

## Assessing the security strength of mobile applications endorsed by smart cards

Jan Verschuren  
TNO-EIB  
P.O. Box 5013  
2600 GA Delft  
The Netherlands  
[verschuren@tpd.tno.nl](mailto:verschuren@tpd.tno.nl)

A variety of mobile applications is expected. Applications in the field of tourism, ticketing/subscription, entertainment, education, health care, payments and m-commerce can be foreseen. All these mobile applications need to be based on the mobile infrastructure (GSM, UMTS, 4G). The user will be able to use these applications by means of his handset.

From functional point of view these applications are different. Also from viewpoint of security these applications are different as each application has its own set of security requirements, each application has to follow its own security policy. A security policy specifies what entities have access to sensitive data and specifies how information has to be protected.

An application will use so-called security services aiming to behave according to its appropriate security policy.

These security services need to be implemented in the different entities (handsets, nodes, backoffice) of the mobile infrastructure. Lots of security services are foreseen: confidentiality, integrity, authentication, authorization, non repudiation etc.

Implementation of these security services can be done in several ways as the developer can make use of a variety of security protocols, cryptographic algorithms and key management techniques. Thus security services are possible having different security characteristics and security levels.

Smart cards will play a role in realising the security services. A solution where each application is supported by its own smart card to secure the application is a cumbersome and an expensive one. A more efficient option is to use one smart card (SIM, USIM) able to support different applications according to its own security wishes.

Thus the smart card needs to support security services for a variety of applications.

The security services to be provided for by smart cards can be determined and derived in the following way.

- An inventory of mobile applications is made and it is determined what security services are needed. This can be done by performing a threat analysis referring to the applications.
- Specification of protocols  
Security services are realised by a combination of security protocols and cryptographic techniques.
- Specifying the functionality of the smart card  
A smart card needs to be devised which can perform cryptographic operations so that the requested security protocols can be executed. Besides it should protect the confidentiality of cryptographic keys stored inside the card.

When specifying protocols and functionality of smart cards, the following items are important.

- Interoperability  
For smooth communication it is required that the communicating entities interpret exchanged data in the same way. Consequently, the security services implemented at communicating entities need to be implemented in a matching way. This points to the need for *standardisation* of security services.
- Acceptance by the entities whose information is protected by the security services.

This refers to:

- Security strength  
Information cannot be protected properly by insecure techniques. Therefore it is essential that one knows the strength of the applied security techniques.
- Implementation choices  
Entities whose information needs to be protected will not accept certain options for protecting their information. E.g. financial institutions will require end-to-end security and not accept that their information is protected by means of keys also used for protecting other – non financial – applications.

Acceptance of proposed security services asks for the need of *evaluation and certification* of implementation of security services.

Now a few remarks on security evaluation and certification of protocols and smart cards are made.

- In order to become sure about the qualities of the security protocol it is best to evaluate the protocol in a formal way. This points to techniques like CSP. Techniques like these need to be further developed and refined in order to give a final security opinion on implementations of cryptographic protocols.
- Concerning the evaluation of smart cards there are some hurdles to take.
  - There is no agreed set of security requirements concerning the smart cards.
  - On a regular basis, new attacks on smart cards emerge (e.g. SEMA/DEMA: Simple/differential Elettromagnetic Analysis). This makes comparison of evaluations of smart cards difficult. Initiatives are being undertaken to qualify labs in this respect (TB3/SG2).
  - Financial institutions are not fond of CC as it is a quite lengthy, expensive and cumbersome evaluation methodology. Thus making a certification of smart cards difficult.
  - It is expected that biometric techniques will be applied in the future. Smart cards have to be adapted in this respect.
  - Smart cards will be loaded with programs (e.g. written in JavaCard) from outside. Verification of the functionality of these programs before executing is essential from security point of view.
  - On a multi application smart card, it must be possible to separate applications from each other so that they do not affect each other in an illegal way.