are the same as for signature panels. Either the magnetic stripe comes on an overlay foil and is laminated or a hot-stamping process is used.

Hologram

Another security element - for example known from some payment cards - is the hologram. It also is applied to the card body using a hot-stamping process.

Components for contactless Cards

While for smart cards with contacts the chip module will be embedded after card body production, for contactless cards this happens by lamination of inlays which contain antenna and contactless chip module.

There are three main ways to manufacture the antenna for such an inlay:

- In the wire embedding technique the wire is laid directly onto a plastic foil and melted into it by using ultrasonics.
- Etched antennas are created using photolithography with copper covered plastic foils. The surplus copper will be etched away by acids only leaving the antenna shape on the plastic foil.
- The printed antenna can be produced using a special silver ink in a silk screen printing process.

The technology to connect the smart card module to the antenna depends on the antenna type. For embedded antennas it is micro welding while for etched antennas it is soldering.

No matter what technologies are used to create a contactless card, it is essential that the unevenness caused by antenna and module is equalized to achieve a good card surface.

2.2.2.6 Preparation of the Chip Module

In most cases chip modules are shipped on reels to the smart card manufacturer. In a first step an incoming inspection will be made on a test handling machine to ensure the quality of the modules before embedding. Usually the ATR of the chip is checked and read/write tests on the EEPROM are performed.

As machine costs for test handlers are lower than for card personalization machines, they are often used to already load data to the chip which are common for a range of products.

For ROM masks this is the completion of the ROM OS in the EEPROM, e.g. for extensions and patches. For Flash controllers the complete OS has to be loaded in this step.

Depending on the contents of the initialization file loaded afterwards, file structures and also partly their contents will be created, applications and keys will be available on the chip.

The criteria which parts to load in which step will not only be dependant on cost calculations but also on the product and related security requirements. So for some products it is necessary to have a clear separation between the initialization and the personalization. For other products it may be better to perform the initialization as late as possible. This avoids logistic problems, as not too much variants have to be kept in stock for the subsequent processes.

As the modules have to be glued into the card body another step is necessary before embedding which applies an adhesive tape to the modules.

2.2.2.7 Milling, Implanting and Punching

Before the smart card module can be embedded, a cavity needs to be milled into the card body (of course this step does not apply for injection moulded cards which already have it).

Now the “marriage” of card body and the module can happen. The module will be applied and glued to the card body in an implanting machine. To verify that the module is still alive after this process step, usually an ATR test is performed in the implanting machine. For some products it is also necessary to write some information onto the card body. This is possible via an inkjet printer within the machine.

For mobile phone cards (Subscriber Identity Module - SIM) finally a punching of the Plug-In is needed. Depending on the type of the punch (ID-000, UICC) different tools are used in the machine.

2.2.3 Personalization and related Services

In personalization an individual product will be created for the end customer. The data necessary to do this is usually provided by the card Issuer - sometimes enhanced by data generated in the process at personalization (see Fig. 2.3).

2.2.3.1 Data Transfer

Customer data usually enters the smart card via ISDN dial-up data connections or encrypted channels over the internet. For big volumes sometimes also tapes or other media are still used.

The data has to be encrypted and will be decrypted only after being transferred to the production network. Depending on the card Issuer’s system and the number of products, several files will be provided. Quite often similar products are within one file, e.g. VISA and MasterCard credit cards.

2.2.3.2 Data Capturing

In most cases the card Issuer will supply the data of his customer, but there are also data capturing services performed by personalization bureaus. In a typical scenario the customer apply form for a card has a special part for the photo, which is teared off and sent directly to the personalization bureau. The photo will be scanned and stored under a reference number, so it can be linked with the other personalization data sent by the card Issuer to create a photo card.

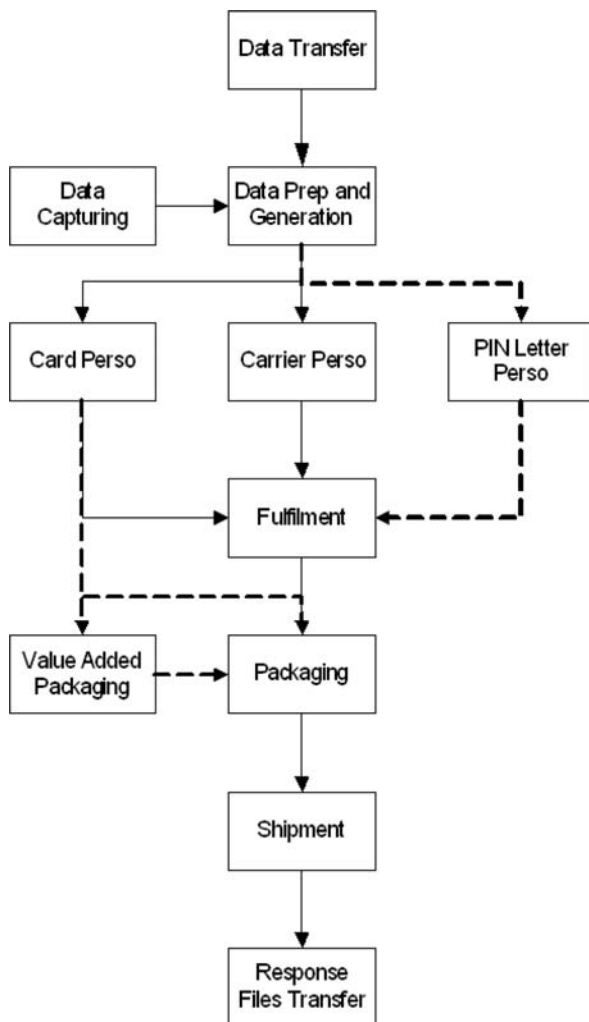


Fig. 2.3 Personalization and Related Services Flowchart.

2.2.3.3 Data Preparation and Generation

Due to security requirements the production network is logically separated from the data transfer network. So before the data can be processed a transfer of the data via the separating firewall has to be initiated.

After decryption of the files a validation of the data takes place. Sometimes also a conversion has to be done, e.g. for banking card Issuers with mainframe systems it is quite common to convert their EBCDIC data to ASCII before further processing.

For validation first the file structure and integrity will be checked, and then also whether the data fields contain allowed values. This may be simple checks like whether a field is numeric or checks whether there is a defined product and process available as requested by control fields of the customer data.

In many cases a grouping and sorting of the data will be the next task. So there may be different service levels and certain records have to be processed and produced on the same day while for others there is a bigger time frame. Other criteria may be different shipment methods (by mail, by courier, etc.), different enclosures to go with the card mailing or different addresses of the card Issuer's locations where the cards should be sent to.

A merge of data from different sources is another task of data processing. This may be photos or logos for optical personalization as well as data for different applications on the chip.

For many products it is also necessary to generate additional data which will go into the chip. This is very common for SIMs, where the network operator often only provides the basic numbers (ICCID and IMSI). The values for keys (e.g. the Ki) and secret values (e.g. PIN, PUK) have to be generated with a random generator or are derived by using certain card Issuer keys and/or calculation methods. In that case the card Issuer needs to receive a response file which contains all the values generated, so he can store it in his systems.

Another task for products being sent out by direct mail is to create the postage information - depending on mail type, weight and destination. Due to the requirements of the local mail service this information needs to be printed on the carrier, probably leads to the usage of different envelopes in fulfilment and must be provided in a billing report.

Also for credit cards with chip (EMV) there is a process which takes the magnetic stripe data and some card Issuer keys to generate data for the chip.

As the secure storage and generation of keys and the encryption of production data is a basic requirement today, a key management system and the usage of Hardware Security Modules (HSMs) is a must.

At the end of the data preparation process there are several outputs: Data validation reports, production files for the different card personalization machines, printing files for carriers and labels, information on the products (bill of material, process steps) for production and sales (what to bill to the card Issuer?), log files and audit trails and also response files for the card Issuer [3].

2.2.3.4 Card Personalization

Depending on the product machines have to offer a wide range of personalization technologies. Most machines can be set up individually by combining different machine modules and can also be adjusted for further requirements later (see Fig. 2.4).

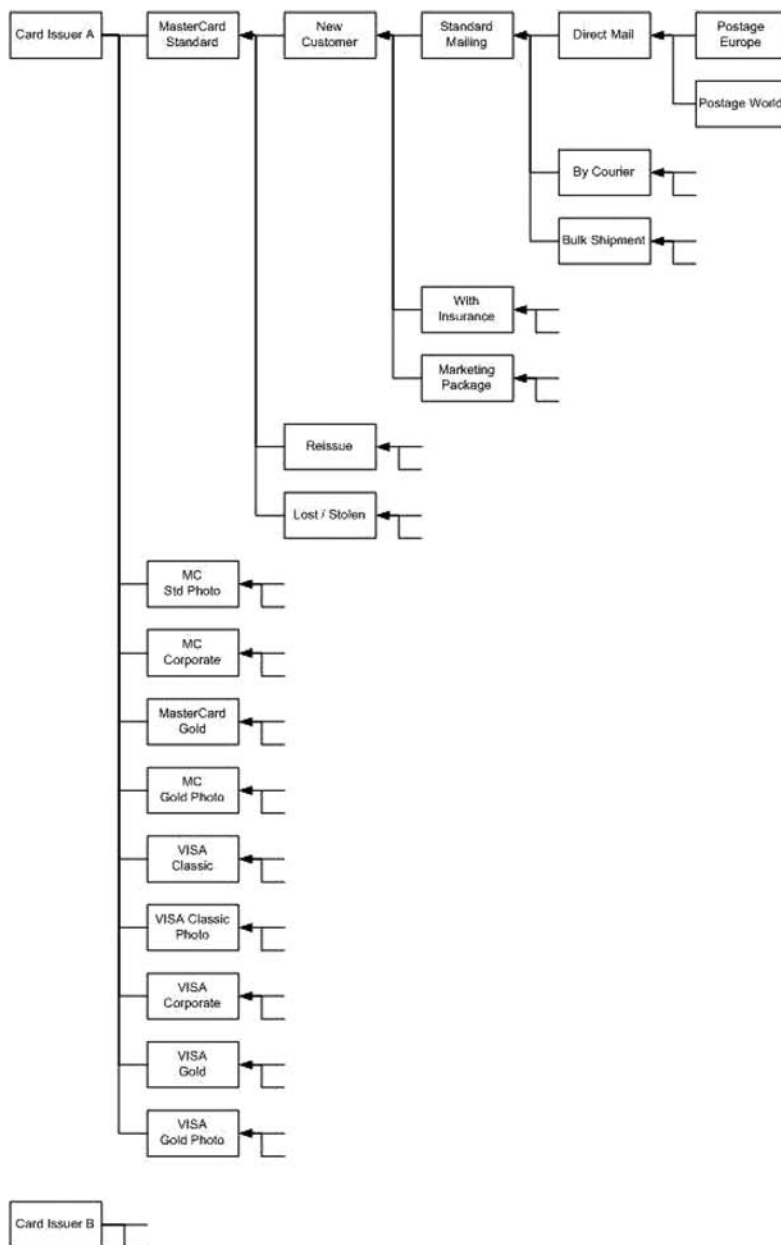


Fig. 2.4 Variants in Personalization (Example).

Laser Engraving

Laser engraving is the most secure way of optical personalization. Its result can be seen in the different layers of a card and be felt on the surface of the card. The laser can either personalize vector fonts or raster images. The latter one takes more time, so for bigger images (photos, logos, barcodes) it is necessary to have more laser modules in one machine for a high output.

Another advantage for laser personalization is reduced cost, as no ink or transfer film is needed.

Embossing and Indent Printing

Embossing and Indent printing are the classical methods for personalizing credit cards. Still in many countries credit cards are not processed online, so the embossed characters are needed to create the receipt. Embossing is done with typewriter wheels with standardized font types (OCR-A, OCR-B). In modern high speed machines two or more modules are used to enable high throughputs. Printing on the rear side of the card is called indent printing, characters are not embossed in that case.

Inkjet

Inkjet printing is often used in conjunction with simple products such as voucher cards. There are machines available which have a very high throughput (40000 cards per hour). On the other hand inkjet also can be used for colour images.

Thermal Transfer, Colour Dye Sublimation and Retransfer Printing

These techniques work with ink ribbons and thermal print heads.

Thermal transfer printing is used for monochrome images, such as logos or barcodes. It delivers high optical quality, but less security than laser engraving, as the ink is applied to the surface only and does not go into the deeper layers.

For colour dye sublimation a three-pass process is necessary, using ribbons for Yellow, Magenta and Cyan. Usually an overlay ribbon is applied on top of the images to protect them against abrasion and fading. Again, the images are only on the surface and therefore not as secure against copying as laser images.

The retransfer method is similar to colour dye sublimation, but instead of printing directly to the card a reverse image is printed to a transfer film which is then applied to the card body. The main advantages are better quality, as an unevenness of the card does not affect the printing result and that the image can be printed over the full surface area of the card and no white borders can be seen. This technique is used for "picture cards" where the end customer may choose his personal design from

a given choice of pictures or even by sending his own photo taken with a digital camera.

Magnetic Stripe Encoding

To encode the magnetic stripe with its three tracks (e.g. for credit cards track 1 and 2 are used) magnetic stripe readers are used. Usually there's at least two of them in a machine: The first one encodes the magnetic stripe, the second one reads back the information from the magnetic stripe to ensure that it is written correctly. It is also possible to pre-encode a card's magnetic stripe to use that information in personalization - e.g. to check whether the right plastic is used.

Chip Encoding

Chip personalization has become quite a complex process in the last few years, as the capabilities of the chips (e.g. Java Card), the memory sizes (Megabytes!) and also the security requirements have increased.

The basic process is that the card reader has to establish a connection to the smart card, perform an authentication by presenting a key and then select files on the smart card and update them with personalized contents provided by the data preparation and generation process.

Depending on the complexity of the product, these steps may involve a mutual authentication between card and reader, the use of an external HSM (Hardware Security Module) to handle/create keys and en-/decrypt the communication channel. Additional data may be loaded from different sources (configuration files, databases) or also be generated during the personalization process and passed back to data preparation. So the smart card itself may perform asymmetric key generation and export the public part for a certificate request.

To cope with the amount of data and the throughput needed, a number of high performance card readers are needed in personalization machines. It must be possible to change parameters like voltage, frequency or divider in a wide range for optimization. With local memory available on the readers, also certain parts of the personalization data can be stored there to improve performance. New and future products also offer new smart card protocols, like USB or SWP (Single Wire Protocol).

There are also high requirements to the hard- and software handling the personalization data and process - regarding quality, performance and stability. A typical scenario today is to handle 60 smart cards in parallel and load each one individually with some hundred kilobytes with other components involved (HSMs, databases etc.).

Typical Personalization Machines

As mentioned before most machine vendors offer a modular design of their machines to fit a wide range of requirements. The input and output modules either handle a loose stack of cards or work with magazines. Some machines may have more than one input module, so different plastics can be mixed in personalization. If the same plastic has to be separated for different card Issuers or sorted for later shipment more output stacks are an option as well.

A typical machine for credit card personalization will have a magstripe reader module, followed by a chip encoding module for EMV cards. With a thermo transfer module (for front and/or rear side) an additional logo can be placed on the design - e.g. a company's logo for company credit cards. A colour dye sublimation module may follow to personalize a photo of the cardholder - again this may be for the front or rear side. The last stations in the machine will be the embossing units, one with types to emboss the credit card number, one or more (for high throughput) other units to emboss the remaining lines, e.g. the cardholder name.

The performance range starts with 200 cards per hour (cph) for small desktop systems and ends at 3000 cph for high volume systems.

A typical machine for SIM card personalization may have a vision system after the input module, which serves two purposes: Verify that the right card body is used and calculate offsets for the origin for optical personalisation to equalize punching tolerances. As the data volume for the chip can be quite high for SIM cards, there will be multiple chip encoding heads working parallel to ensure the machine throughput does not go down for longer loading times. High volume machines which run at more than 3000 card-per-hour may have 40, 60 or even more chip encoding heads. Many SIM cards will only receive an optical personalization with a number (the ICCID), some may also have a barcode. So the typical number of laser stations is one or two. To be flexible for either front or rear personalization often a flip over station is used. To verify the quality of the optical personalization, a vision system can be the last module before the cards go to the output stacker.

If cards can't be processed (e.g. if the chip does not work) the machines will treat them as rejects and put them on a separate reject output stack.

Additional modules are available for printing the card carrier, affixing the card to the carrier and also to put this in an envelope, probably together with some additional enclosures. Higher volumes are often handled on separate machines instead of this "inline process". This will be described in the next two paragraphs.

2.2.3.5 Carrier and PIN Letter Personalization

The letter to the end user which carries the card is in most cases personalized using a laser printer. For small volumes this may be simple office printers, for high volumes there are high speed machines printing up to 250 pages per minute (ppm) for cutsheet printers or even over 1000 ppm for continuous feed printers.

Most card Issuers today provide a blank paper which only has their pre-printed logo and probably some fixed text on the rear side. All the rest will be printed variable, which gives the card Issuer a maximum of flexibility and enables him to address his customers very personally. For smaller volumes colour printers are an option as well, which will print all information including logos etc. on a white sheet of paper.

To enable an automatic matching of the card and the carrier in the fulfilment step, a machine readable card identification number needs to be printed onto the carrier - either as barcode or using an OCR (Optical Character Recognition) font type.

PIN (Personal Identification Number) letter personalization today most often also works with laser printers. One method is to cover the PIN with a sealed label after printing, another one works with a special paper which already incorporates a sealed label.

Another method still used works with needle printers and carbon coated multilayer paper. There is no carbon ribbon in the printer, so the PIN cannot be seen during printing - but will be found in the PIN letter after tearing off the seals.

2.2.3.6 Fulfilment

The most common way to hand out a card product to the end customer is to attach it to a personalized letter (carrier), optionally add some information leaflets (enclosures) and put it all into an envelope.

Depending on the card Issuer requirements this leads to a high variety of products, e.g. by sending out the same card product with different enclosures.

The process may either be handled manually for small batch sizes or by dedicated mail processing systems for higher volumes, with a throughput of up to 8000 mailings per hour. These machines are set up from different modules; a typical configuration looks like as follows:

The paper feed module will take the pre-printed carriers, in case of continuous paper a cutter will then cut it into single sheets. In the next module an adhesive label will be placed onto the carrier. The card attaching station reads information from the card (usually from the magnetic stripe or chip) and the corresponding information from the carrier (usually OCR or barcode). If the information matches, the card will be affixed to the carrier. It is also possible to attach more than one card to the carrier - so a bank may send out a MasterCard and a VISA card on the same carrier to its customers or a family receives all their health cards within one mailing.

Afterwards the carrier with the attached card is folded (e.g. z-fold, wrap fold) and inserted into the envelope. An inserter module consists of a number enclosure stations from which for each mailing additional enclosures can be individually pulled and inserted. Most often these are non-personalized information leaflets or booklets, but also personalized items are possible, e.g. by matching them via a barcode.

After all components are in the envelope, it is sealed and a weighing scale behind it checks the weight of each mailing. This may be used to check whether the mailing is correct (e.g. the card didn't get lost in the machine) and to calculate postage or to

sort out different mailing types as well. From the output stacker module the operator can take the mailings and put them into boxes, which will then be handed over to the shipment area..

2.2.3.7 Packaging

For products which are not sent directly to the end customer, packages have to be made according to the logistical needs of the card Issuer. These packages may either contain only cards or cards in mailings which are distributed in other ways after they leave the personalization bureau. Related to packaging there is the printing of shipment lists and identification labels to the cardboard boxes. As these lists and labels apart from some overall product information also contain some personalization data (e.g. first and last card number in a box, on a pallet) the data has to be provided by the personalization data processing systems.

2.2.3.8 Value Added Packaging (VAP)

To address customers even more individually, there are many variants to packaging of cards. In nearly all cases this is a manual process, as the individual items cannot be handled by a machine and the volumes usually are not high enough for the investment in an automated solution.

Typical products for VAP are gift or SIM cards. There's a wide range of boxing available, e.g. CD boxes, sophisticated cardboard boxes, blister packages and even wooden boxes or leather cases. With the cards may go user guides, mobile phone handsets and manuals or different marketing items.

2.2.3.9 Response Files

Last but not least there are also non-physical products which have their origin in personalization. During data generation and processing some data is created which the card Issuer may need in his systems for either logistical or technical reasons.

Some card Issuers need the information which card number has when left the personalization site. On the one hand so they are able to answer requests from their customers "(When will I receive my card?) ", on the other hand this information may be necessary for them to start a related process, e.g. printing and sending out a PIN letter.

Whenever a card contains individual values created or allocated in personalization, the card Issuer will need these values in his system. This may be individual card keys like the Ki for GSM cards which is needed in the provider's authentication system or a chip hardware identification number to be stored in a CAMS (Card Application Management System) for later purpose.

For some processes it is even necessary to send a response file to the card Issuer or another related party and wait for an answer to this response file to continue production. For example this applies to load certificates for keys generated on the smart card: During personalization the smart card generates an asymmetric key pair, the public key is sent in a certification request to an external certification authority (a trust center) and the certificate received gets personalized to the smart card in a second personalization step.

2.2.3.10 Logistics

One of the challenges in personalization is to handle logistics most effectively. Due to the many variants which are generated by different card bodies, carrier papers, enclosures and shipment methods production breaks down into small lot sizes.

On the other hand there are very restrictive rules how cards have to be treated in a secure production environment. The cards are stored in a vault and any movement and withdrawal has to be recorded. A counting of cards takes place between the significant process steps. When a card is spoiled in a process, this of course has to be recorded as well. At any time a “four-eyes-principle” has to ensure the integrity of the process.

There are two main ways to provide the cards to personalization: Either the amount of cards given by the card Issuer order is moved to personalization and rejects produced on the machines have to be pulled in an additional run - or a higher amount is moved to production and the rest needs to be balanced at the end when returned to the vault.

In order to reduce machine setup times, similar orders can be processed together - this can also be supported by intelligent data preparation. Example: There are four different card designs which are applied to the same type of carrier paper. The data preparation will create one carrier printing file and four card embossing files. So there is only one order at the printer instead of four. The same then applies to fulfilment where the card stacks are combined and the machine can produce with one carrier stack in one run.

2.2.4 Security and Quality

Security is one of the main issues in smart card production. A card manufacturing plant or personalization bureau has to fulfil high requirements on physical security. This starts with the fences around the building, which must be constructed in a way that no car or lorry simply can break through it. Additional electronic systems detect any other trials to break through this first barrier. Video cameras need to survey the whole plant area as well. The building itself has to fulfil certain standards (wall thickness, stability of doors, etc.) and of course especially in the production area.

The security areas may only be entered via man-traps and there are clear policies for any access necessary by non-registered staff (e.g. for service of production machines). Only people who are able to prove their integrity may work in those areas and all their comings and goings are recorded. No single person is allowed in the security area, a four-eyes-principle needs to be guaranteed in any case, supported by video cameras all over.

Security is also part of all processes - there is a continuous counting of security relevant materials, such as cards, holograms etc. during an order workflow. Another very important task to ensure logical security in personalization is the protection of data. Networks for smart card production are strictly separated from other networks and of course from the internet. Access to data is limited to the persons who need to deal with it and encryption of data is applied wherever possible. It is also essential to delete the personalization data after production in a safe way. On the other hand certain data has to be kept on behalf of the card Issuer or to ensure traceability.

Organizations such as MasterCard, VISA or the GSM Association will perform regular audits to prove the physical and logical security in card production sites. If severe problems were detected by them, this could lead to a decertification and such to the loss of the business. Therefore an ongoing process has to be established, which always ensures the compliance with the actual security regulations.

Quality is the other very important issue. Well defined quality management procedures and a quality assurance during the whole product lifecycle are a matter of course. This starts with the definition of a product, continues with development, test and the production release process following it. During the production various sample tests and in some cases 100% tests are performed to finally prove the quality of the products before they get shipped. Examples are:

- Visual and electronical control is performed after printing processes
- An incoming inspection on modules checks the physical dimensions and the EEPROM as well
- A depth control is performed on the milled cavity before embedding the module
- Cards are tested in bending and torsion cycles to ensure they and the smart card module are fit for use
- Personalized cards are checked against the personalization data to ensure that the right data got onto the card
- Sample mailings will be opened to ensure that the end customer gets the product in the right configuration
- Response data is checked against personalized cards to ensure it matches to the product delivered to the end customer

Everyone can imagine that all these investments in security and quality lead to very high initial and ongoing financial efforts. This means high hurdles for newcomers in the market and a challenge for the existing companies to remain competitive.

2.2.5 Current Trends

2.2.5.1 More individual Products and Services

In the last years there has been an emerging trend to supply even more individual products and services to the card Issuer.

It starts with a high variety of card body designs. So a typical bank portfolio comprises MasterCard and VISA credit cards - standard/gold, private/business, in cooperation with other companies (Co-Branding), special editions for an event (e.g. World Cup, Olympics), with and without photo, etc. On top of that there are debit cards, customer cards, savings account cards - again with different characteristics. Up to fifty different designs per card Issuer is not unusual, some even have hundreds.

This leads to small batches in card body production and to even smaller lot sizes in personalization. With the "picture card " this reduces to lot size of one: The individual card design is made from a digital photo provided by the cardholder.

Variants which can be handled quite easily in production are different texts which are printed on the card carrier. Many card Issuers have dozens of text variants to send out the same card on the same carrier to address their customers individually. The print programs will print the different variants in one run, but there is considerable effort to create and maintain the related templates. If the carrier papers also shall be in many different designs, colour printing on demand is a possible solution.

The next level of variety comes with packaging. Much of it can be handled with mail processing systems, which are able to pick different enclosures to create the mailing. But for special formats, enclosures that are not capable of machine handling and VAP, manual work is often necessary.

Finally there are different shipment methods which expand the number of variants. There is bulk shipment using different carriers, there is direct mail with the established post or alternative service providers and there is shipment by different couriers. A related service requested from card personalization bureaus is to pull certain cards during production and switch their shipment type, e.g. from direct mail to courier.

The card Issuer today expects narrow service levels. For the introduction of new card body designs this are still weeks, smaller changes of a product configuration may be already requested on a day-to-day basis. Card personalization and shipment for many products (in the daily low-volume business) are handled within one or two days, but for some products the time-frame is even limited to hours (e.g. emergency credit cards).

2.2.5.2 Extended Data Services

The main business for personalization bureaus today still is "data in - card out - delete data ". But more and more card Issuers ask for also management of their data and request more detailed information on their orders during the production process.

Managing data starts with such simple solutions like the storage of scanned photos or a secure storage of the keysets on a card, which may be recalled for later customer applications. Another more complex example is an internet gateway for the cardholder which enables him to select an individual card design or to provide his digital photo for his personal credit card.

When it comes to completely manage the lifecycle of a card, enable post issuance personalization (e.g. adding a new application to a smart card after the cardholder already received his card) and store and manage all related information, a Card Application Management Systems (CAMS) is required.

As personalization bureaus handle material on behalf of the card Issuers (cards, carrier paper, leaflets, envelopes etc.), the card Issuer either needs continual information to control his stock levels or can ask his supplier to do so for him. Monthly stock reports often are still state of the art, but card Issuers more and more ask for an online and actual access to this data.

Similar requirements are showing up for a more detailed and actual view on the production process. Card Issuers want to view the progress of their order - even down to the cardholder level. As on the other hand requirements on data security are very high, this is not easy to implement.

2.2.5.3 Memory Encoding

One of the challenges of the smart card industry is to cope with the increase in memory sizes now available in chip modules. While for years there were only a few kilobytes to handle in the initialization and personalization, with the propagation of flash technology today a typical SIM card will be loaded with a few hundred kilobytes. And the first SIM products with 512 megabytes or more additional memory are available.

As the encoding times are limited by the standard protocols ($T=0$, $T=1$) and in the end physically by the memory write times, personalization machines have to be equipped with a number of card readers to achieve a reasonable throughput. Let us illustrate that with an example: For a throughput of 3600 cards per hour the machine cycle time is only one second for each card. If the chip encoding time is 40 seconds, we need 40 card readers working in the machine in parallel to keep this throughput.

2.2.5.4 Increasing Security Requirements

While the card industry formerly was mainly concentrated on the physical security of the production sites - including walls, doors, vaults, man traps, video systems etc. - today the focus is more on the logical security.

As personalization bureaus handle such sensitive data as credit card numbers, their processes and related IT systems have to be on a very high security level. This involves the secure handling and storage of keys and data, a reliable firewall concept,

an effective data access restriction and a gapless monitoring of all activities in the network - right up to the operation of Intrusion Detection Systems (IDS).

The encryption of cardholder data throughout the whole process is one basic requirement, even though the data is already kept in separated network and most of the data can be seen on the card and the carrier during the production process.

Even higher security levels can be achieved by the separation of different fire-walled segments within a production network. This may also be necessary to segregate data from different card Issuers.

The access to data has to be based on a “need-to-know” basis. The requirements here often exceed the capabilities of the on-board functionality of operating systems. So the applications need to establish an additional layer, e.g. by implementing four-eyes-principle, the use of smart cards for access etc.

There is considerable effort to implement such a consistent data security and as it also leads to more complex processes, there are additional ongoing costs as well.

2.3 In Conclusion

Smart card production entails a broad selection of activities and technologies. It begins with printing, laminating or injection moulding of the card body and the application of several card related items - such as magnetic stripes and holograms. It is followed by the test and initialization of the smart card modules which are then embedded into the card body.

In the personalization process of the card there is a physical part performed by laser, embossing and thermo transfer modules. And an electrical part whereby the magnetic stripe and the smart card module (with contacts or contactless) is encoded. Personalization also happens for card carriers, followed by related services such as mail processing, packaging and shipment. All these steps are strongly linked with a data preparation process.

One of the current trends and challenges is the demand for even more individualized products and services, including an extended data management process. Others trends are the increasing memory size of smart cards with its related impact on personalization times and the increasing security requirements, which need to be supported by appropriately improved IT architectures.

Quality and security are the most important aspects in smart card production and mature audited processes need to be implemented at all times.

“This article is the result of the experience of the author and colleagues at G&D, who I would like to thank for their kind support. It represents the author’s personal views only and not necessarily those of G&D or any of its affiliates.”

Useful Websites

The reader may find the following websites useful:

<http://www.icma.com>

- Website of the International Card Manufacturers Association.

<http://www.gi-de.com>

- Website of Giesecke & Devrient.

Glossary

3FF	3 rd Form Factor.
ABS	Acryl Butadiene Styrene
ASCII	American Standard Code for Information Interchange
ATR	Answer To Request
CAMS	Card Application Management System
Cph	Card per hour
CTP	Computer to plate
EBCDIC	Extended Binary Coded Decimals Interchange Code
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMV	Europay, MasterCard, Visa
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
ICCID	Integrated CirCuit IDentification
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identification
ISDN	Integrated Services Digital Network
Ki	Individual Subscriber Authentication Key
OCR	Optical Character Recognition
OS	Operating System
PIN	Personal Identification Number
PC	Poly Carbonate
ppm	Pages per minute
PVC	Poly Vinyl Chloride
PET	Poly Ethylen Terephthalate
PETG	PET Glycol-modified
PIN	Personal Identification Number
PUK	PIN Unblocking Key
ROM	Read Only Memory
SIM	Subscriber Identity Module
SWP	Single Wire Protocol
UICC	UMTS Integrated Circuit Card
USB	Universal Serial Bus
VAP	Value Added Packaging

References

1. Yahya Haghiri, Thomas Tarantino: *Smart Card Manufacturing: A practical guide*, John Wiley & Sons Ltd, 2002.
2. ISO/IEC 7810. More Information Available via
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31432, Cited 3 Oct 2007.
3. ETSI, *Smart Cards;UICC-Terminal interface;Physical and logical characteristics* (Release 7) TS 102 221 V7.9.0 (2007-07). More Information Available via
<http://www.etsi.org/>, Cited 3 Oct 2007.

Smart Cards, Tokens, Security and Applications

Mayes, D.K.; Markantonakis, K. (Eds.)

2008, XXXVII, 392 p., Hardcover

ISBN: 978-0-387-72197-2