SESSION ON SMART CARDS

TUESDAY APRIL 10

INTRODUCTORY REMARKS

by Alain TURBAT
DGT - Délégation Carte à Mémoire

Since a few years, smart card has began to appear in the field of cryptography. Today it is possible to hold a special session of Eurocrypt 84 on this subject because, after a period of experiments, the smart card is now becoming a commercial product, especially in France.

You all know what a smart card is : this standard dimensioned plastic card contains a micro electronics package including a memory and a microprocessor controlling read and write access to this memory.

This new card differs from magnetic stripes cards, not so much by its memory capacity, as by its internal computing power, hence its name : the smart card.

Cryptographic computation using personal secrete keys, is possible inside the card itself, allowing the smart card to carry out complex dialogues with the external environment. This permit a high degree of security in a large field of applications through processes of autenthication of the card, identification of the user, confidentiality of transmitted information, certification of a transaction by all the parties involved.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 457-458, 1985.

The card internal processing capacity, and its ability to store a non erasable record of each transaction provide an unrivaled degree of security and performances such that it will, during the coming decade, become one of the key elements in the expansion of electronic funds transfert, as well as an extremely reliable mean of identification for access to buildings, data banks, videotex services, pay TV channels and so on.

It would also be very helpful as a personal electronic file in applications that require portability and self contained security, for instance in the medical services field.

Therefore, by making information storage and processing possible anywhere, the smart card opens up new horizons in the design of networks, in regard to security and cost.

In France, the first project coming just now to mass production is the smart card payphone project. The French Telecommunications Administration have already ordered more than 10 000 payphones and one million cards including 200 000 with the microprocessor monochip designed by BULL, which are capable of both payphone and banking functions including point of sale, home banking and telepayment. Such a multifunction card will be used this year for all these applications in BLOIS, in the area of castles on the Loire.

All the French Banks and Financial Instutions have also decided to adopt a mixed smart/magnetic stripe card to be generalized in the whole country before the end of the eighties.

But the subject today is the link between smart card and cryptography which will be explained in many details by the different experts.

I suggest just to listen them.