Use of smart cards for security applications by Deutsche Telekom

Bernd Kowalski

Deutsche Telekom AG, PZ Telesec

Untere Industriestr. 20, 57250 Netphen, Germany,

telephone: +49 271 708-1600, fax: +49 271 708-1625

X.400email: kowalski@04.sgn.telekom400.dbp.de

Abstract

Smart cards will be a key technology for secure electronic commerce and electronic payment applications on the Internet. They offer the unique advantage to keep cryptographic mechanisms securely in a tamper-proof equipment. Smart cards will be used for access control instead of passwords, for the generation of digital signatures, for encryption/decryption, as an electronic purse and as a repository of any confidential information.

Several years ago smart cards have mostly been used at card telephones and for banking applications and there usage was restricted to dedicated terminals like public telephones and ATMs. With the introduction of the health insurance card in Germany the first multi-application smart card terminals for PCs appeared on the market. Since 1993 prices for PC smart card interfaces dropped dramatically and made the card terminal a standard device for PC-hardware at least in Germany. In the following months the number of card applications for PCs and networks grows rapidly.

Already some time ago Deutsche Telekom recognised that Information Security will become a key issue for telecommunication companies. Telekom also decided that a big company's security should be independant from specific software or hardware suppliers. This strategy, however, required compatibility of security devices and applications between different products. This proved to be very difficult because of the lack of security standards and appropriate products on the market.

A Security Platform has been developed consisting of a number of security components like a smart card, a smart card terminal, a Trusted Third Party for keymanagement, a high speed PCMCIA encryption card, various authentication and encryption terminals and a security management system.

The smart card plays a key role in Telekom's information security strategy. The card includes a public key calculation unit for RSA, symmetric cryptography and a session key generator.

In 1995 Telekom started to issue smart cards for all its employees. Today more than 100.000 of them have access to information processing and all of them will use the card for digital signature, encryption and access control shortly.

Besides information security Telekom's „Company Card“ is also used for physical access to buildings and rooms, flexitime, electronic purse and electronic railway tickets. This makes the smart card very cost-efficient. On the other hand the card solves the problem of managing user passwords across different applications in a distributed and interconnected environment.

Several products will be offered to Telekom's customers with the smart card's security features. One important project is a country-wide intranet backbone. The network services are protected by a user smart card that provides for authentication and encryption between client and server. Applications use the smart card for signing electronic documents or to encrypt confidential messages. Keymanagement and card personalisation are performed by a Trusted Third Party and the network's directory service.

Deutsche Telekom has also developed a smart card solution to protect an ordinary analogue local loop. Also the operation of the management system of the digital exchanges in the telephone network (TMN) is protected by smart cards for operators.

Keywords

Access control, authentication, company card, cryptography, digital signature, encryption, public key cryptography, smart cards, Trusted Third Parties