Business
Substances
Environment

Information
for the
underwriter

apropos

Chipcards

The chipcard market
The concept
Types of card
Fields of application
Security aspects
Data protection
Tips for the underwriter

1.13

AssTech
Sederanger 4–6
D-80538 München
Germany

The range of services offered in the information, communication, banking and health-care fields is constantly growing. To ensure that these services are provided in a controlled manner and that the sensitive data involved are protected against misuse, we require suitable tools.

Business enterprises also need tools to help implement internal procedures such as time data entry, access authorisations, the use of technical facilities, and even the cashless supply of food and drink.

One such tool able to meet these often quite diverse requirements is the chipcard.

The chipcard market

In 1994 roughly 460 million chipcards were manufactured worldwide, some 89 % of them in Europe. If current growth rates remain unchanged, by the year 2000 we can expect an annual production rate of 2.2 billion chipcards worldwide.

The production of chipcards involves not only the chipcard manufacturers, but also the producers of computer chips. The three leading producers of computer chips have a 76 % share of the international market, while the three biggest chipcard manufacturers control as much as 86 % of the market.

The concept

A chipcard is a piece of plastic the size of a credit card with an integrated module. The base of the module is composed of a foil incorporating strip conductors, contact points and a surface on which the chip is mounted. The computer chip is glued to this surface and connected up to the strip conductors.

There are various types of card which can be differentiated in terms of their variable structure, the characteristics and functions of the chips used and the way that data are exchanged between the card and the reading device.

Types of card

Memory card

This type of card contains a memory chip and is used as a storage medium. Owing to its greater storage capacity and enhanced reliability, this type of card is an alternative to a magnetic stripe card.

A memory card can be upgraded to include security and access functions that make it harder for unauthorised persons to misuse the card. A prime example of such a function is the personal identification number (PIN).

Microcontroller card or smartcard

The chip used in this type of card has a microprocessor and a programmable memory. In addition to data storage, the chip allows flexible data processing and the active programming of access authorisations.

The cryptocard goes one step further: it has an additional coprocessor for encryption and decryption of sensitive data.

The cryptocard boasts the highest security standard of all chipcards.

The following card types are available as either memory cards or smartcards:

Non-contact card

This card gets its name from the method by which data are transferred from the card to the card reader, i.e. non-contact data transfer by means of high-frequency waves. Depending on the type of application, the maximum distance between card and reader may vary from a few millimetres to several metres.

At present, however, the contact card is the more widespread type. As the name implies, a contact card must make a direct connection with the sensors of the card-reader.

Hybrid card	A hybrid card has two storage media: a chip and a magnetic stripe. The idea behind hybrid cards is to allow chipcards to be used in conventional magnetic card readers. The term hybrid card is sometimes also used to describe cards that permit both contact and non-contact data transfer.
Personalised chipcards	In contrast to anonymous chipcards, which contain no information about the cardholder, the information stored on personalised chipcards makes them clearly assignable to an individual person. The personal data are stored in the chip itself and also on the plastic card in the form of identification features.
Multifunctional card	As the name implies, these chipcards can be used for various purposes, e.g. an employee ID card designed not only for access to buildings and facilities, but also for recording working hours and making cashless purchases from food and drink machines.

Fields of application	Through the integration of state-of-the-art computer chips, cards that were previously employed for simple storage purposes (e.g. a telephone card with a certain number of units) can be used multifunctionally, namely for anything from data management to administration of security codes against unauthorised access. The following breakdown shows current and potential fields of application for chipcards.
Communications	A telephone card is the most widespread form of chipcard with a fixed amount of units. It is also available as a telephone credit card, recording the units used and debiting their value from the cardholder's bank account at regular intervals. A mobile radiotelephone network card allows cardholders to charge use of their own or other people's mobile phones to their own subscriber account. A company card authorises the cardholder to use company telephones, fax machines and photocopiers. A cryptocard provides its holder with a forgery-proof digital signature for the purposes of electronic correspondence.
Financial transactions	An electronic purse is a chipcard which is loaded with a certain amount of money at the bank and then used to make cashless payments in shops, public transport, etc. There are plans to install chips in Eurocheque cards, bank-customer cards and credit cards. Banks and credit-card companies can also use this chipcard to provide other services.
Health care	In Germany, most members of the public health funds already have a personalised chipcard. More advanced versions of this are the patient data card containing information on examinations carried out, existing illnesses, required medicines as well as data for emergencies, and the hospital card for storing data required for or gleaned from examinations and treatments carried out in hospital.
Security technology	The authorisation card controls entry to buildings and electronic facilities and is a means of identifying users of databases, networks and computer systems. It also serves as a security module to prevent unauthorised copying of software.
Charge monitoring/debiting	A chipcard can provide descrambling codes for pay-TV channels and can also be used as a permit or debit card for the use of ski-lifts and other sporting facilities.

Private and public transport

Implementation of the EU's 2nd Driving Licence Directive in Germany in July 1996 includes plans to issue new licences in the form of chipcards. In addition to the information shown in conventional licences, it will be possible to store data on vehicle-licence taxes and road-use charges paid, along with a record of any traffic fines imposed by the police.

A debit card allows cashless payment of public transport fares or road-use charges (= road pricing).

A chipcard can serve as an electronic key for a car's door locks and ignition as well as for activating/deactivating a car immobiliser.

Security aspects

Dangers

Apart from the fact that they can easily be stolen, the main dangers posed by chipcards are the possibility of unauthorised access to and manipulation of the stored data, of reading and decoding the chip, and of forging chipcards.

There is a wide array of security measures that can help reduce or even eliminate these dangers by physically protecting the chipcard and the chip itself, by shielding the software and by making data communication between the card, reader and background systems safer.

The level of security required depends largely on the purpose for which the chipcard is to be used. A health insurance chipcard, for example, demands a much lower level of security than, say, an access pass to a highly sensitive computer centre.

Experience has shown that in the field of technology there is no such thing as 100 % security. Chipcard developers must therefore work constantly on replacement systems and test all possible types of illegal use and manipulation so that, in the event that a chipcard is discredited through manipulation or fraud, they can immediately introduce replacement systems that do not have the same shortcomings.

Chip manufacturers

Chip manufacturers are one group of relevance to chipcard security.

No matter how sophisticated a security system to protect chips and data transfer may be, it is useless if security-relevant manufacturing data are not kept strictly confidential.

Such information leaks can be hindered only if the chip manufacturer has a closely meshed security net in place.

Chipcard manufacturers

Chipcard manufacturers not only provide the plastic base for the computer chip, they are also responsible for personalising the chipcard.

"Personalising" means identifying the holder of the chipcard as its authorised user. The corresponding personal data include the cardholder's name, the individual card number, the corresponding ID number in the provider's system, the cardholder's PIN, the security-algorithm code, the card's expiry date, other user and identification data as well as the specific applications which the card entitles the cardholder to access. Personalising is thus a highly sensitive and security-relevant aspect of chipcard manufacturing.

Use of chipcards

The non-technical dangers posed by chipcards can be of either a human or organisational nature.

It can never be ruled out that chipcards may be used by unauthorised persons if the card is lost, stolen or lent. Even the very best security measures are useless if they are not matched by a similarly sophisticated organisational structure for monitoring card security.

Data protection

There is a host of ways in which chipcards can be used, all of which involve the collection and concentration of often sensitive customer data in the hands of chipcard providers. This can quite conceivably pose data-protection problems, some of which are outlined below.

Right to data

Once users have inserted their chipcards in a reading device, they relinquish the right to the data stored on the cards. The data can potentially be made available on-line all over the world via the card provider's data pool. Incorrect data or the unwanted dissemination of data can redound to the customer's disadvantage.

Even now it is almost impossible to maintain proper control over such data stocks, and there is an acute need for legal, technical and organisational measures to ensure data protection.

Basis of trust

As a rule, the chip software is provided by the service enterprise that has an economic interest in the stored data. The user of the chipcard, however, has no control over the software employed or the stored data and thus no possibility of monitoring whether the data are actually stored as agreed in his contract with the service provider.

Chipcards for several application areas

A prime objective of chipcard development is the multifunctional card, on which several, possibly different, data sets are stored.

One problem posed by such cards is the possibility that a company or institution authorised to access only one data set might succeed in reading all the data on the card.

Another aspect is the way in which a particular application is accessed: for instance, all applications stored on the card must be read to check whether the desired application is present. From the point of view of data protection this is problematical since, if all applications on the card have to be read, conclusions may be drawn, for example, regarding the cardholder's credit rating or health status.

User identification

Chipcard technology is set to become the norm in many areas. As a result, users will have an array of chipcards, for the use of which they will have to memorise different user IDs, usually PINs. For this reason – and also because of the need for ever greater security – it will be necessary to devise new security features for chipcards. Unambiguous personal features such as a fingerprint or the fundus of the eye are possibilities. Among data protection experts, however, the storage of such personal features is still viewed as subject requiring much discussion.

Tips for the underwriter

The following areas are loss potentials of relevance to the insurance industry.

Chipcard manufacturing

Chip manufacturers
Quality shortfalls and damage to products as a result of deficiencies in the production and testing of chips. (The same is true for the liability of manufacturers of chips for electronic data-processing systems.)

Chipcard manufacturers
If the wrong data, authorities or security codes are assigned to a personalised chipcard, card providers and, by way of recourse, chipcard manufacturers may be faced with liability claims, depending on the purpose of the card.

Claims for damages may arise if warranted access security features are implemented inadequately or not at all and the card-user then suffers disadvantage owing to misuse of the card by third parties. Inadequate access restrictions may also result in claims of recourse from card providers whose reputation has thus been tarnished.

Chipcard use

Owing to the wide variety of application areas for chipcards it is impossible to provide a complete list of all insurance claims that may arise.

However, the following are the main areas of interest to underwriters:

- liability claims arising from bodily injury or financial loss traceable to defective hardware or software or to erroneous or false data. A possible scenario could concern the loss, corruption or incorrect entry of data on a patient or hospital chipcard, which might necessitate repeated examinations or lead to prescription of the wrong treatment;
- claims of recourse following a malfunction in the chipcard as a result of premature wear and tear;
- negative interest due to the criminal manipulation of chipcards;
- misuse through the illicit use of access-authorisation cards or the unauthorised access to company data because warranted security standards were not fulfilled.

The property insurance field could witness an increased demand for cover, with card providers wanting to insure the cards they issue, primarily against misuse, theft and physical damage.

This demand is currently met under electronic equipment insurance policies. However, such policies are problematical for insurer and policyholder alike as the loss potentials involved under what is virtually an all-risks cover are difficult to estimate and, as a result, the risk premiums charged are very high. The need for new forms of cover here is quite evident.

Postal address:
AssTech
Assekuranz und Technik
Risk Management Service GmbH
Postfach 221150
D-80501 München
Germany

Office address:
AssTech
Assekuranz und Technik
Risk Management Service GmbH
Sederanger 4–6
D-80538 München
Germany

Telephone +4989 3844-1585
Telefax: +4989 3844-1586
Telex: 5215247 bav d

Spanish subsidiary:

BEER & AssTech, S.A.
RISK MANAGEMENT SERVICE, S.A.
Miniparque Empresarial de La Moraleja

Telephone: +34 1 6509142
Telefax: +34 1 6509514