Smartcards

These days, when information technologies uncompromisingly and with great pace permeate all spheres of everyday life, chip cards (smart cards) are being increasingly put to use. Many of them fill our wallets, other lie scattered around at home. We often don't know what purpose they serve or in what way they are an asset to our lives. In addition to credit cards, which are nowadays mostly equipped with electronic chips, there are a growing number of electronic documents such as passports, identity documents and vehicle certificates. Other documents, unfortunately little known to the general public, are used to implement advanced electronic signatures, system authentication or encryption.

Benefits of Smartcards

The main benefit of chip cards is the security of data stored thereon. Security is interpreted from the perspective of the chip itself - physical security, as well as from the perspective of the operating system - software security. With their technology, chip cards allow for the secure storage of data which varies in nature and purpose; they not only protect the data but also ensure their authenticity. Depending on the sensitivity of data, it is possible to request different degrees of protection to access data on the chip card. The simple ones require a PIN entry, the more complex ones use modern authentication protocols that not only authenticate the user, but also offer additional options for mutual authentication of the terminal and the chip.

For example, data such as the name and surname of the holder, card number, validity period, etc. stored on a payment card is protected from being read by a PIN code, i.e. by entering the PIN the holder agrees with the reading of data from the chip and thus authorizes the requested transaction. Data stored on the chip is protected from modification by means of an electronic signature by the bank that issued the payment card. Some cards are also equipped with protection against their contents being copied - so-called protection against cloning.

Security

With the progress in technology, modern cryptographic algorithms have been embedded in new chip cards, which not only extend the possibilities of data protection by means of authentication protocols, but also allow for the active use of chip cards in the electronic communication of citizens with public administration systems - eGovernment. In Slovakia, this includes e.g. the forthcoming national identification documents - eID. A document will contain data which can only be read by an authorized terminal. The terminal will authenticate itself against the chip using the so-called terminal authentication protocol, enabling the chip to evaluate terminal authorization for access to the stored data. The authenticity of the chip and data stored thereon will be ensured through chip authentication, in which a secure encrypted channel will be established between the chip and the terminal. The data can only be read with the consent of the holder by entering a PIN. A terminal with special permission, also called the inspection terminal, accesses data on the document without the consent of the holder. This includes police checks on persons.

The combination of the above authentication protocols also enables the establishment of a secure channel between the eID card chip and a remote system, e.g. an electronic service provider's server, enabling the server to verify the identity of a citizen in a guaranteed way and thereby authorize him/her to gain access to eGovernment services offered.

The access management method used in eID documents will enable their further enhancement with additional services such as an advanced electronic signature and encryption.