Cryptographic Application of Programmable Smart Cards[*]

István Zsolt BERTA – Zoltán Ádám MANN
smartcard@ebizlab.hit.bme.hu
http://ebizlab.hit.bme.hu/smartcard

Budapest University of Technology and Economics
Department of Telecommunications

Internet Security and Financial Mathematics Application
Research & Development Laboratory (E-BizLab)

Smart cards have been utilized excessively during the last couple of decades. In recent years though, a new generation of smart cards evolved: programmable smart cards. The distinguishing characteristic of these cards is not merely the presence of a CPU, but rather the ability to load and run separate programs.

In a complex, smart card based system this feature turns smart cards from passive data-storage devices into active computational units. In fact they contain a tamper resistant secure one-chip microcomputer able to execute various cryptographic functions. Moreover, their potential can be extended after the issuance of the card by uploading various new applications. However, the limited resources of the card (e. g. 4Mhz 8-bit processor, 8 kilobytes of storage capacity) require special programming methods and restrictions.

Programmable smart cards are – although for years on the market – still not widely used. This is partly because of their higher price: in multitudinous applications (such as phone cards) the performance of non-programmable smart cards is in most cases sufficient and high manufacturing costs of the cards are intolerable. Therefore, the adequate operational area of programmable smart cards remains a subject of intensive research. It is probably in systems with great security expectations that programmable smart cards can play a substantial role because they are capable of executing cryptographic algorithms on their own. They are downward compatible to traditional cards and can be inserted into the same readers, or as SIM cards (such as Bull's SIM Rock 'n Tree), inserted into the same mobile phones, as their ancestors.

The authors had the opportunity at E-BizLab to develop security-oriented applications on different programmable smart cards of different vendors and architecture. Microsoft Smart Card for Windows Professional and Bull Odyssey 1.2, cards designed by two concurrent manufacturers on the market, were studied.

[*] This is an outline of our presentation at Nokia Hungary, 16th February 2000.

The first card examined more closely was Microsoft Smart Card for Windows Professional. It is not long ago that Microsoft decided to join the smart card market, therefore the card and the development kit (based on Microsoft Visual Basic) are still in beta. This fact had some negative consequences: incomplete and inconsistent documentation, some not implemented functions, bugs etc.

However, this card possesses a cryptographic coprocessor that supports DES (Data Encryption Standard), a standardized encryption mechanism so the authors decided to build their cryptography package on DES. The following features were implemented: encryption and decryption using ECB and CBC, message authentication (MAC) and card authentication. The results suggested that all major cryptographic schemes can be safely implemented in a smart card environment; the most crucial factor is speed. Authentication of a long message can take hours if the whole procedure is done by the card. As an alternative the authors suggest the usage of a one-way hash function on the PC side to minimize the amount of data actually transferred while maintaining the sufficient degree of security.

On the other hand an implementation of Sun's Java Card specification was examined. In contrast to the card described above, this type has already been used so it has a more sophisticated and reliable structure. However, this card possesses no cryptographic coprocessor so the authors were constrained to implement only a simple coding algorithm (one-time pad) that can work efficiently without hardware support.

Odyssey 1.2 was manufactured by Bull Corporation and can be programmed in the Java programming language. The Java Card specification uses the Java language as a platform-independent development tool. Various manufacturers produce cards that conform to the Java Card specification, thus making applet development manufacturer-independent.

Since applications can be uploaded onto the card after the manufacturing process, application development is possible without the expensive devices of IC technology. This trend separates two parties: card manufacturers and card issuers. Card manufacturers would not have to produce different cards for each issuer's purpose, a programmable multi-purpose card would suite the needs of all issuers, who could customize and personalize their cards for the end users. Since only minimal equipment is needed for this personalization, even small companies could issue smart cards. This would allow new participants to enter the market and also allow card manufacturers to produce only a few types of cards, but produce them in a large number. This would break down prices and make smart card technology cheaper.

This is the main economical significance of programmable cards. The other main significance is cryptographic. Since any algorithm could be implemented on the card, the issuer would have wider possibilities than those the manufacturer planned for it. Intelligent smart cards could also be blessed with the ability of decision making, thus expanding the possibilities and cryptographic power of the technology. A smart card is a device designed to hide and protect data. An intelligent smart card extends the traditional one by containing not only data but also the operations on it. The idea is similar to the object orientated concepts of encapsulation and information hiding. The data (e.g. a cryptographic key) is stored on the card, but cannot be accessed directly, only through pre-defined gateways: operations. These operations are provided by the applications running on the card thus improving the flexibility of the secure system.

From the results of their research the authors conclude that programmable smart cards do have a great potential in cryptographic computations. These new possibilities will most probably reshape the smart card world and sensitive applications in particular.