Non Conditional Smart Card Technology to Deliver Personalized iTV Services

Giorgio Rascioni
Università Politecnica delle Marche
D.I.B.E.T.
Via Brecce Bianche 12
60131 Ancona Italy
00390712204129
g.rascioni@univpm.it

Susanna Spinsante
Università Politecnica delle Marche
D.I.B.E.T.
Via Brecce Bianche 12
60131 Ancona, Italy
00390712204894
s.spinsante@univpm.it

Ennio Gambi
Università Politecnica delle Marche
D.I.B.E.T.
Via Brecce Bianche 12
60131 Ancona, Italy
00390712204845
e.gambi@univpm.it

ABSTRACT

Among the most important innovations brought by the introduction of Digital Television, interactive MHP (Multimedia Home Platform) applications have a prominent role. This paper describes in detail how non conditional access smart cards may be used to allow the realization of personalized iTV services through properly designed MHP applications, to widen the benefits that separately come from a broadcast pervasive technology and smart card security, and thus creating synergies between information, technologies and processes. We also assess the performance of available cryptographic procedures by comparing their execution on enabled commercial digital terrestrial television receivers.

General Terms

Algorithms, Performance, Design, Experimentation, Security.

Keywords

Interactive TV, smart card, cryptography, usability, T-government, security.

1. INTRODUCTION

We live in the digital era, where the transition from analog to digital gave a strong boost to the innovations that are changing the way of creation, consumption and redistribution of services, under new business models, and through new telecommunication technologies. In this context, firms, institutions and, more in general, every type of public or private entity would like to offer advanced services to accomplish the needs of citizens, in a pervasive way. To this aim, services are requested to provide a level of personalization that implies critical issues, due to the private nature of the information exchanged. Avoiding unwanted access to personal information is fundamental to ensure a certain level of security; as a consequence, modern systems have to face issues that completely belong to the field of cryptographic technologies [1],[2].

As a general term, cryptography defines a set of techniques, procedures and algorithms that, among several possible options, allow to hide data of different nature, such as audio, video, textual data and so on, to unauthorized users. Cryptography provides efficient and powerful ways to ensure information integrity and secrecy, but the robustness of cryptographic techniques may be weakened by the difficulty to adequately protect private keys. Microprocessor smart card technology may overcome this issue thanks to the intrinsic anti-tampering protection provided in the internal microchip, mainly due to the presence of a cryptographic co-processor able to perform the main functionalities on board [3], without releasing any key material stored in the card. As a consequence, at present the smart card technology is becoming the most viable and solid solution for the development of personalized secure services, supporting digital signature as a tool for authentication, integrity, and non repudiation, and the private key-digital certificate pair for strong authentication and confidentiality. Hence, progressively, a number of entities, especially public institutions, are migrating their own set of services into on-line, Internet-enabled service infrastructures based on the PKI (Public Key Infrastructure) architecture. A general view is shown in Figure 1, where user access to a service is provided by the release of a suited smart card.

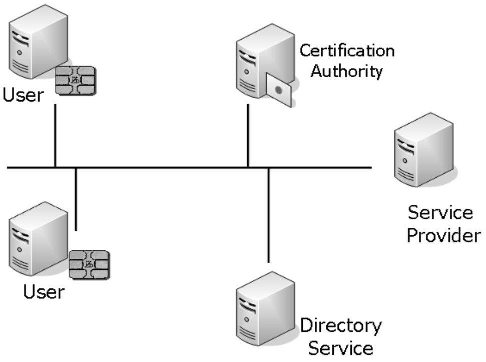

Figure 1. General view of a PKI based service architecture

In the digital TV environment, the smart card technology has been adopted since a lot of time, but only as a tool for implementing Conditional Access to specific, pay-per-view contents. Actually, a new set of applications using smart cards in the TV environment may be designed, exploiting the interactivity supported by the digital television, to widen the user experience, by simplifying the way of accessing information recovered also directly from the Internet network. Hence, the possibility to manage a non conditional access smart card by the iTV decoder opens the way to new scenarios, to move services of the Internet PKI infrastructure inside the TV environment. Several interactive services may be conceived, exploiting the peculiarities of smart card based security and authentication, such as job finding ser, learning and education , banking and financial services. The basic requirement is the possibility of accessing the smart card device through the MHP interface, in order to ensure user authentication and protection of personal data exchanged over the available return channel.

In this paper we focus our attention, as a case study, on the possibility of extending to the iTV context services involving the use of the recent Italian smart card standard called NSC, i.e. National Service Card [4], born to favor a convergence between different digital identification solutions. Actually, the most part of our considerations is valid also for other types of non conditional smart card based solutions. In particular, we discuss possible cryptographic procedures, and their application, when the use of the NCS is extended to the interactive television context, by means of suitably developed MHP interfaces, and provide some performance evaluations focusing on user experience and comfort.

The paper is organized as follows: Section 2 briefly presents details about the MHP technological infrastructure, discussing how it is possible to manage smart cards through MHP applications, to implement the procedures made available by the NSC. Section 3 outlines the NSC chosen as a case study, its file-system design and related cryptographic procedures supported. Section 4 reports the results of experimental tests; finally, Section 5 concludes the paper.

2. SMART CARD MANAGEMENT IN MHP MIDDLEWARE

The Multimedia Home Platform [5] is a set of Java based open middleware specifications designed to add interactivity to the DVB-T transmission technology. In a digital terrestrial television receiver, the MHP middleware can be thought of as an operating system, that has the role of managing the hardware and software resources, handling and executing all the operations related to iTV applications and user interaction. Among the resources handled by the MHP middleware, the smart card reader is included, usually involved in the decoding of received pay-per-view programs within a CAM (Conditional Access Module) component, which also comprises a specific decoder for the received encrypted signal.

Almost all the commercial receivers provide at least one smart card reader slot, that is compliant to the physical and electrical standards defined in [6], and can be consequently used to communicate with a compliant smart card. Since the 1.0.3 profile, the MHP specification has introduced the SATSA (Security and Trust Services) Application Program Interface [7] as the reference environment for smart card interfacing. The SATSA package contains a set of programming interfaces dedicated to security and cryptographic functions. Among all the functionalities provided by SATSA, two sets of functions have to be necessarily supported by a interactive decoder: the SATSA Generic Connection Framework (GCF), and the SATSA-APDU package. An Application Protocol Data Unit (APDU) is the communication format between the card and the off-card applications. The format of the APDU is defined ISO specification 7816-4; a SATSA-APDU enables an MHP application to exchange APDU messages (commands or responses) with a card, according to [8]. By this way, the connection to the smart card through the GCF, and the support to exchange APDUs with the card are ensured, with the further advantage that the complex low level communication between the card and the application is made completely transparent to application developers and users. In particular, the Generic Connection Framework has been designed to supply a homogeneous interface for different types of data connections and communication protocols.

In the context of interest, by using the GCF, an Xlet may request a connection with the card through a *factory* Java class, the *javax.microedition.io.Connector*; if the connection is established, the *Connector* returns the Xlet an object able to exchange APDUs with the related data over the established connection. The *exchangeAPDU()* method is used to send a command to a card application and receive a response: a byte array containing a command APDU is passed to the method, the command is sent to the card, and when the card sends its response APDU, this method returns the response in the form of another byte array.

3. THE NATIONAL SERVICE CARD STANDARD

The migration towards personalized services, accessible through different platforms and technologies, requires access procedures that should be secure, easy to use, and as much general purpose as possible. In Italy, to accomplish and favor the convergence among different digital identification solutions, a standard called “National Services Card” has been defined. It acts as a reference paradigm, by prescribing the minimum set of functional specifications required to a smart card for compliance, without dealing with the implementation details, nor imposing a specific technology, but allowing also the use of proprietary platforms, such as JavaCard or Multos platform. The NSC device is a microprocessor smart card based on the ISO 7816 standard, and released through a specific emission circuit, according to a standardized procedure, as prescribed in a PKI infrastructure. The NSC standard defines the file system architecture of the smart card, which is shown in Figure 2, allowing the insertion of cryptographic information necessary for authentication and digital signature operations, but also leaving free space to store information useful for supplementary types of services (bank, postal services and others).

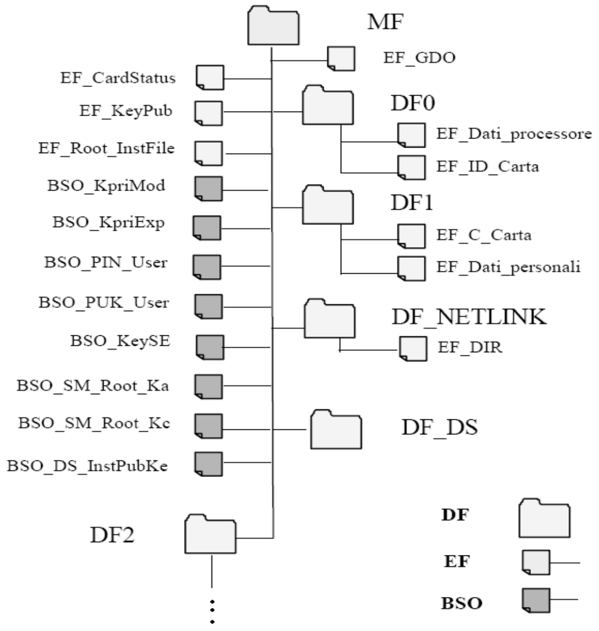

Figure 2. File system architecture according to NSC

The file system, composed by a set of Dedicated Files (DF), corresponding to directories, with the related Elementary Files (EF), is conceived in a flexible way, to allow several cryptographic operations. In particular, we can locate an area reserved to card management (including DF0, Personal Identification Number PIN, and PUK), an area to supply digital signature functions (DF Digital Signature), an area with the information necessary for authentication (Kpri, C_Card and Personal Data), and finally an area for supplementary services, under DF2. Referring to possible iTV scenarios, as outlined in the previous section, the most important basic cryptographic operations supported by the card, and available to an MHP application, are:

- *Get ATR* (Answer To Reset): this operation is necessary to reset the smart card environment, in order to open a new session with the card, for data exchange;

- *Get Data Holder*: operation that allows reading the Elementary File containing data about the smart card holder;

- *PIN Verification*: the PIN is the TEST BSO (Base Security Object) associated to binary security conditions in the card, that can be either VERIFIED (True) or UNVERIFIED (False);

- *GetCardType*: this operation performs parsing of the ATR answer to recognize the type of card inserted into the reader;

- *Get Public Certificate*: a certificate is an electronic proof which links the Signature Verification Data to a person, and confirms the identity of that person. Recovering the certificate is important because the national Italian project states that the credentials necessary to perform strong authentication are those stored in the subject section of the Public Certificate (EF-C_Card);

- *Data Signature* and *Signature Check*: operations that are equivalent to traditional handwritten signature, to subscribe digital documents.

Some of the procedures listed above are atomic, in the sense that each of them involves only one operation, or, equivalently, a single APDU command. Others are complex procedures, composed by the execution of a chain of atomic procedures. As an example of atomic procedure, we can cite the ATR (Answer To Reset) command, usually invoked to begin a new data exchange session with the card. Among the complex procedures, we can consider the digital signature functionality. A digital signature is an asymmetric cryptographic transformation of data that allows the recipient to prove the origin and integrity of the received data; digital signature protects data against forgery by third parties, and the sender against forgery by the recipient. Digital signature implementation is carried out through several transformations involving a number of APDU commands, as described in the flow-chart of Figure 3.

The data signature operation is quite complex as it results from a combination of the RSA public-key cryptosystem with the SHA1 hashing function, that provides an output of 160 bit (digest). The length of the digest does not depend on the input message length, as usual for hashing algorithms. As evident in the flow diagram of Figure 3, not all the operations are performed by the smart card cryptographic co-processor that supports only a limited number of cryptographic functions; for example Hash Computation and ID Hash encapsulation are left to the Java environment of the DTT receiver. The same happens also for *GetPublicCertificate* and *GetDataHolder* operations calling the API from the *java.security* package, and performing also other operations useful for data parsing.

4. EXPERIMENTAL TESTS AND RESULTS

Compared to traditional software and, in particular, to web or desktop applications, iTV applications have different, specific requirements that should be taken into account. Most of them are due to the features of the operating systems the digital terrestrial television receivers are equipped with. They strongly affect the way an interactive application may access specific resources within the receiver, such as a modem or a smart card reader. Besides that, interactive applications designed for the iTV context shall respect specific requirements about usability and comfort of the final user: displaying information on a TV screen requires suitable design rules to be agreed upon.

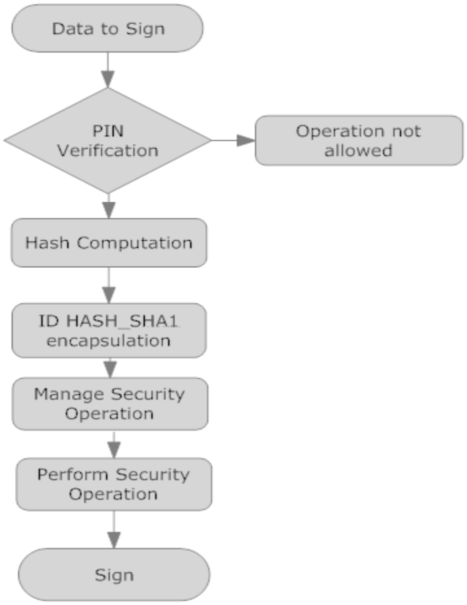
Data to Sign
PIN Verification
Operation not allowed
Hash Computation
ID HASH_SHA1 encapsulation
Manage Security Operation
Perform Security Operation
Sign

Figure 3. Flow-diagram of the signature operation

Usability of the applications can be accomplished by the definition of a set of rules about the application context and the way contents are displayed and accessed, the structure of the application, navigation strategies through the remote control, orientation, graphics, tools for advanced interaction (forms and return channel management) and, finally, some suggestions about how to write textual contents for the television [9]. The comfort felt by a user in enjoying an interactive application is mostly related to the receiver ability of providing a prompt and quick response to the user's inputs. If a receiver does not react promptly to the user's input, he will not feel comfortable and will probably switch to a different channel or content. As a consequence, interactive applications aiming at providing personalized services should be secure but also able to quickly react to the user's inputs, and to perform smart-card related operations in the shortest time. According to these considerations, we will evaluate commercial digital terrestrial receivers' performance with respect to the execution time required to perform actions related to use of a smart-card.

Experimental evaluations are performed through the execution of various routines of an iTV application written in the Java-MHP language, and adopting the SATSA API to interact with a smart card compliant to the Italian NSC standard. The routines are executed by different commercial DTT receivers, in order to verify latency or malfunctions related to the increased elaboration time required by the execution of security operations, through the interaction of the receiver with the smart card. The experimental environment available to test the way smart card based operations affect the set top box functionalities is constituted by the following elements: a smart card compliant to the Italian NSC standard, equipped with a CISC processor working at 5 MHz, three commercial digital terrestrial television receivers and a software Java-MHP application implementing the SATSA API. The first two decoders, although produced by different vendors, are based on the STi5100, mounted on different motherboards, with an amount of memory of 32 MB and with distinct firmware implementations released in different time. The third decoder is based on the STi7100, a new generation set-top box decoder chip with enhanced performances working on a motherboard with 128 MB RAM over a Linux operating system.

Table I reports the smart-card related operations that have been tested for execution by the available DTT receivers.

Table I. Execution Times

Cryptographic operation	Decoder 1	Decoder 2	Decoder 3
ATR	1 sec	0 sec	0 sec
Get Data Holder	20 sec	3 sec	1 sec
PIN Verification	3,5 sec	1 sec	0 sec
Get Public Certificate	43 sec	7 sec	3 sec
Data Signature	19 sec	3 sec	1 sec
Signature Check	44 sec	7 sec	3 sec

As shown, we tested either atomic and complex procedures, according to the description provided in Section 3. Evaluation of the execution times has been averaged over 10 experiments for each operation, and the corresponding values are reported in Table II. Results show a very different behaviour among the three decoders; these differences are not due to a single reason, but have to be addressed to the overall architecture, that comprises java middleware implementation, firmware implementation, hardware components and so on. In particular, the most recent Decoder 3, equipped with a modern chip and an high amount of memory, shows very good performances, achieving execution times near to that obtainable by a small personal computer. From a usability point of view execution times of the Decoder 1 are too long, considering that TV' users are not so tolerant. Hence, to maintain a high level general user experience of such a system, execution times have to be lower. We can assert that the execution times of the Decoder 2, with obvious reference to complex cryptographic operations that are at the base of a PKI infrastructure, represents a border line between acceptable and unacceptable performances: a TV user cannot wait more than 8-10 seconds for a procedure to complete. On the contrary, as mentioned before, Decoder 3 obtains instantaneous reaction, thus creating the foundation for an efficient system on which it is possible to build a solid PKI infrastructure involving TV platform.

5. CONCLUSION

This paper discussed the possibility of implementing personalized iTV services on the Digital Terrestrial Television platform by the integration of smart-card based security operations with the MHP environment, thanks to suitable software interfaces provided by the Java SATSA APIs. We tested usability and feasibility of such personalized services on different platforms, to show how the execution times may vary, and influence the final perception by the user. As a matter of fact, the receiver quick reaction to user inputs is essential in ensuring a comfortable approach to iTV services, and in providing the user a sense of effectiveness of the solutions proposed. By analysing the results achieved, we can conclude that although security and usability might be in contrast, efficient software and hardware implementation of decoder elements can ensure low execution times, that means more services with a high user experience.

6. REFERENCES

[1] Nie J., Hu X.2008. Mobile Banking Information Security and Protection Methods. International Conference on Computer Science and software Engineering ,2008 Volume3, 12-14 Dec 2008 Page(s): 587-590

[2] Noponen, S.; Karppinen, K. 2008. Information Security of Remote File Transfers with Mobile Devices. 32nd Annual IEEE International Computer Software and Applications, 2008. COMPSAC '08. July 28 2008-Aug. 1 2008

[3] Cooke, J.C.; Brewster, R.L. 1993. The use of smart cards in personal communication systems security. Fourth IEEE Conference on Telecommunications, 1993. 18-21 Apr 1993 Page(s): 246 – 251

[4] CNIPA Centro Nazionale per Informatica nella Pubblica Amministrazione (in Italian). DOI= http://www.progettocns.it/cittadino/usaCarta.aspx

[5] ETSI ES 201 812 V1.1.2 "Digital Video Broadcasting (DVB); Multimedia Home Platform (MHP) Specification 1.0.3", August 2006.

[6] International Standard Organization, "Smart Card Standard 7816-1: Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics", 1998.

[7] "Security and trust services API for J2ME (SATSA); JSR177" [Online]. DOI= http://java.sun.com/products/satsa.

[8] International Standard Organization, "Smart Card Standard 7816-4: Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry Commands for Interchange", 2005.

[9] Fondazione Ugo Bordoni-FUB (2005). "*Raccomandazioni per le interfacce dei servizi interattivi della televisione digitale*", Working Group GLAD1. DOI= http://www.iconmedialab.it/pdf_interattive/interfacce_interattive.pdf