Using Smart Cards in an Educational Environment

Services and Security Features

COSTAS LAMBRINOUDAKIS

Department of Information and Communication Systems, University of the Aegean, 83 200 Karlovasi, Samos, Greece - email: clam@aegean.gr

Key words: Smart Cards, Education, Certification, Authentication, Data Security

Abstract: The immense advances in the area of information technology and more specifically in the fabrication techniques of integrated circuits, has allowed the manufacturing of *Smart Cards* that feature processing capabilities through an embedded microprocessor, erasable memory and a variety of security features through the execution of cryptographic algorithms. This paper presents the main functional, architectural and security characteristics of a smart card pilot application for an Educational Institute, together with the resulting benefits for both the students and the institute. A detailed description of the way that the smart card security features have been capitalised for implementing certification and authentication mechanisms is also provided.

1. INTRODUCTION

The use of smart cards is entering a period of real sustainable growth. Key factors are: improvements in the technology, progress in standardisation[8], and a number of external factors such as the growing level of fraud in related fields. As opposed to memory cards which contain a few bytes of reusable memory and some type of hardwired security for protecting the card from being tampered with[9], smart cards have an intelligent, single chip micro controller embedded within the plastic[5]. This facilitates the implementation of a very high level of data security and means that data can be securely updated or written to the card after it has been issued. The key development in recent years has been the integration of reusable memory --Electrically Erasable Programmable Read Only Memory

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

(EEPROM)-- onto a single chip micro controller[9]. As a result it is now possible to readily change and update data, and even to add new applications, after the card has been issued. The aforementioned smart card advantages, have become the driving force for many organisations around the world to adopt this new ICC technology for many distinct application areas like electronic purse[5], mobile phones[6], health, network security [13,14,15] etc.

In this paper we will present the overall architecture and the functional specifications of a smart card pilot application that has been designed and developed for an educational environment. Special emphasis has been given to the security mechanisms implemented, in the framework of that application, for ensuring the integrity and confidentiality of the information stored on the smart cards, as well as on the protocols employed for authenticating the cards[7].

2. SMART CARD ARCHITECTURE

The smart card used in the pilot application is a 24 Kbits card from BULL CP8. The component embedded into the card is a true microcomputer driven by a microprocessor controlling three types of memory[3].

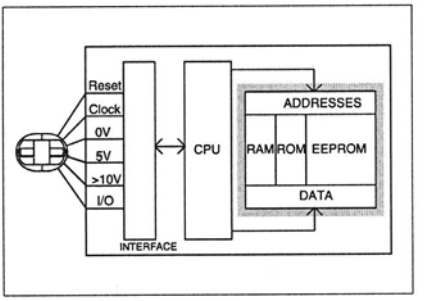

Figure 1. Architecture of the Smart Card Microprocessor

The **working memory** (RAM: Random Access Memory) which loses its data when its power supply is disconnected and is therefore used by the processor for temporary storage only.

The non-erasable **program memory** (ROM: Read Only Memory) which retains its information even when the power supply voltage is removed. This non-erasable memory is etched when the chip itself is manufactured. It contains the **operating system** which supports the card's *intelligence* and *security features*[2,4], by providing services for the everyday operations, key management and cryptographic algorithms.

The **user memory**, that is blank when the chip is manufactured. This is programmed, or written, by electrical means, during the card's life cycle. It can be also erased and re-written (EEPROM technology). It normally stores information about the card owner and other application specific data. Organised in 32-bit words, this memory's capacity increases as technology progresses (2, 8, 24 and 64 kbits in EEPROM). The user memory is divided into distinct areas, each one accommodating specific data categories and implementing different access control mechanisms. These areas are:

Secret Area: This area can be written only once and there are no physical or logical means that can be used for reading it from the outside[1]. The secret area accommodates different types of keys:

- the **manufacturer's** key protecting the chip from the very beginning until the point that it has been personalised.
- the **card issuer's** keys (Primary Issuer PIK, and Co-Issuer CIK) protect the application data against unauthorised read, write or erase operations.
- the **card holder's** keys (Personal Identification Number - PIN) are assigned to the person to whom the card is issued.
- the **Secret** Code used by mechanisms against counterfeiting and forging, for verifying that a card is used by authorised users and also for the computation of electronic signatures attached to a text.

Access Area: This area automatically records the keys submitted for accessing protected information, keeping a profile of access attempts with correct or incorrect keys and reacting by barring access when repeated errors lead to suspicions of fraud.

Public Area: As its name suggests, this area stores information of a public nature that can be freely accessed. It is usually used for non-confidential identity information.

Work Area: This is probably the most important area, from the application's point of view, as it is the part of the smart card memory accomodating the data throughout the card's life cycle. Depending on the application, this information may be read protected and/or write protected and/or erase protected through the appropriate keys.

3. THE APPLICATION OF SMART CARDS IN AN EDUCATIONAL ENVIRONMENT

The pilot system that was designed and implemented has capitalised on the smart card technology for easing the stiffness and bureaucratic procedures of educational institutes. It can significantly contribute towards:

- the modernisation of the organisational and operational sector of the educational institute,

- the reduction of its operational expenses,
- the extension of the services offered to its members and finally,
- the development of the necessary infrastructure for flexible co-operation with other educational institutes or independent organisations.

The simplification and acceleration of various operations is achieved by utilising smart cards for organising and transferring information like:

- Student data (personal, educational, financial and other specific information categories).
- Teaching staff data (such as the position of the staff, his/her salary status, his/her authorities and activities).
- Administrative personnel data (working position, salary status, holidays, overtimes etc.)
- Data related to other facilities / services offered by the institute (libraries, university clubs, student's dormitories etc.)

The architecture of the pilot system is depicted in Figure 2.

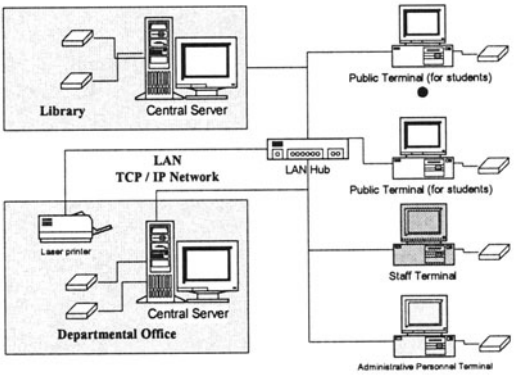

Figure 2. System Architecture

It becomes clear that although the system is functionally integrated, architecturally it can be easily divided into two subsystems, namely:

- The central site (one for each service category- departmental office, library etc) that maintains a database for managing all related information (for example personal and educational student data). This subsystem is also provided with specialised software for managing (issuing, erasing, un-locking etc) the user smart cards.
- The interactive terminals (for students, teaching staff, administrative personnel etc) that actually "offer" to the "users" the supported services.

In order to provide the reader with a more detailed description of the application's main features and design characteristics, the functionality of each subsystem, in respect to the services offered to the students, is presented next.

3.1 Central Site

The departmental office maintains a database organising all personal and educational student data, information about the courses offered by the department, as well as other specific information. The main data categories stored in this database are: (a) Personal Information for all undergraduate and postgraduate students of the department, (b) Information related to all courses offered by the department, (c) The examination results (marks) for all undergraduate students, (d) The courses that each student has chosen to attend for the current semester, (e) The departmental timetable for the lectures of the current semester and (f) The exams timetable.

In addition, the departmental office is provided with specialised smart card software in order to: (a) *Issue student smart cards*: During this operation a brand new smart card will be personalised for a specific student, meaning that the student's personal data will be fetched from the database and will be written to the smart card memory. Also the smart card keys and secret codes will be specified, (b) *Update student's smart card*: In case that the student's personal information, stored in the central database, has changed (for example his/her home address), his/her smart card will be also updated, (c) *Erase smart card data* and (d)*Un-lock a smart card* that has been previously locked due to the submission of a wrong PIN for three consecutive times.

Activation of the aforementioned functionality is only possible after presenting to a smart card reader a specially designed "authorisation" card that stores the necessary authorisation codes.

3.2 Student Public Terminals

Using their personal smart cards, students will be able to utilise the available public terminals for getting information about their performance and other educational and departmental issues. More specifically the functionality provided by the terminal application is the following:

- List all courses that the student will attend during the current semester.
- List all courses that the student has attended from the very beginning of his/her studies, including information like the academic year, if the course was compulsory or optional, the exam mark etc.
- List the grades for all exams that the student has passed.
- Provide a personalised lecture timetable.
- Provide a personalised exam timetable.
- Request progress/marks certificates. The departmental office's network printer will immediately print these certificates. After they have been signed they will be distributed to the students.

It should be stressed at this point that every time that the student presents his/her smart card to a terminal the educational information stored in the card is automatically updated from the central server, without requiring any user intervention. Therefore if, for example, new exam results have been entered in the central database they will be also passed to the smart card.

The 3 Kbytes (3.072 bytes) of the smart card's EEPROM memory have been divided into the areas depicted in figure 3.

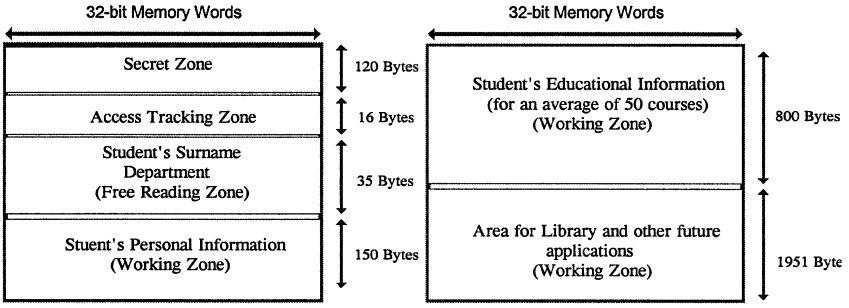

Figure 3. Memory allocation

The Working Zone of the smart card's memory is read protected with the card holder's key (PIN), while it is write and erase protected with the PIK (department's) key. In this way the student can only read the contents of his/her card without being able to erase or modify any of the information.

4. SECURITY MECHANISMS REALISED

Applications based on smart cards can enjoy the advantages offered by specialised "*Security Modules*"[2], mainly used for managing security and cryptographic functions and thus protecting the system from possible attacks resulting from its operation in an open network environment[10,12]. *The combination of such security modules with smart card applications can ensure the integrity and validity of remote transactions over Local but also Wide Area Networks.*

4.1 Smart Card Personalization

Before the smart card enters its *utilisation phase* it must be *electrically personalised.* During this operation the secret keys and codes of the smart card are set and the read/write/erase attributes and size of its memory areas are specified (see Figure 3 above). The procedure followed for the generation of the secret keys and codes is presented below.

In order to protect the confidentiality of the secret keys/codes that will be stored in the student cards, their generation is based on the diversification of a *master secret code* stored in a *security module* (*mother smart card)* that has been installed in the central departmental server. As illustrated in Figure 4, the input parameters used for the execution of the DES algorithm (which is supported by the specific card we used) are: the aforementioned master secret, a predefined memory address of the security module, the contents of this address and the serial number of the card to be personalised.

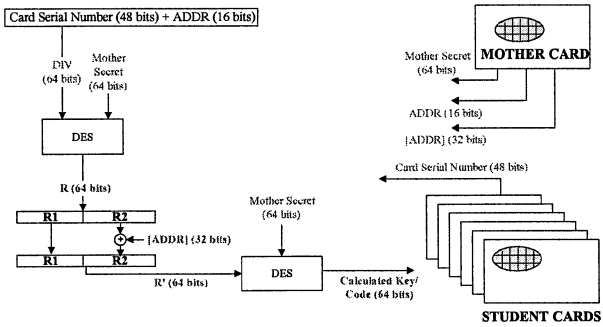

Figure 4. Smart Card Electrical Personalization

The security module memory address used for the diversification procedure is different for each secret key/code (secret, PIK and CIK) of a smart card, thus ensuring their uniqueness. Furthermore, the fact that the serial number of each card is different ensures that no two student cards can have the same secret key or code.

An exception to the above procedure is the specification of the card holder's key (PIN), which is defined and communicated to the card owner by the departmental office in clear text. The student can then change his/her PIN from any of the available terminals.

4.2 Certification of Student Smart Card Updates

Certification is useful to check the validity and integrity of a transaction. As already mentioned in the previous sections, when a student inserts his personal smart card in a public terminal the information stored in it is updated with any new information that has been stored in the central database of the departmental office (for example exam results).

In order to enable the central application server to check that the correct information has been recorded in the desired memory address of the student's smart card, the following *certification mechanism* has been implemented.

As Shown in Figure 5(a), the central server, through its security module, *asks* the student's smart card to generate a certificate using a random number RND and the memory address ADDR that the information is stored. The same certificate is calculated by the security module and is compared with that of the smart card. If the certificates are found to be the same then the correct information has been stored in the right memory address.

The steps realised by the certification mechanism are listed below:

Certificate Calculation by the Student Smart Card

- The security module generates and sends to the smart card a random number (RND), together with the address (ADDR) of the memory location that will be certified.
- The smart card executes a DES algorithm using this random number (RND), the card's secret key, the memory address (ADDR) and the contents of that memory location ([ADDR]). In fact this calculation involves a double-DES execution in a fashion identical to that shown in Figure 4, with the only difference that a random number RND is used instead of the card's serial number and that the memory address ADDR refers to the smart card memory and not to the security module.
- The result (R) of this calculation is sent by the smart card to the security module of the central application server.

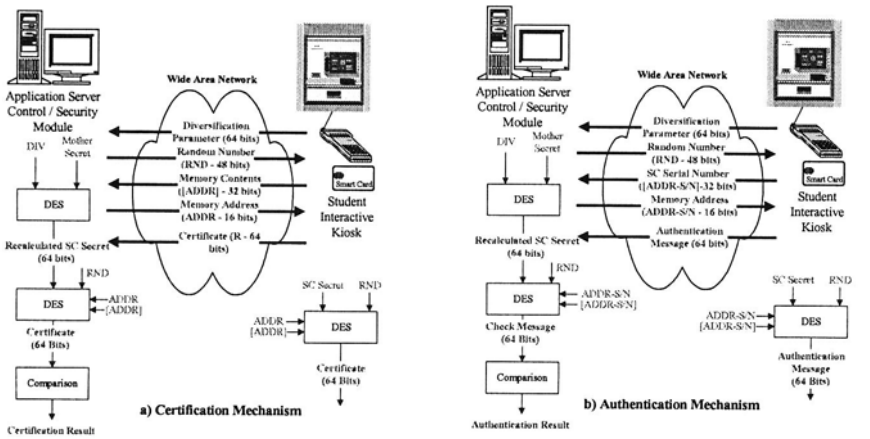

Figure 5. Certification - Authentication Mechanisms

Recalculation of the Smart Card Secret by the Security Module

- The smart card generates and sends to the security module the diversification parameter (DIV).
- The security module re-generates the smart card secret code in a way identical to that presented in Figure 4.

Certificate Calculation by the Security Module

- The smart card transmits to the security module the contents ([ADDR]) of the memory address ADDR.
- The security module utilises the re-generated smart card secret in order to calculate the certificate R in a way identical to that of the smart card.

Check Certificate

- The security module compares the locally calculated certificate with the one calculated by the card. If the certificates match then the information stored in the memory location with address ADDR is correct.

It is important to notice that no secret keys or codes are transmitted over the network. The only *sensitive* information transmitted is the certificate R that the smart card has calculated, which, however, will be never repeated since the random number involved in the calculation will never be the same.

4.3 Student Card Authentication

The authentication mechanism is used for enabling the central application server to check that a card presented to a public terminal has been issued by the department and is valid. As illustrated in Figure 5(b) the security module *asks* the smart card to generate an *authentication message* using a random number RND and its serial number. The same message is then calculated by the security module locally and is compared to the one produced by the card. If the two messages match then the card is authentic.

The steps realised by the authentication mechanism are identical to those described for certification, involving the calculation of an authentication message by the student's card, the recalculation of the smart card's secret and a calculation of a check message by the security module. Next a comparison of the two messages is performed. Also during authentication the address of the memory location storing the student's card serial number (ADDR-S/N) and its contents ([ADDR-S/N]) are used (see Figure 5(b)).

As already pointed out for the certification mechanism, during the authentication process no secret keys or codes are transmitted over the network. Furthermore, the use of the random number ensures that the calculated authentication message will never be the same.

5. CONCLUSIONS

A pilot application of the smart card technology in an educational environment has been presented in this paper, demonstrating enhanced flexibility, interoperability, less bureaucracy, financial gains and a high degree of security, in respect to the confidentiality and integrity of the

information managed. Special emphasis has been given to the certification and authentication mechanisms that have been developed.

However, the threats that an information system is facing are frequently complex and varying. Furthermore, the continuous technological evolution results in more sophisticated and hard to identify threats. It is therefore clear that information systems should be continuously evaluated in respect to their security procedures using well established risk analysis methodologies and if possible allow for a dynamic countermeasure activation scheme[11]. We believe that the intelligence and processing capabilities of smart cards and that of the associated security modules can be further exploited for the implementation of security mechanisms towards that direction.

REFERENCES

1 Bruce Schneier, Adam Shostack, "Breaking Up is Hard to Do: Modelling Security Threats for Smart Cards", Proceedings of USENIX Workshop on Smart Card Technology, Chicago May 1999, pp.175-185.

2 Bull CP8 "*Operating Systems - Security Modules*", Ref: TU 0208 A01, 1992, France.

3 Bull CP8, "*Smart Cards User Guide*", Ref: TU 0221 A01, 1993, Bull CP8, France.

4 C. Markantonakis, "*The case for a Secure Multi-Application Smart Card Operating System*", Information Security Workshop 97 (ISW97), September 1997, Springer-Verlag (LNCS 1396), pp. 188-197.

5 Carol Hovenga Fancher, "*In your pocket: Smartcards*", IEEE Spectrum, February 1997.

6 European Telecommunications Standards Institute, "*Digital Cellular telecommunication systems, Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface*", ETSI GSM 11.14.

7 Gritzalis D., Katsikas S., "*Towards a formal system-to-system authentication protocol*", Computer Communications, Vol. 19, no. 8, pp. 954-971, 1996.

8 International Organization for Standardization, "*Identification Cards - Integrated Circuit Cards with Contacts*", ISO 7816.

9 Jose Luis Zoreda, Jose Manuel Oton, "*Smart Cards*", Artech House Inc., 1994.

10 Katsikas S., Gritzalis D. Spirakis P., "*Attack modeling in open network environments*", in Proc. of the 2nd IFIP Communications and Multimedia Security Conference, pp. 268-277, Chapman & Hall 1996.

11 Labuschagne L., Eloff J., "*The use of real-time risk analysis to enable dynamic activation of countermeasures*", Computers & Security, Vol. 17, no. 4, pp. 347-357, 1998.

12 Louis Guillou, Michel Ugon, Jean Quisquater, "*The Smart Card: A standardized security device dedicated to public cryptology*", Contemporary Cryptology. The Science of Information Integrity, ed. G.J. Simmons, IEEE Press 1992, pp. 561-613.

13 Michael C. McChesney, "*Banking in cyberspace: an investment in itself*", IEEE Spectrum, February 1997, pp.54-59.

14 Naomaru Itoi, Peter Honeyman, "*Smartcard Integration with Kerberos V5*", Proceedings of the USENIX Workshop on Smart Card Technology, Chicago, May 1999, pp. 51-62.

15 Tom Verschuren, "*Smart access: strong authentication on the web*", Computer Networks and ISDN Systems, 30, 1998, pp. 1511-1519.