Enabling Development of Applications for Smart Cards – Between Native Solutions and Javacards

Przemyslaw Kubiak and Miroslaw Kutylowski
Wroclaw University of Technology

Nowadays the smart cards aimed for ID-cards and e-administration services fall into two main categories:
native cards and Javacards. The first choice imposes lower requirements on smart card resources, whereas the second choice allows third parties to develop applications for the card, and thereby makes the product less dependent from the developer of its operating system (OS). This independence might be a crucial factor for choosing a solution to be deployed in a large scale. Indeed, in other areas of IT open architectures disseminate faster than its closed counterparts, and enjoys greater number of applications cooperating with the architecture.

We propose a new business model for smart cards' OS developers: ``earn on the service'' instead of “earning on the product''. Even if many details of the OS system would become disclosed, uploading an application would still require a strong authorization of the card producer personalized for a single card or a group of cards.

In order to realize this idea we propose to use a mediated version of Merkle Signature Scheme (mMSS). Among others mMSS fulfills the following requirements:

- with currently available techniques a mMSS signature of the software loaded on the card can be checked by card's microprocessor;
- signature verification protocol is very simple,
- the verification key is a really long term one, so it may be stored in a ROM memory of a card,
- the private key is divided between at least two parts, and if some of them become compromised they may be replaced without changing verification key stored in smart card.

----

emerging technology: multipurpose smart cards

class of cryptographic requirements: authorization system of third party applications for smart cards