Report on the protection of personal data with regard to the use of smart cards (2001), by Mr Karel NEUWIRT

(Czech Republic)

FOREWORD
II. TECHNICAL ASPECTS
A Definitions
B Brief history of Cards
C Overview of the available technology
D Application of Smart Cards
E Specificity of data conservation, access and processing
III. LEGITIMACY ASPECTS
A Adoption of Convention 108 principles
B. Domestic legislation
C Standardisation
D Code of conduct
E The Council of Europe and Data Protection Instruments

FOREWORD

The plastic card with a memory has been a part of peoples' lives since 1950, when the Diners Club issued pay cards as members' identification. The first plastic credit card was then issued by the Bank of America in 1960. Since that time, it has been used in various areas of human activity: in banking, business, health care etc. Later on, the card was equipped with memory elements which enabled the card to carry more and more data. The capacity of these memory elements increased along with developments in technology. The amount of personal data concerning cardholders also increased. These data serve as identification and also characterise the cardholder within the scope of the area for which the card was issued (health data, payment data, consumer data, etc.).
It is important to say at the outset that smart cards are only part of a large complex system, which includes terminals, networks, servers, customisation systems and software applications, as well as key encryption management. This complex system is secure only if each part of it is secure. Smart cards are only one link in a longer chain.

- the "card" phenomenon complementary to the "net" phenomenon
The smart card is being considered as a specific tool for a reasonable increase in the quality of today's information society in general. The smart card phenomenon stands in opposition to the networks, especially the open and unsecured but widely used Internet. The cards represent individualised sophisticated tools in comparison with the commonly shared (but unique) network.
While smart cards offer multiple functions such as, for example, digital signature, encryption and storage of selected information, networks provide universal access to information and knowledge. To achieve the optimal benefit for users/citizens, the two technologies should be combined. Thus the synergies of cards and networks for the advanced information society must be analysed and recommendations for appropriate solutions must be developed.
In this sense the dual platform of card + network paves the way for the challenged applications and ought to be evaluated as complementary technology for both its benefits and risks.

- the card as a security-enhancing tool - key holder/generator

Adequate and trustworthy use of information and communication technologies represents a critical success factor for the modern information society.
Smart cards ensure security features in very specific and individualised ways: they enable the collection of private data related to the cardholder, but a processing facility is added so that access to the data content can be controlled in various ways by both the cardholder and the information system.

Whilst in the past many projects tried to build their communication infrastructure either on cards or on networks, it is now widely accepted that some needs of security, privacy and universal access to personal data may only be achieved by combining the functions of smart cards and networks.
One of the essential features is the possible generation of cryptographic keys within the smart card itself. Together with the provision for electronic signature, encryption and advanced standardisation make the smart card unrivalled as a tool. It must be noted that GSM[1] is often considered as a potential competitor aiming to provide individuals with a mobile handset instead of a smart card. But GSM is in fact based on the plugged smart card, called the SIM[2] card, and the handset is nothing more than a smart card and human interface. In this sense the rules and recommendations for card-users and GSM users became identical.

The use of cryptographic smart cards implies the setting up of public key infrastructures, where access to relevant data will not be possible without permanent access to these infrastructures. Hence internationally harmonised infrastructures have to be built and operated. The need for international interoperability by these measures is obvious.

- the card enables effective off-line transaction management
Besides security, smart cards also bring a business-oriented advantage, which is the feasibility of providing secure off-line transactions. This means mainly user authorisation – a procedure by means of which the cardholder proves his relation to the card - and mutual authentication between the card and the information system to which the card has been connected.

The off-line operation is important for two basic reasons:
Firstly, it makes certain solutions feasible thereby saving costs of communication on-line (and real time in the same case) and it solves emergency cases in which the on-line connection is not available for whatever reason.
On the other hand, off-line procedures bring a new class of risks which must be evaluated, related to off-line secure computation which is not supervised via powerful enhanced servers and with the security of authentication between remote off-line running workplaces and network servers.

Smart cards provide sufficiently secure solutions for these requirements.

Electronic cards have played an even more significant role in the creation of an information society. That is why the European Union, at the conference held in Lisbon in April 2000, decided that the smart card issue would also be resolved within the framework of the "eEurope 2002: An Information Society for All" initiative. The Smart Card Charter program, currently containing 12 partial sub-programs that solve various problems connected with the application and utilisation of this technology in practice, has been ratified.
The expected expansion of smart card applications anticipates the increase in personal data processing. With a growing amount of personal data being stored in a card's memory, the risk of these data being misused and of the cardholder's privacy being compromised increases. The goal of this report is to call attention to these risks and to determine principles to ensure that the risks are minimised.

[1] GSM – Global System for Mobile communications
[2] SIM – Subscriber Identity Module card

II. TECHNICAL ASPECTS

A Definitions

Smart cards are divided into categories according to different characteristics. For the purpose of this report we use *function* and *access* as fundamental.

By function we recognise two categories:

A smart card is a card of an established form[3], incorporating one or more integrated circuits (IC), capable of storing data and giving access to information systems, containing a safety device, with its own identity, owned by a given person, single or multi-purpose, on an everyday basis. It carries a built-in microprocessor, enabling it to carry out intelligent functions. It has its own operation system and memories.[4]

A memory card is card that contains a memory-integrated circuit with low-level protection and secure technology.[5] Memory cards have been used in some health and social applications and in early telephone pre-paid applications. They are not widely used at present.

Cards are divided according to their type of access:

Contact smart card – this is a smart card with electronic contacts placed on the card for interface and communication with the outside world (application information system). Data may be read from the card memory only if the card is directly inserted into a card reader.

Contactless smart card – this is a smart card that uses low-frequency radio waves to provide power and to communicate with smart card readers.[6] Communication with the outside world is by means of an antenna wound into the card.
Some multiple applications use so-called Dual cards, with both types of technology for access to data.

A cardholder is a natural person whose personal data are stored on the card in his or her possession.

B Brief history of Cards

Smart cards as such are a European invention. The key moment is considered to be the patent of the French technician Roland Moreno of March 1974. This represented the culmination of international development and, by means of timely standardisation, made the industrial and application utilisation of this technology possible.

From the point of view of innovative steps, the following milestones are significant:

- memory cards - data carriers
In the following year, 1975, an ATM memory card was tested, replacing magnetic cards. This simple change of data carrier did not result in an improvement in data security; it was still

[3] The size of the card and the location of the integrated circuit are generally defined by an ISO standard (e.g. ISO 7816-2).
[4] The operating system for a smart card is usually installed on the card by the manufacturer and cannot be changed.
[5] With EEPROM (Electrically Erasable Programmable Read-only Memory) circuit.
[6] Most contactless smart cards can be read from a distance of about six inches. They can be read without being removed from a purse or wallet.

"publicly" accessible. What did occur, however, was a verification and confirmation of the practical utilisation of the new technology. This conclusion made it possible for the banking sector to unblock the investments needed for a change in the technology, which has now lasted for 25 years; it is a rational policy both from the point of view of high costs, as well as from that of the complicated integration of new, ingenious applications.

- microprocessor based cards
In the ten-year period from 1974 to 1984 a number of patents were submitted which made possible the introduction of industrial production of standardised smart cards. At the same time as Bull in France (1985), ORGA (Germany) presented the world's first multifunctional processor card at the CeBIT trade fair. It furthermore supported the authorisation of the cardholder with respect to the card and then also authentication (mutual verification) of the card with respect to the system in which the card was operating.
It is only thanks to the properties of a microcomputer that it became possible to start building systems that are essentially secure.

- extension for sophisticated operating systems on cards
Progress in the card's chip architecture was followed, after a certain interval, by progress in its software, particularly in increasing the quality of its operating system. The original design, reminiscent of the software monitors of single-chip microcomputers, was gradually replaced by professional operating systems, providing secure management of multifunction cards under the ISO 7816 standard.
While prepaid telephone memory cards were in massive use by 1990, their biggest application today (GSM) is in the first year of card orders.

- multi-functions and multi-applications solution
Following GSM's rapid take-off around 1995, applications aimed at other segments began to revive as well, particularly in banking, loyalty systems and secure identification as the basis for secure access to the Internet, e-commerce, e-health, e-government …

The capital costs of the general application of smart card technology are, however, too high (in the health-care and health insurance sector they may be estimated at 3-7% of annual turnover); for this reason a legitimate demand comes to the fore for multiuse smart cards for various purposes. In technical terms, there is nothing that would hinder such grouping of applications. From the point of view of uniform identification, data aggregation on the card, user profiling and data mining, however, the problems that emerge are hard to deal with.

The cards generally used today are mono- or multifunctional. In practice this means that they have a single issuer, administering the database of the cards issued, while the cards constitute its natural extension. The card issuer then administers the data on a contractual basis and makes their use possible within the scope of its own or contractual applications.

For future use—after 2001—it is anticipated that multi-application cards, very similar in terms of their character to a personal computer, will be distributed publicly. It will be possible to purchase such a card empty and each of its holders will be able to insert a set of applications in his card based on his own choice.

- enhanced security features
Smart cards belong to a family of technology which provides protected confidentiality of communications and authentication and verification of data subjects. This technology is called "Privacy Enhancing Technology (PET)". PET includes such techniques as encryption software, anonymous mechanisms of hardware use, biometric identifiers for secure and

confidential data transactions, and other techniques for preserving anonymous communication.[7]

Since about 1993, massive measures have been under development against fraudulent practices, brought about by the mass introduction of smart card applications (particularly involving unprotected memory cards). These measures, initially at the level of the producers and operators, culminated in 1997 in France with the establishment of SEFTI[8] (Information Technology Fraud Investigation Bureau) and BCRCI[9] (Central Service for the Suppression of Computer Crime); similar institutions have been established in other countries as well.
In order to increase the security of smart cards, two basic principles have been gradually applied since 1997-98.

A card is viewed as a specific product, whose properties are gradually upgraded: the implementation of multifunctional operating systems, with the ability to control access rights to data on the chip; further, by adding special-purpose hardware elements, such as random number generators, a cryptoprocessor, cryptographic key generators, detectors of unusual chip states and finally, self-destruction mechanisms, which destroy the card in the event of detection of an attempt at its abuse.

- development of the infrastructure
Even from this brief outline of the development of the card it is evident that its properties are in part, though not entirely, influenced by the quality of the overall smart card system design. Among the most important remaining components are secure terminals (particularly multi-application terminals), transmission records for the collection of transaction data and software for the data collecting servers and databases.
The legally binding standards and ethical rules have a substantial influence; without their acceptance the development of mass smart card-based systems could not be harmonised or operated.
In an effort to address and resolve these issues at international level, in 2000 the European Commission formulated the eEurope Smart Card Charter initiative, within the scope of Information Society Technology (IST) [10].
Smart cards are held in the possession of citizens and seen as private, personal and secure objects under their control. They are perceived as trusted tokens storing citizens' personal data. When using the smart card the citizen may be assured of security of access and operation, and will have consistent and easy-to-use service presentation.

C Overview of the available technology

Real running applications are mostly based on mixed technologies, which are used in parallel. In a review of card technology development from pure plastic towards the smart card (which contains an integrated circuit (IC) with an embedded operational system and application software), the basic classification might be:

The classification of the cards as a form of data carrier
All plastic cards provide the possibility to place visible data such as the cardholder's name or picture on the card surface. Some of the data could in consequence be machine-readable, for example via OCR[11] recognition. Some data are embossed into the plastic and are used to generate paper sheets related to the card transactions. Even visible, but incomprehensible,

[7] See e.g. Borking J.J.: On PET and other privacy supporting technologies (www.privacyservice.org).
[8] SEFTI – Service d'enquête sur les fraudes aux technologies de l'information.
[9] BCRCI – Brigade centrale de la répression de la criminalité informatique.
[10] see http://www.eurosmart.com
[11] OCR – Optical Character Reading

data (e.g. bar code) might be placed on the surface. All these provisions are dependent on card technology.
On the other hand certain data dedicated for automated treatment are to be placed in the chip, or written on the magnetic strip or laser-engraved into the optical field of the card. In such cases, in relation to the application design, data might be saved in open or encrypted form. Except for the data placed within the microcomputer chip, all data are still publicly accessible and must be treated as such. Even though not understandable for the cardholder, data can easily be extracted from the magnetic strip or optical field or non-protected memory in any appropriate reader.
The institution of once written memory has been used to protect memory cards from unauthorised issuing. Plenty of security provisions (originally developed for the printing industry – such as water marks) are used to secure the plastic body from being copied.

Enhanced processing
The microprocessor brings processing power and is used for essential protection, which comprises:
Management of microprocessor environment, physical and electrical conditions around the chip itself and possible auto-destruction facility.
Setting up and management of access rights to data structures located on the chip.
Generation of random challenge used for chip authentication.
Computation of electronic signature using private key and verification of the received ones.
On-chip data stream encryption and decryption.
Enhanced cryptocards provide key generation and essentially simplify PKI[12] installation, no private key dissemination is required.

Characteristics of the communication of electronic cards with the external environment
The smart card contains an integrated circuit with an embedded operational system and application software; it is in fact a small computer.
The standard way of communication between the card and the external world occurs by means of contacts mechanically fixed to the card within the card reader.
In some cases, users have difficulty plugging the card into the tiny slot, or the open slot of the reader is exposed to severe conditions which considerably decrease its reliability. Therefore contactless cards are successfully applied in compliance with ISO 14443 standard.
The contactless or dual card (contact + contactless card) might be remotely detectable, which seems to be a practical advantage, but brings in consequence the security risk of remote monitoring or the unintentional processing of card transactions.
Where other details besides the cardholder's personal identification data are being scanned, a contactless card should not be used.

Authentification of cardholders
Some technologies (password, personal identification number - PIN) are suitable for secure access to the distributed information systems. These technologies have minimal memory and processing algorithm requirements but in many cases may be seen as weak. They are not exceedingly safe and can be relatively easily misused.
Identifying the cardholder through biometric signs – finger/thumbprint, hand geometry (palm prints), retina scan, iris scan – is a safer form of identification. Biometrics describes an automated process used to verify an individual based on physical or behavioural characteristics. For biometrics to operate, a cardholder must provide an example of the particular characteristics that are to be used when verification is required. This process (called enrolment) allows the system to create a template of the characteristics (for example fingerprint image). Biometric verification is where the cardholder's template is compared with an offered characteristic. However, these technologies are more demanding for the memory carrier. This safe identification is suitable for off-line authorisation; the picture of the

[12] PKI – Public Key Infrastructure

biometric sign is stored on a chip card, not on the central system. Biometric identification does not require the cardholder to remember anything (e.g. alphanumeric chain, PIN, ID number), it cannot be guessed or broken.
For the authentication between the card and connected system the standard rules for computer networks are used, thanks to the on-chip microcomputer processing power.

D Application of Smart Cards

Smart cards offer a wide spectrum of possibilities for handling transactions involving personal data and thus facilitate the use of such data in many sensitive areas of application. The basic function of a smart card is data storage and transmission, as well as exchange between the individual parts of the given application's overall information system.

Smart cards are held in the possession of citizens and seen as private, personal and secure tools under their control. Smart cards can be used as a key element in providing user-friendly and secure access to those services they require and access to personal information in application (information system).

Smart cards are today used in many sectors - retail (electronic cash, loyalty systems), telecommunications (SIM cards, GSM), banking (payment transactions), security (access control), transport (road tolls, parking fees, bus/tram tickets, fuel stations), health (patient records, professional data, pharmaceutical), government (transaction between citizens and government bodies, keys for electronic signature), etc.

Today's division of smart card applications, however, is not sector-oriented, but is based on technical and security requirements. A dozen essential fields of smart card applications have been identified during broad discussion on new technology within eEurope public activity:

Public Identity

The aim of this activity is a common European Citizen Digital Identification Document. For this purpose, a qualified citizen's certificate[13] is needed. It will be a very important step towards e-government in the European member states. One of the benefits is enhanced data security. In general, smart cards may provide a unique relation between the citizen and its government.

Identification and Authentication

The target of this application is to contribute to a common, feasible and affordable security platform for all electronic transactions in need of identification and authentication.
Prior attention is focused on PKI and smart cards while it aims at supporting trusted services in need of identification, digital signature and confidentiality.

Protection profiles, security certification

The goal is to declare and facilitate the adoption of the specific standard[14] (through the smart card industry) for the evaluation and certification of products and systems, to provide trust and confidence to the smart card users.

Generalised card reader

[13] This certificate enables reliable authentication of citizen, encryption of data and use of digital signatures.
[14] Common Criteria (CC) - ISO/IEC 15408.

The aim of this activity is the specification of the architecture of general card terminals. These unified facilities enable secure interconnection of smart cards into the open networks, regardless of the type of card and sort of application.

E-payment and M-payment [15]

The prior objective of this activity is the adoption of smart cards as a means of secure payment. Strong requirement for interoperability across channels, sectors and countries is obviously necessary.

Contactless Smart Cards

Contactless smart card technology will be widely used in m- and e-commerce and in public transport systems. Necessary rules and regulations ought to address to two key overlapping areas - the industrial offer and end-user needs.

Multi-Application Smart Cards

The aim is to enhance the citizen's freedom of choice in the selection and management of the Information & Communications Technologies (ICT) services. The smart card seems to be the generic access token. The objective is to achieve a framework for open interoperable multi-application smart card platforms under strong security control.
Multi-applications of smart cards need technical coordination of all the components - smart card, chip technology, operating system and management activities.

Public Transport

The objectives are services supporting public transport utilising the smart card as the access token. It is also needed for interoperability between European transport ticketing systems utilising smart cards.

e-Government

The target is to achieve definition, rationalisation and implementation of a European model for procedures employing smart cards for interfacing the public administration; mainly to promote more effective use of government information resources, access to public services and simplify on-line administrative procedures. Utilisation of electronic signature, PKI infrastructure and Internet are essential needs.

Health care

Health care was one of the first areas of smart card application. The objective of joint European activities is to attain wide interoperability of health information smart cards for health care, emergency services, health and social insurance, pharmaceuticals, etc. It is necessary to set up the framework of legal regulations, professional standards and ethics relevant for the operation of health information systems in which electronic cards are used. These apply to patient data cards as well as to health professional cards and to their usage in networks, covering administrative data as well as health-care/health-related data; they could be seen as three different cards with different functions, e.g. ID-card, signature card and health card, which could of course also be combined in one card.

Advanced Electronic Signature

[15] Electronic payment and Mobile payment.

A new area of the application of smart cards is electronic signature. The target is to allow European citizens to carry out transactions in open networks, such as the Internet, with confidence and in multiple domains without restrictions.

E Specificity of data conservation, access and processing

Multipurpose – multifunctional utilisation of card terminals and smart cards as such makes the introduction of modern and expensive technologies affordable. However, it brings with it specific problems of how to share the technical resources, while at the same time guaranteeing that no conflicts occur in data storage and processing. Furthermore, it is essential to ensure that no conflicts occur in the case of indispensable external procedures—such as when data from various databases are merged prior to the personalisation of the smart cards, in the course of monitoring the circulation and customer complaints involving the cards, and in the course of distributing cryptographic keys into the cards and terminals.
From this point of view it is possible to distinguish three models based on the choice and administration of smart card applications:

Issuer centric model

The model is based on the administration of various applications exclusively by the card issuer. An example is today's banking systems, where the bank owns the card as well as the data contained in it and in various ways lends it to the client (cardholder). It is up to the bank to decide what data will be on the card (as well as on the terminals) and how they will be recorded, and the client must comply with the rules if he decides to use the system. He can, however, refuse to use the system.
Conceptually this model may be considered an extension of the current (e.g. banking) information system by an auxiliary card subsystem.
It is not suitable for obligatory systems, because if the cardholder is required to use a particular card, he must have an adequate guarantee that his personal data will be protected.

Service provider centric model

The model is based on the fact that some card issuers — typically GSM operators — permit their cards, in this case SIM cards, to be used for the procurement of services from other providers as well as for the payment of such services (e.g. in the case of purchases from automatic vending machines or in car washes using SIM cards, pre-paid applications, etc.). The safety of such a solution lies in the quality of the root identification (SIM) and in the quality of the safeguards for GSM transmissions, which limit the security of other applications.
In this model, however, the threat of information leakage is real. From a GSM application it is impossible to ascertain, for example, what anyone personally buys through the telephone SIM card, but it is possible to precisely localise the place and time of the purchase. A typical problem is the technical implementation of the servers on which such (GSM) applications run—these are very fast computers, equipped with memory banks, allowing very rapid response to transactions being elaborated in parallel. On the other hand, they aggregate an enormous quantity of data of sundry value—some intended for the GSM system's own operation, others for the processing of the providers of supplementary services.
Data warehouses might be set up effectively and provide exhaustive data mining. This is to be considered as a risky activity and requires supervision in terms of human rights protection. The main risk is to the data communicated through aggregated channels from where they might be extracted even without the knowledge and consent of the service provider.

Cardholder centric model

This is a model more or less applied in the Nordic regions. In an extreme case the interested party receives a freely distributed smart card (=pocket computer) and through a safe terminal, kiosk, etc., himself selects the applications that he wants to have on the card: citizen identification, certificate permitting electronic signature, health/social insurance, electronic wallet, prepaid or loyalty applications, home banking, etc.
In this case the cardholder is the owner both of the card as an object and of the data on the card. His ability to utilise and administer them securely depends on a pre-existing infrastructure. The infrastructure is produced by (from top to bottom):
a definition of the rules from the applicable legislation to generally accepted practices (e.g. to protect the PIN and not to write it on the card);
the infrastructure of connection locations—card terminals;
the available SW applications for the terminals and for the cards themselves—in the form of plug-in applets; and
the technological platform – this is the smallest problem; thus far we cannot safely, effectively and rationally utilise the technically feasible functions.

Specific risks associated with the processing of personal data with the help of smart cards

The increasing volume of data recorded on card memories increases the risk of attacks against the cards, or the data. There is thus a growing demand for the protection of information against unauthorised access and any unauthorised processing of personal data. It can be said that the success of the system in the application of a smart card depends on the protection of the data recorded on the card.
Among the most serious risks involving the use of smart cards is the processing of sensitive personal data. If sensitive personal data relating to the cardholder or his family members are recorded on the card, then it is necessary to be cognizant at all times of the fact that a number of authorised individuals have access to the data and, in the event of misuse of the card, other persons as well. In allocating access rights to the data (e.g. with the help of the card of a professional staff member) it is difficult to specify the individual measure of authorisation.
A specific risk of the abuse of smart cards is represented by applications allowing payment operations (credit cards, electronic purse, pre-paid card). Such cards are very often misused and have became an object of interest to those who wish to gain access to the cardholder's property (mainly funds) with the help of such cards. If these financial functions are combined with other uses of the card (multi-application card) then, in the event of an unauthorised operation with the card the objective of which is access to funds, other personal data recorded on the card, including sensitive data, become accessible as well. Thus, besides the original risk, an additional risk arises following from the unauthorised knowledge of sensitive personal data. This risk can however be prevented by not using payment operations on multi-application cards in combination with the cardholder's sensitive personal data.
For these reasons certain sensitive personal data should not be recorded on the smart card at all. This concerns, for example, data on race or ethnic background, religious affiliation, sex life. In some countries legal regulations prohibit including these categories of personal data on smart cards.
It is necessary to devote particular attention to health cards, if personal data on the state of health of the cardholder or that of members of his family are recorded in the memory chip. Discussions are still under way on the extent of the health data that should be recorded on the chip. No standard has yet been adopted, so that the individual countries are using in their applications (for the most part in the experimental or testing stages) various ranges of personal health data. In health care applications the smart card is used either as a key for access to health data, which are kept at a given location (generally with the attending or

family physician, at the hospital, etc.)[16] or as a carrier of selected data from the patient's (cardholder's) health documentation.[17] Nor is it appropriate to link a health smart card in a multi-application regime with payment functions or with functions unrelated to health care or social services, with health insurance, social security, etc.
The protection of personal data is related to the solution of two problems:

Access to personal data

In dealing with access to personal data recorded on a smart card, it is necessary to distinguish access by a cardholder
access by a third party.
The cardholder always has the opportunity to read the data recorded on the card. This approach is often dealt with by the installation of public booths, with the help of which the cardholder can confidentially read the data on the card.
Access to the data recorded on the card by a third party is a more complicated problem from the point of view of application. It is necessary to set up groups of authorised individuals who have access to the personal data and to grant them different degrees of authorisation. For example, a certain group of persons may be permitted to read only a limited amount of data, another group may have access to all data, someone may be permitted read-only access to the data, someone else can also change it, supplement it and update it. Various levels of authorisation are generally allocated to third parties by means of the so-called professional cards.[18]

Adoption of reliable cryptography

An important method of data security is software-level security. It has benefited from cryptology by incorporating a specialized co-processor. For a high level of security, smart cards encrypt data using the Public Key Technology (PKT) system. This cryptography system allows two entities to communicate in such a way that a third party is unable to read, determine or alter data in an on-line transaction (e.g. between the card-reader and the central database). Digital signature is one of the applications of PKT.

Notification

The smart card application relates to an increasing number of data subjects. Smart card memories allow for the recording of ever larger volumes of personal and other information. The risks arising from the inadequate use of security measures may infringe the privacy of the data subjects (cardholders). For this reason it is recommended that the national supervisory authority be notified of the use of smart cards in various applications.

III. LEGITIMACY ASPECTS

Smart cards offer not just a number of advantages in electronic communication, but they also entail risks for private citizens, particularly due to the fact that they make it possible to map out the transactions performed and thus to monitor the private life of their holders. These facts generate many legislative questions. In using smart cards it is often unclear who is the

[16] In principle it is not possible to accept the method of setting up databases containing patients' health data, whose administrator is an entity other than a healthcare facility.
[17] E.g. emergency data.
[18] A professional card is a smart card by means of which one can co-ordinate access by a third party to personal data. The application software first reads the data recorded on the professional card and, on the basis of the identification of the third party and the measure of authorisation ascertained, will permit manipulation with the cardholder's card.

"owner" of the personal data recorded on the card, who is responsible for their completeness and accuracy, who is responsible for card and system security etc.

With respect to the issue of the personal data recorded on the card, there is no question of the "ownership" of the personal data recorded on the card. Discussion on this must not be accepted. The cardholder is in possession of the card at all times and has total control over information concerning him. Personal data must be accessible regardless of who collects and writes the data on the card or into chip. The relationship between cardholder and other persons who collect and write personal data on the card must not limit access of the data subject to the data in any way.

In using smart cards as a technology for personal data processing, it is necessary to stipulate legislative, ethical and other rules for the protection of such data from unauthorised access, modification, publication or any other unauthorised processing. The extent and severity of these rules increase with the number of applications for which the personal data are used (multi-application). The multi-application use of a smart card entails an increasing aggregation of personal data on the card and hence also the risk of its abuse and the risk of unauthorised monitoring of personal privacy.

Alongside the growing number of applications in the case of multi-application use of the card, there is a growing number of rights and responsibilities that ought to be specified by legal regulations. In the case of multi-application use of smart cards it is necessary to address the rights and responsibilities of the card issuers, the data controllers and the cardholders. In the case of single-purpose smart card applications it is, on the contrary, possible to specify most of the rules by means of non-legislative regulations (e.g. by internal regulations, codes of ethics and principles, standards, etc.).

The majority of smart card applications contain personal data relating to an identified or identifiable person. They also contain many sensitive data and information pertaining to a person's intimate sphere. Legal regulations must therefore be found to guarantee the protection and confidentiality of personal data. The basic principles that must be respected in using smart cards are based on the following requirements:

A Adoption of Convention 108 principles

In the case of any use of smart cards using identification of the citizen in combination with his other personal data, it is necessary to observe the basic principles that have been laid down for the processing of personal data: the Convention for the protection of individuals with regard to automatic processing of personal data (ETS 108):

Personal data shall be obtained and processed fairly and lawfully
the application administrator (card issuer) processes personal data recorded on the smart card only for fair purposes;
the card issuer shall ensure that the personal data will not be merged by the use of any procedures whatsoever;
the card will include the personal data of the cardholder; no data recorded on the card will be used without the knowledge of the cardholder. The cardholder should be educated about smart card applications. Information must be transparent for the cardholder;
the cardholder shall have access to the data recorded on the card and the data will be made accessible to him in a legible and understandable fashion. The method of access to the data will respect confidentiality and the protection of privacy (not displayed together publicly);
If disclosure is made in case of emergency or protection of the cardholder's life or prevention of injury or serious damage to his/her property, the cardholder must be informed of that disclosure as soon as possible or practicable.

Personal data shall be stored for specific and legitimate purposes and not used in a way incompatible with those purposes
no smart card application may employ personal data for purposes other than that for which such personal data were stored in the card;
each application shall make use only of the personal data pertinent to the given application and to the extent essential for fulfilling the purpose of the application;
in the case of multi-application use of a card the personal data must be compartmentalised for the individual applications;
smart cards may not be used as an instrument for monitoring persons or curtailing their rights in any way. Any discrimination must be excluded;
third parties, to whom personal data are disclosed in the course of a smart card transaction, do not always need to know exactly who the cardholder is. In such cases it is sufficient for the cardholder to provide authorisation only for the given transaction.
Personal data shall be accurate and, where necessary, kept up to date
personal data, which are inaccurate, incomplete, or not up to date with regard to the purpose for which they were collected or for which they are processed, must be erased or rectified,
Personal data shall be preserved in a form which permits identification of data subjects for no longer than is required for the purpose for which those data are stored
the card issuer and the administrator of every application shall ensure personal data protection in the event of a loss, theft, destruction or other abuse of the card, as well as protection against copying of the card;
for a specific application, security systems shall be used that will ensure protection against access to the data by persons who are not parties to the application.
One of the basic principles is that the cardholder is the owner of information stored on the card. As has been seen above, the cardholder may or may not be the owner of the card itself. Ownership of information has certain implications: the cardholder has the right:
to know what data and functions are on the card;
to exclude certain data or information from being written onto the card;
to reveal at discretion all or some data from the card;
to remove specific data or information from the card.
Exceptions from the above-mentioned principles may be stipulated solely by law.

B. Domestic legislation

The minimisation and prevention of risks in the use of smart cards cannot be a matter merely for the card issuer or data controller. In the course of extensive or nationwide applications it is the government, the respective ministries and other state bodies that must play an active role (e.g. national application of the cards in the health care sector, in social security, in the tax system, in the insurance industry, etc.).

In the case of the card application of a nationwide extent or significance, it is necessary to define the rights and responsibilities of smart card issuers, controllers, processors and holders of personal data, safety rules, the content and organisation of the application, methods of verifying cardholders, supervision over the application and other areas of the entire life cycle of the card. These rights and responsibilities are defined by applying the principles promulgated by Convention 108 and other national legislation.

C Standardisation

Standardisation is a particular form of self-regulation. In standards there are three common characteristics: standards are *consensus-based*, *industry-wide*, and *voluntary*. There are also three main phases in the standard development process.
Activities in the area of standardisation, besides defining the technical criteria and parameters, focus also on other practice-oriented problems. In smart card applications the objective of these standardisation activities is also to define privacy standards, security and protection of

data, which will make it possible to apply the principles of Convention 108 in projects using smart cards. The national standardisation activities, for example, define the extent and structure of the data, including national identifiers. They also define the application standards for the collection, processing and utilisation of personal data and for access to them. The European standardisation effort creates the conditions for the interoperability of the individual national applications, i.e. their connectivity and applicability within Europe. The main role in this area is played by the International Organisation for Standardisation[19] (ISO) and the European standardisation organisations, such as - CEN[20] (European Committee for Standardisation), CENELEC[21] (European Committee for Electrotechnical Standardisation) and ETSI[22] (European Telecommunications Standards Institute).
The European Union defines Information Technology Security Evaluation Criteria (ITSEC), which define six levels of confidence. Each level of confidence corresponds to the overall strength of security mechanisms. One of advantages of ITSEC is that they can be used to evaluate a joint hardware-software system. The smart card is an ideal solution.

D Code of conduct

Article 5 (a) of Convention 108 states that personal data that are the subject of automated processing must be obtained and processed fairly and in conformity with the law. An analogous requirement is stipulated also by Directive 95/46/EC. A frequent subject of discussion is the fulfilment of the requirement to obtain and process "fairly". One of the ways of meeting this requirement is to specify the rules for correct and ethical conduct in the processing of personal data.

The penetration of modern technologies, including smart cards, is not always accepted with understanding by citizens. One of the reasons is fear of the violation of the individual's privacy and of the possible abuse of the personal data they contain. The data collected in the electronic card's memory banks are coming to the forefront of interest not only on the part of those who would like to misuse such data, but also of those who see in this technology a facilitation of their own activity – e.g. research, state offices, commercial institutions, the police, etc. Smart card applications are also often insufficiently transparent for citizens and their advantages and merits are not evident. The code of conduct specifies in a non-legislative manner the rules for the position and behaviour of the individual parties in the smart card project – industry, technology providers, card issuers, system operators, data controllers, service providers and cardholders. They address the linkages between the actual technology and its application. The code of conduct may be general or specific to the particular application of the smart card (e.g. health care, banking, telecommunication etc.). The principal effect of the code of conduct in smart card applications is the formulation of guiding principles for the collection, use, storage, disclosure and access of information, for the securing of personal data protection, the confidentiality of their processing and respect for the rights of individuals.

The code of conduct is an important part of the whole security framework of the project. Ethical issues influence the general acceptability of the project of smart cards by citizens (cardholders). A good solution guarantees that there are no risks for human rights and freedoms of citizens. If these issues and problems are not solved adequately, citizens (insured person, patient, etc.) may not use this card or only in very limited situations. This negative position and access of citizens also has a negative influence on the success of the project. There are not only legal but also ethical principles with regard to multifunctional card applications and sharing of personal data for different and incompatible purposes. In the

[19] ISO (www.iso.ch).
[20] CEN - Comité européen de normalisation (www.cenorm.be).
[21] CENELEC - Comité européen de normalisation électrotechnique (www.cenelec.org).
[22] ETSI - European Telecommunications Standards Institute (www.etsi.org).

ethical area it is necessary to solve the problem of how to assure a cardholder (citizen) that his personal data will be used fairly and lawfully. How to assure him/her that personal data will be read and processed exclusively by authorised professionals? How to ensure that, on the basis of his/her personal data, reading will not automatically produce legal effects concerning him? And many other issues must be solved because the "ethics" of the application of new technology is a precondition of its success. The code of conduct describes principles of "fair" behaviour for all participants in smart card applications (industry, card issuer, service providers, cardholder and any card-users).

E The Council of Europe and Data Protection Instruments

The protection of fundamental human rights and freedoms has been one the Council of Europe's principal activities since its founding in 1949. Data protection is understood to be a part of the protection of private and family life, home and correspondence, which was declared for the first time in Article 8 of the European Convention on Human Rights (1950). In this context, this right was developed by the Council of Europe in its Convention 108[23] (1981), which is the basic legal instrument for the processing of personal data. Convention 108 has thus far been ratified by 25 member states of the Council of Europe and signed by 8 member states.

Without any doubt, the principles of personal data protection set out in Convention 108 extend also to smart card applications, insofar as these applications operate with personal data. Data processing with the help of smart cards is always automated data processing and the principles of Convention 108 must be applied in all cases.

Besides Convention 108, the Council of Europe has issued 12 recommendations, 2 resolutions, 4 publications and some reports on the work carried out by the Council of Europe in the data protection field. Most of these documents are sector-oriented.
A new area of Council of Europe activities is the protection of personal data using new technologies in the daily life of citizens. Rapid progress in computing technology, telecommunications and other modern technologies raises new problems connected with damage to private and family life. This is the reason why the activities of the Project Group on Data Protection (CJ-PD) focus on these issues. Personal data protection on the Internet[24] and data protection in relation with surveillance[25] have been covered so far.
Since 1996, the Project Group on Data Protection (CJ-PD) has been engaged in problems of personal data protection used in smart cards. The Council of Europe issued the first document concerning this problem in 1985[26].

The full list of information and documents issued on data protection is available on the website of the Council of Europe[27].

[23] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[24] Recommendation No. R (99) 5 for the protection of privacy on the Internet.
[25] Data Protection in relation with surveillance activities (Report and Guiding principles).
[26] CJ-PD: Legal Problems Resulting from Official Machine-Readable Identification Documents. Council of Europe, CJ-PD(85)3, 1985.
[27] www.legal.coe.int/dataprotection/