
Integrity mechanism in German and international payment systems

Detlef Kraus, SRC Security Research & Consulting GmbH, Bonn,
detlef.kraus@src-gmbh.com

Abstract: An overview of measures used to ensure data integrity in German and international payment systems will be given. While symmetrical cryptographic algorithms are mainly used in national electronic cash system or in electronic purse, asymmetrical procedures are in use in international systems in order to simplify the key management. The descriptions of the payment systems are kept short and focus merely on some measures to ensure integrity and process control. They are not suitable to give a complete description of the overall system security.

It is assumed that the reader knows, how an asymmetrical cryptographic algorithm works and is acquainted with the various operation modes of a symmetrical asymmetrical cryptographic (here Triple-DES).

1 electronic cash

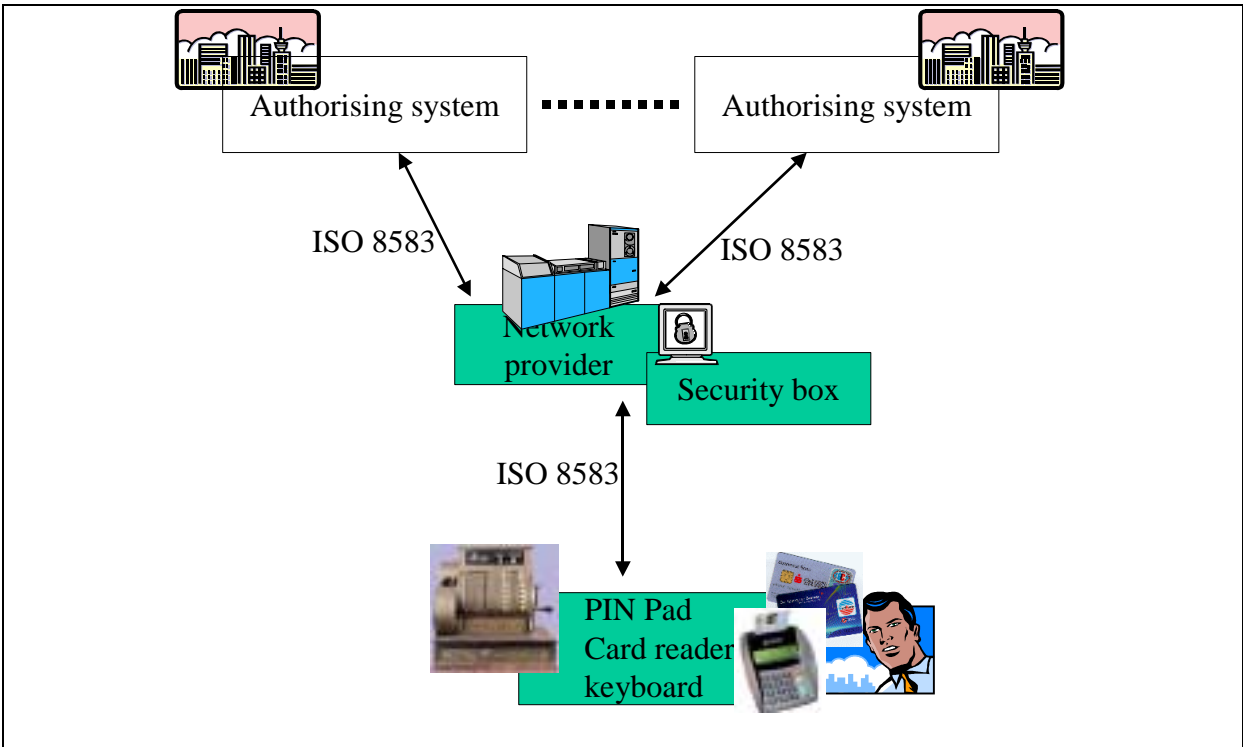
electronic cash is a payment method based on debit cards, which is used at the Point of Sale (POS) as well as at vending machines. When paying with his card the card holder must authenticate himself by using his four digit PIN.

The amounts paid by means of this process will be debited from the card holder's account by the merchant upon presenting the transactions. This takes place normally already on the next day, depending on the time of the merchants submission of the transaction. The issuing banks guarantee the acceptance of every electronic cash transaction to the merchant. For this payment guarantee the merchants have to pay a fee to the card issuer. Consequence of the payment guarantee is that under no circumstances electronic cash transactions can be returned from the card issuer to the merchant. Thus the merchants do not have to handle the complaints and the efforts involved.

Precondition for this payment guarantee is a high security level of the payment system, which must be implemented particularly on acquirer and issuer side. For explanation we briefly describe the authorisation procedure in the following.

Every transaction will be routed online to the issuer's authorising system and will then be authorized there. Main parts of this authorisation are the PIN verification and the verification of the individual card holder's credit line. The latter ensures that the amount, which the customer wants to pay at the POS is available at his account. Additionally there also will be an alignment with the issuer's blacklist – depending on the issuer's system – and an alignment with a positive list, which contains every issued card. The structure of the authorizing messages is in accordance with the standard ISO 8583

Typically the electronic cash system is processed by so-called electronic cash network providers. These network providers run a host computer, to which they connect electronic cash terminals. The network providers are responsible to transfer each transaction in accordance with the bank code number coded on the card to the correct authorising system and to return the answers received to the terminal. Based upon the security requirements defined for this role, network providers will be accredited by ZKA. At present there are approx. 25 certified electronic cash network providers in Germany. In addition network providers fulfill supply services for the banking industry to monitor and to account the merchant fees and to compile system statistics.



Picture 1: Schematic representation of the process of electronic cash transactions

Security Criteria

The German banking industry has formulated security criteria for the operation of such a system. Network providers, who want to receive an approval have to demonstrate the observation of these security criteria by an evaluation. It would be beyond the scope of this article to numerate and describe all security criteria in detail. Therefore only some important ones are described in the following.

I Component-Authentication

All components actively participating in POS systems must authenticate each other by means of cryptographic procedures.

This requirement does not establish any specific authentication procedure. In general, component authentication is achieved by proving possession of a secret information

A component actively participates in communication if, due to its position in the system, it can evaluate, modify or process security related information. Such information comprises especially the personal identification number (PIN), PIN trial counters, message authentication codes (MAC), the amount acknowledged by the customer.

II Message Integrity

1. All security related message data must be protected in the components of the payment systems before and after their transmission against unauthorised modification by appropriate means
2. The modification of security relevant data performed during their transmission between the system's components must be recognized. Such violations of integrity require an adequate reaction.
3. The unauthorised intrusion of messages into the system must be recognized. Such violations of integrity require an adequate reaction

III User authentication

If the based payment system requires the authentication of the cardholder by means of his PIN, it must be ensured that corresponding functions can only performed, if the right PIN code was entered

IV Secrecy of PINs and cryptographic keys

1. The PIN must never be transmitted in plain text outside secured components. If it is processed or stored in system components, it must be protected against unauthorised disclosure and modification.
2. Cryptographic keys must never be transmitted in the clear over electronic lines. If they are used or stored in system components, they must be protected against unauthorised disclosure and modification.

-
3. No system component must provide for a means to determine a PIN by exhaustive PIN search.

In connection with message integrity (criteria II) and the secrecy of PIN and key (criteria IV) it is referred additionally to the following criteria:

V Hardware requirements

1. All encryptions, decryptions, re-encryptions, MAC generations and cryptographic checking procedures are performed in security modules specially protected against unauthorised access. The corresponding keys are also stored in such security modules.
2. Security relevant data and processes (e.g. keys or programmes) and secret data (e.g. keys and PINs) in security modules must be protected against unauthorised disclosure. This requirement must be assured by the following means:
 - the hardware construction of the security module, eventually combined with security mechanisms of the security module's software,
 - the restriction of software loading into security modules to the production process itself or to software loading done only after the mutual authentication of the communicating entities,
 - securing the loading of security relevant data, especially cryptographic keys, by cryptographic means.

Secret data in security modules must also be protected against disclosure attacks, which accept the destruction of the module.

Integrity mechanisms and process control in electronic cash

In the electronic cash system the cryptographic protection of the transactions is effected by symmetrical algorithms. The triple DES algorithm is used for both the encryption and for the message integrity with a Message Authentication Code MAC. This code is calculated for the complete authorizing message according to ISO 8583 and contains transaction counters, the amount, the information on the customer account, the encrypted PIN and further information.

This ensures that

- the account information (as well as all other message fields) can not be manipulated during the transmission and therefore the "correct" account (the customer's account at the POS) can be charged. Additionally the account and PIN must fit.

-
- no messages can be re-transferred into the system, since the transaction counter is incremented in each session. This shows which importance the strict requirements for the hardware have beside the protection of the cryptographic keys. The transaction counter is controlled by the software in the PIN Pad and it is a substantial part of the security evaluation to examine this behaviour. The back-office systems additionally store for each terminal the current status of the transaction counter.
 - no false messages can be introduced into the system.
 - the cryptographic keys used for encryption and message integrity for each session are derived dynamically from a master key. Therefore different MACs are generated for messages in different sessions, even if the contents of the messages are the same. A session is restricted to one authorisation transaction. The master keys are changed annually and every network provider uses his own keys.

The security of the electronic cash system is ensured by the network provider, particularly by the operation of the security components PIN pad and security module at the host computer. In addition organizational measures have to be implemented, like naming the security representatives, monitoring system irregularities or controlling the life cycle of the security components.

2 Chip-based payment systems

2.1 Electronic cash offline

Predominant parts of the electronic cash system, described in the preceding sections, are still implemented at present on the basis of magnetic strip cards. Since the majority of German debit cards are equipped with processor chips including cryptographic co-processors, whose operating system and applications were specified by the German banking industry, payment processes, like electronic cash or so-called "GeldKarte" (electronic purse) are transacted offline, as far as card and terminal are accordingly equipped.

With the offline variant of electronic cash the PIN of the card holder and the credit limit stored in the chip are verified and during the payment process the latter will be reduced by the appropriate amount. The card issuer determines the level of the offline credit line during the card production. This however can be changed during online authorisation¹. The offline variant has the advantage that communication costs and transmission times to the authorising systems can be reduced. Since the German banking industry also provides a payment guarantee, there are the same requirements for security, as described in the preceded section.

¹ If the credit line is reduced to the extend, so that a further payment is not possible, than the credit line can only be raised by an online procedure. The process is similar to the online variant.

This can be reached for electronic cash offline, among other things, by the fact that communication between smart card and terminal are secured by Secure Messaging [ISO 7816-4].

Secure Messaging in this context provides message integrity for the complete command and the associated answers.

The secured command message for the smart card contains:

- command parameters (CLA, INS according the specifications)
- amount of payment and
- terminal ID.

The message integrity is effected via computation of a Retail CFB-MAC² with a card-individual key, which the terminal derives from a master key³ and card data, by using an Initial Chaining Value (ICV), which has been generated as a random number by the smart card itself. The random number was requested with the command GET CHALLENGE by the smart card before and is used by the smart card operating system to verify the following commands. A manipulation from outside, i.e. a change of data, for example the amount of payment, on the interface between chip and terminal is thus not possible or recognized by the operating system and leads to an immediate termination of the process.

The integrity of the answer generated by the smart card is secured by the same mechanisms - the random number for the ICV, however, is now a value generated by the terminal and transferred to the smart card with the previous command. The message contains

- card and account information, which allows a debiting of the customer's account
- a certificate, generated by a further card-individual key and securing card data and payment amount and
- a Retail CFB-MAC on the complete message including the tag and length coding of the data.

Herewith the integrity of all relevant data of the payment transaction are ensured and intended or unintentional manipulations can be recognized. At the same time the MAC verifications performed by terminal and smart card result in an implicit authentication⁴ of these components with respect to the above mentioned security criteria.

² Cipher Feedback Mode

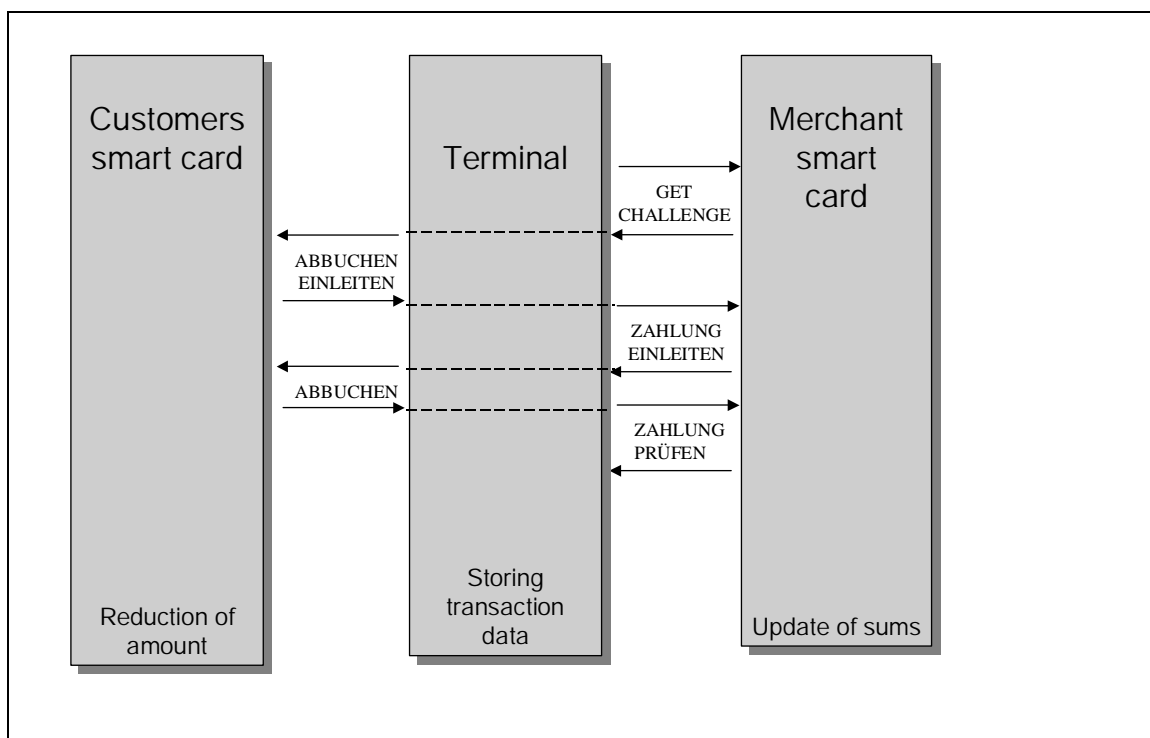
³ These master keys are changed every year. In case of key compromise the key is changed immediately.

⁴ Or not, if the MAC cannot be verified by either side

The fact, that master keys are stored in the terminal, again demonstrates the importance and role of the security requirements for the hardware. A master key has to be protected in particular against physical attacks, which put up with the destruction of the module. On the basis of the fulfilment of all security requirements the German banking industry can provide a payment guarantee to the merchants. For the sake of completeness it must be mentioned that the payment command is only processed by the card if the customer has authenticated itself beforehand with his PIN. Otherwise the card would terminate the procedure.

2.2 Electronic purse – GeldKarte

The German banking industry has launched an electronic purse named „GeldKarte“. For the description of the measures used for message integrity, we confine ourselves to the description of a paying procedure. We assume that there is a certain amount stored in the electronic purse.



Picture 2: schematic presentation of the commands during a GeldKarte-payment procedure

The payment procedure is effected offline and without PIN verification. As a security module, a so-called “Händlerkarte” (merchant smart card, also called “PSAM”) is used by the merchant. It is based on the same operating system as the customer smart card. For the comple-

tion of a paying procedure, however, specific commands and file structures are implemented. The merchant terminal transfers the messages between the merchant card and the customer card and shows on its display e.g. the amount of purchase, which must be confirmed by the customer.

Since the debiting procedure takes place offline, a mutual authentication of the smart cards is necessary. The keys specified for this purpose are regularly changed; additionally reserve keys are determined for a case of key compromise. By the authentication it is ensured that only certified system components communicate with each other.

With the command ABBUCHEN EINLEITEN⁵ a random number generated by the merchant card will be transferred to the customer card. The customer card returns this value and a sequence counter, the so-called "purse sequence counter" (Börsensequenzzähler), which has a unique value for every payment, in an integrity-secured response⁶.

The command ZAHLUNG EINLEITEN⁷ sent to the merchant card includes these data and after examination on correctness - in particular the correctness of the random number is examined - the merchant card returns its answer including the purse sequence counter and a merchant sequence counter (Händlerfrequenzzähler), which is a sequence number defined by the merchant card and unique for each payment transaction,. These data are cryptographically secured by a MAC and are included in the command ABBUCHEN (DEBIT), which is sent to the customer card. Therefore the customer card can check the correctness of these data.

The cryptographically secured answer of the customer card contains among other things:

- a unique number identifying the merchant card,
- account information for the settlement of the amount claimed by the merchant,
- both sequence counters,
- the payment amount and
- the new current amount in the purse.

⁵ Sorry, but it is a German specification. ABBUCHEN EINLEITEN means 'prepare debit'

⁶ For this procedure one key out of 10 can be selected. On the basis of the explicit key-ID the Händlerkarte determines which key will be selected.

⁷ 'Prepare payment'

These data will also be transferred to the merchant card⁸ for verification.

In each protocol step and with each command a whole set of examinations take place in both smart cards. The protocol only leads to a successful payment, if each individual step is kept in such a way, how it was specified and each individual examination - mainly the cryptographic message integrity of the transferred data – has not been interrupted. The processing control is integrated therefore in substantial points into the operating system of the smart card and/or the special commands for the paying procedure. Further controls and verifications are performed in the background systems, so called evidence centres. Thus it is prevented that unauthorized debiting of money from a customer card by means of a falsified terminal or a falsified merchant card can be effected.

The last example makes clear that the high security requirements to the hardware can precisely be reduced. The terminal does not have to store cryptographic keys anymore and is only a communication mediator between customer card and merchant card and of course a guide (via the display) for the customer. The hardware security requirements to the smart cards remain of course the same.

3 Integrity control in Key Management

The preceding explanation of the national paying systems showed that the measures used for message integrity are based on the cryptographic protection by symmetric algorithms. A large range of keys must be transferred to appropriate institutions and persons safely, so that the production of the smart cards, terminals, Pin Pads and the operation of the network providers and authorizing systems runs smoothly. Apart from the confidential transmission of the keys to the authorized receivers, a series of check values have been defined in order to provide integrity of cryptographic keys. For example this ensures that the keys were entered correctly into a security module. It must be considered that a cryptographic key consists of a random sequence of hexadecimal numbers and the input over a keyboard in this case is very error-prone. The Key management of the German banking industry therefore defines check values for integrity control such as:

⁸ Apart from the security issues one can also see from this overview that the paying procedure takes place anonymously. Not the account of the customer, but the so called 'Börsenverrechnungskonto' is used in the paying procedure. This account is used by the card issuer specifically for the GeldKarte system, in order to collect the amounts loaded to each card. The amounts claimed by the merchants are paid from this account.

-
- 16 Byte hash value of the key K according to [ISO 10118],
 - 8 Byte Retail-CBC-MAC, which is calculated over the logical key name (in ASCII), an algorithm identifier, key-ID and version as well as the key in clear,
 - 8 Byte Retail-CBC-MAC, which is calculated on the encrypted key as well as the other data as in the preceding paragraph,
 - verification pattern compatible to IBM-TSS⁹ with an 8 byte random number RND.

The receivers of the keys select the check value suitable for their hardware component and enter these together with transfer keys and cryptogram into the security module, which uses the key.

4 EMV

The credit card organizations Europay, MasterCard and Visa (EMV) are currently changing their world-wide debit and credit cards from magnetic stripes to smart card technology. Apart from the higher security of the chip technology there are further reasons for the conversion, like the possibility of being able to offer customer loyalty programs by additional applications (e.g. electronic purses, bonus systems) on the smart card.

For the purpose of the technology conversion EMV has developed and published specifications [EMV B1]. These specifications set a world-wide, open standard for payment functions in the debit and credit card field. The standard covers the specification of the smart cards and requirements for the terminal and/or the back-office systems, in particular a description of the interface between smart card and terminal in detail.

In contrast to the national payment systems described before, offline security procedures for card authentication and PIN encryption defined by EMV are based on asymmetrical cryptographic procedures (in this case the RSA algorithm). The reason for this is that issuer and acquirer normally come from different organizations and countries with very different security infrastructures and thus a key management with common keys for symmetrical security procedures can hardly be realized¹⁰.

By the implementation of the EMV specifications it is ensured that

⁹ TSS Transaction Security System by IBM

¹⁰ The asymmetrical procedures use no common keys for communicating components, but are based on pairs of public and secret keys.

-
- the smart card is a "genuine" smart card, i.e. the integrity of the smart card is checked offline,
 - the card holder can use the smart card only after a successful authentication,
 - the payment transaction is verifiable,
 - the payment transaction can not to be changed.

For the use of the smart cards at terminals it is – in accordance with EMV specifications - among other things, necessary that the terminals contain the authentic public key of the payment system. Although it is a public key and not a key, which has to be kept secret, like the keys in the mentioned payment systems so far, it must be ensured due to system availability and security against counterfeiting that this key was not falsified or changed.

It follows, that after storing the key into the terminal (e.g. during the personalization process at the manufacturers side) should not be modified by any means. Otherwise it becomes possible to use manipulated or faked smart cards. Manipulations of the terminal hardware must be recognized by the user – which is a property called ‘tamper evident’. From this we see, that even for the handling of public keys it is necessary to obey hardware security requirements.

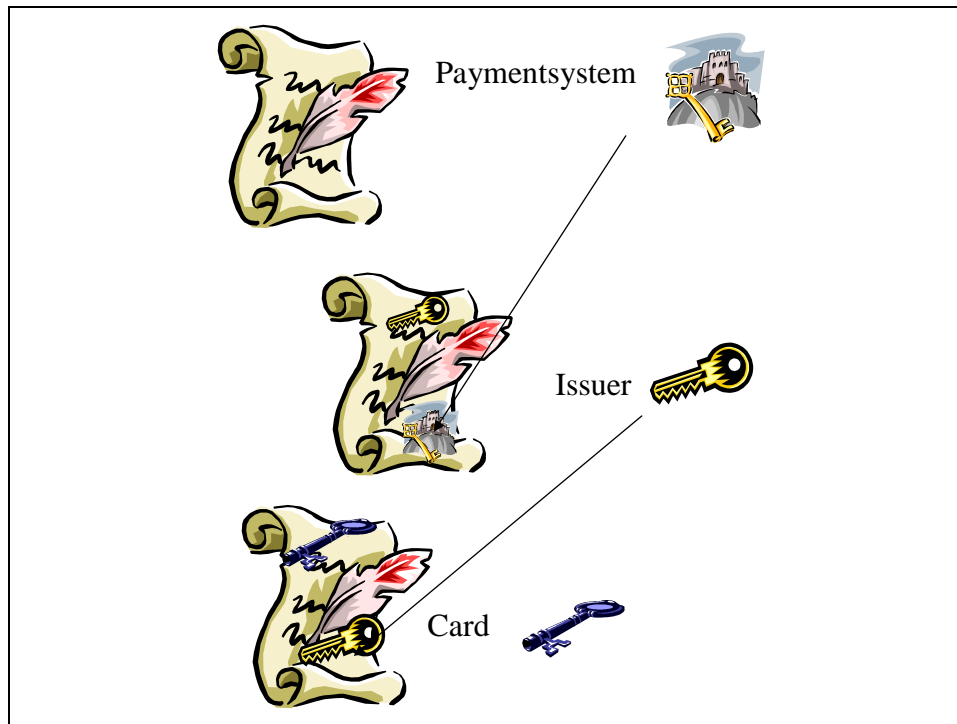
We discuss in the following only the mechanism of key exchange of a public key of the payment system. This key is transferred to the acquirer in terms of a self-signed certificate. The format specified by EMV contains identification data contents such as ID of the certificate holder, key index and algorithm identification and also

- the length of the modulus of the public key,
- the length of the exponent and
- the public key (modulus and exponent).

The certificate is calculated over the identification data mentioned above and over parts of the public key and a hash value over the complete public key. For this the secret key of the payment system is used.

The receiver of the key has thus the possibility to examine its integrity by verifying the certificate with the same public key, which has been transferred to him. As a hash algorithm a SHA-1 algorithm [EMV B2] will be used.

The authenticity of smart cards used at the terminals is examined by verifying the card issuer's signature on certain data fields of the chip. For the verification a public key of the card issuer is used, which was certified in turn by the payment system provider. In this way the certificate chain is attributed to the public key of the payment system stored in the terminal.



Picture 3: certificate chain

It must be marked here that this static data authentication of smart cards alone does not offer complete security. It is e. g. possible to produce a copy of the card – even it is a little be more difficult than doing this with magnetic stripe cards. To avoid these kind of attacks - and this is intended by EMV also - further protective mechanisms like a dynamic data authentication of the components must be used.

The German banking industry will introduce the EMV standard on smart cards gradually. Thus e.g. the ATM's will change over to chip technology for both international and German cards. The national ATM application on smart cards will satisfy the EMV standard, so that German smart cards are usable also at ATM's internationally.

5 Literature

- [EMV B1] Europay International, MasterCard International and Visa International, Integrated Circuit Card Specification for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.0, December 2000
- [EMV B2] Europay International, MasterCard International and Visa International, Integrated Circuit Card Specification for Payment Systems, Book 2, Security and Key Management, Version 4.0, December 2000

-
- [EMV B3] Europay International, MasterCard International and Visa International, Integrated Circuit Card Specification for Payment Systems, Book 3, Application Specification, Version 4.0, December 2000
- [EMV B4] Europay International, MasterCard International and Visa International, Integrated Circuit Card Specification for Payment Systems, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.0, December 2000
- [ISO 10118] ISO 10118 - 2, Information technology - Security techniques - Hash-functions, Part 2: Hash-functions using an n-bit block cipher algorithm, 1994
- [ISO 7816-4] ISO 7816 - 4, Identification cards - Integrated circuit(s) cards with contacts, Part 4: Inter-industry commands for interchange, 1995
- [ISO 7816-4A] ISO 7816 - 4, Identification cards - Integrated circuit(s) cards with contacts, Part 4: Inter-industry commands for interchange, AMENDMENT 1: Impact of secure messaging on the structures of APDU messages, 1996