Delivery of a Certified E-mail Service over the Digital Terrestrial Television Platform

Giorgio Rascioni, Susanna Spinsante, *Member, IEEE,* Ennio Gambi, *Member, IEEE,* and Carla Alfonsi

Original scientific paper

***Abstract*—At present, the electronic mail service is probably the most widespread and commonly used asynchronous way of exchanging information among people, thanks to its immediacy and easiness of use. Information delivered through E-mail can be sensitive or confidential: ensuring the sender's identity and providing privacy has become a vital step in stopping spam, fraud and even more serious crimes. To this aim, public entities have adopted Certified E-mail systems to manage secure interactions with citizens.**

Digital Terrestrial Television introduced new facilities in the traditional broadcasting environment, and determined the transition of several Electronic based-services to Television based-services. The availability of commercial Set Top Boxes equipped with network interfaces and smart card readers enables the provisioning of personalized interactive TV services, requiring user's identification and authentication, that still represent open issues in the TV context. In this paper we discuss the challenges of a Certified E-mail service over Digital Terrestrial Television, and present the case study of the Italian Regione Marche, in which this service is under development to support the remote request of certificates issued by the public administration. In particular, our attention is devoted to user authentication and secure access to the administrative services, addressed through the use of a Regional Service Card, an interactive application, and a centralized authentication framework.

***Index Terms*—Certified E-mail, DVB-T, Authentication, T-Government, Interactivity**

I. Introduction

Digital Terrestrial Television (DTT) represents the last evolution of a traditional and well known communication technology enabling the rapid and wide spreading of information, in an incisive and complete way. Taking into account the capillary diffusion of television equipments in home premises and public buildings, and the increasing number of DTT Set Top Boxes (STBs) sold or rent, DTT is in the position of becoming an effective mean for the delivery of innovative applications in the area of public administrative services, that, at the moment, are provided over the Internet.

Interactive applications for the Digital Terrestrial Television may be classified according to different criteria and requirements. Referring to the information flow defined by an application, and the service it relates to, it is possible to have unidirectional, bidirectional, and secure bidirectional applications.

Unidirectional applications represent the innovation provided by the Digital Terrestrial Television, with respect to the traditional analog service. Interactivity, standardized by the Multimedia Home Platform (MHP) [1] specifications, gives the possibility to develop new informative services, designed from scratch for the DTT platform, but also to extend the range of usability of the existing ones. As an example, E-learning services may be moved from the Web world to the DTT platform, thus originating T-learning applications [2]. The motivations for this transition are manifold: if compared to their corresponding Web versions, T-services have the further advantage of being delivered through a communication medium that, to many people, is significantly more familiar and easy to use than a PC, because of several different reasons (low education, scarce knowledge of information technologies, age). Moreover, T-services can address specific needs of "weak" social groups, like elderly or less independent people, people living in rural areas, and so on, by exploiting the capillary diffusion of TV receivers. In this sense, DTT can contribute in overcoming the so called *digital divide* [3], in many countries and regions where PCs and Internet are still not widespread, as reported in [4]. Far ahead the basic services of entertainment and dissemination of information expected from traditional television, digital TV may be exploited to help the inclusion of low-income people into the digital world, at low cost and with high penetration.

The availability of a return channel interface on DTT STBs, and the corresponding proper design of the STB middleware, make it possible to establish a bidirectional flow of information between home TV users and remote servers. Thanks to this feature, services requiring a two-way interaction, such as social services (health related services, job offers, assistance for elderly or disabled people), services related to tourism (hotel reservations, tickets booking, up-to-date traffic information), and public utilities, may be provided.

Among the services based on a two-way interaction, a more specific class comprises services requiring user authentication and/or data confidentiality, which may be provided by means of secure bidirectional interactive applications. Thanks to them, E-commerce, E-business, E-government may be extended into T-commerce, T-business, T-government [5]. T-government services, at a National or Regional level, are provided to manage the interactions between citizens and public administrations (such as request of certificates, payments). As they strongly rely on the exchange of personal user data, suitable means to protect data confidentiality and to ensure user authentication must be adopted. Since many years the use of smart cards has assumed a fundamental role, in this sense, in

Manuscript received March, 2008 and revised July, 2008. This Paper was presented as part at the International Conference on Software, telecommunications and Computer Networks (SoftCOM) 2007.

G. Rascioni, S. Spinsante, and E. Gambi are with Universitá Politecnica delle Marche, Italy (e-mail: s.spinsante@univpm.it). C. Alfonsi is with Regione Marche, P.F. Informatica, Italy.

the context of E-services. The same may happen in the delivery of certified services over the DVB-T platform. This paper focuses on the importance of exploiting the MHP capabilities in order to allow the adoption of smart cards as a mean for ensuring confidentiality and strong user authentication. As a case study, an example of application to a Certified E-mail service is discussed.

Figure 1 shows the main components of a generic DTT infrastructure through which T-government services can be delivered. In a typical Digital Video Broadcasting Terrestrial (DVB-T) system, Audio and Video (A/V) signals are generated by a content provider in MPEG-2 format. The MPEG streams are collected and organized by a network operator in a single MPEG Transport Stream (TS), through a multiplexer. The multiplexer receives also another input stream, provided by an Object Carousel generator Server (also known as MHP Playout System) [6], containing a service of MHP interactive applications (named Xlets). By such means, a TV channel is composed, and can be transmitted at the assigned radio frequency. The role of the Object Carousel Server is essential in enriching DTT with MHP contents. At the user's side, the MHP compliant STB receives the transmitted MPEG TS, decodes the MPEG A/V contents, and, thanks to its middleware, can execute the interactive applications received. In the case of T-services, Xlets are essential to handle the STB return channel interface, which, in its turn, allows the user connection to a service management operator, i.e. the available interface to a T-service provider (public administration, health institution, certified private entity, and so on). The service management operator shall perform the necessary functions to implement a bridge between the Web and the TV worlds. As discussed by Ferretti et al. in [7] and [8], the integration of DTT and Web requires the development of suitable techniques to allow the retrieval of Web contents, on the basis of TV watchers' requests, and the proper presentation of these Web contents in a format suitable for a TV screen. Finally, the service provider included in Fig. 1 represents the entity that supplies a service usually available through a different technology, such as the Web. In the context of interest, it may be identified with the public administration. The service management operator may be physically located inside the same LAN where the service provider is, or it can be located in a different network, and connected to the service provider through a Virtual Private Network (VPN). As a matter of fact, if we are concerned with user authentication and data confidentiality, these security services must be supported throughout all the path covered by the exchanged data.

Besides a network interface, DTT STBs are usually equipped with Conditional Access (CA) modules and smart card readers; moreover, the middleware of MHP receivers is able to interface ISO 7816 [9] compliant smart cards. This is a key point in the delivery of personalized T-Government services, for which user authentication is essential. In the context of the case study discussed in the following, user identification and authentication can be performed by means of National or Regional Services Cards (NSC, RSC) [10], or Electronic Identity Card (EIC) [11], issued and delivered to the citizens by local and national Italian public administrations.

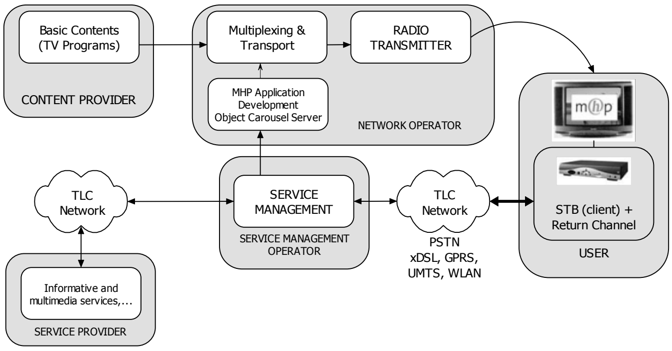


Fig. 1. A generic DVB-T technological infrastructure

Among the services requiring user identification and authentication, we are interested in Certified E-mail (CE). The object of this paper is to outline and discuss the technical issues related to the implementation and delivery of a CE service over DTT, that emerged during the design of an experimental service involving the public administration of the Italian Regione Marche, through the use of an RSC issued by it, called *Raffaello* card [12]. Examples of interactive applications developed to provide E-mail services over DVB-T already exist [13], by which usability problems have been already evidenced and solved. This work is consequently focused on the security related functions, which are to be supported by an MHP application, in order to allow the use of CE as an effective mean of interaction among citizens and public administration.

The paper is organized as follows: Section II briefly presents the main features of a CE service; Section III deals with DVB-T STBs middleware, describing the main Application Program Interfaces (APIs) provided, and focusing on return channel interfaces and smart card readers. Section IV deals with the security framework supported by the MHP Public Key Infrastructure (PKI), and focuses on the possibility to establish a secure Internet connection over Transport Layer Security (TLS) protocol. Section V discusses the issues of user authentication by means of RSC, and smart card management in MHP; in Section VI, we present a project currently under development, involving the *Raffaello* RSC, the *Raffaello Mail* Web portal, and an interactive MHP application, named *RaffaelloMail*-Xlet, for a CE service over DVB-T, through which citizens can issue requests of certificates to the local public administration. Section VII concludes the paper.

II. Certified E-mail Service

Since several years, E-mail has become a communication service of great importance, both for personal and business matters. Besides immediacy and easiness of use, it features the possibility of sending not only text messages, but also videos, images and many other file types. Text and attached files can be related to important information addressed to people, commercial organizations, institutions, and so on.

The Simple Mail Transfer Protocol (SMTP) [14], that handles most of today E-mail services, was designed in the early 1980's, when the few Internet users were (or were supposed to be) honest people interested in this new technology, who expected others to be equally honest. Unfortunately, SMTP does not provide suited means to counteract identity forgery, or to authenticate senders. Nowadays, ensuring users' identity in an E-mail scenario has become the necessary first step in stopping spam, fraud, and even more serious crimes. To answer this demand for user identification and authentication, CE systems have been developed.

CE systems allow to certify that a message, and all of its attachments, have been sent and delivered to the mail provider the recipient is subscribed to, by generating a legal proof of it (receipt). At the same time, the receiving E-mail provider is able to certify, with a precise temporal tag, that the message, and all of its attachments, have been stored in the recipient's mail account, or that this process failed. Consequently, a CE system can avoid identity forgery and message repudiation, thus being suited to interface citizens and public services provided by national and local administrations. In other words, an E-mail message sent through a CE system has the same legal value of a filed letter, and can effectively replace it.

Obviously, the whole CE process has to be regulated by law. In the Italian scenario, the main references are Law n. 59/1997 [15], stating that electronic delivery systems are legally usable, and DPR n. 445/2000 (art. 14) [16], issuing the principles for the use of electronic delivery systems, and the legal value of electronic addresses. In 2005, the matter was completely regulated by the DPR n. 68 [17], defining the characteristics of an official electronic delivery service, named Certified Electronic Mail (in Italian, Posta Elettronica Certificata, or PEC), and ensuring its legal value. More specifically, an E-mail message is considered:

- *sent*, when the recipient's provider, after several checks, accepts the E-mail and returns a receipt to the sender;
- *received*, when the message is stored in the E-mail account of the recipient. Then, the recipient's provider returns the sender a receipt of delivery.

CE providers must implement a logging scheme, to track and store all the system events for 30 months. In the case a receipt is lost, the logging system can provide a copy of it, having the same legal validity. If compared to traditional E-mail, PEC ensures recognition of the sender (that is to say, the corresponding mail account), integrity of the message sent, no delivery refusal, and matching between the delivery receipt and the message sent by the user.

The main differences between PEC and traditional E-mail are evidenced in Fig. 2. PEC can certify that the message and its attachments have been stored in the recipient's mailbox, can provide authentication of the sender, and generate receipts having legal value. The sender's PEC provider, that belongs to a public registry of certified providers, ensures authentication and integrity of the message (including its header), and of all the attachments.

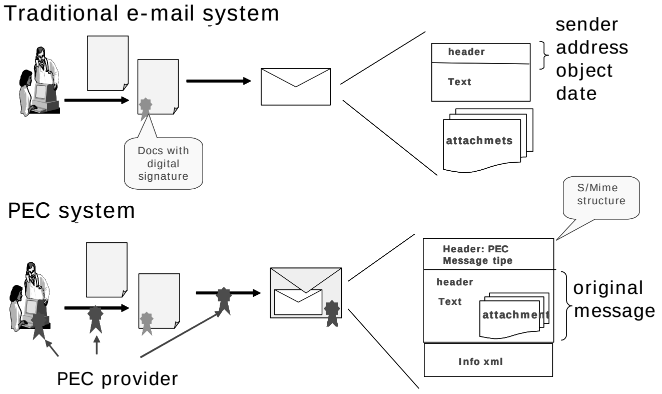


Fig. 2. Comparison between traditional E-mail and PEC systems

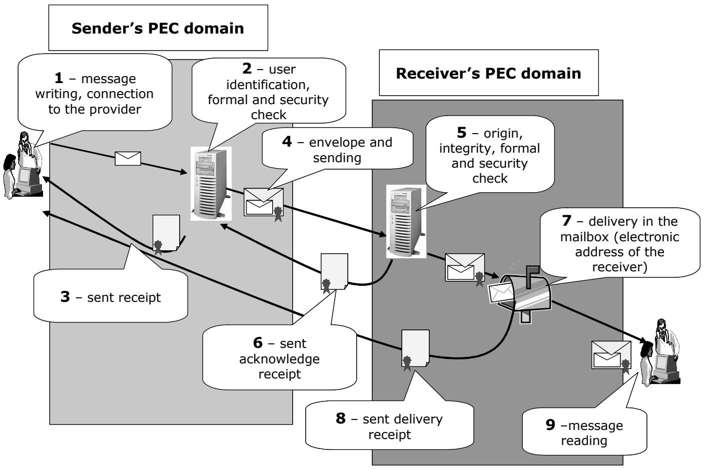

Sender's PEC domain
Receiver's PEC domain
1 – message writing, connection to the provider
2 – user identification, formal and security check
3 – sent receipt
4 – envelope and sending
5 – origin, integrity, formal and security check
6 – sent acknowledge receipt
7 – delivery in the mailbox (electronic address of the receiver)
8 – sent delivery receipt
9 –message reading

Fig. 3. Functional scheme of the interactions between sender and receiver PEC domains

Figure 3 shows the workflows related to a functional scheme of PEC implemented by means of Web technologies. When a message to send is available, the sender connects to the PEC provider by means of his credentials (stored in his smart card). If successfully authenticated, the sender can compose his message and send it, like in a traditional E-mail scenario. At this point, the sender's PEC domain has to perform a number of checks on the message, to avoid viruses or formal mistakes. If one of these checks fails, the sender is notified through a suited signed receipt. In the case of successful checks, the sender's PEC domain signs the message and forwards it to the receiver's PEC domain. Receiver's PEC domain can verify authenticity and integrity of the message by the sender's PEC domain signature. Further checks are then performed, for viruses or other security threats; again, if one of them fails, a signed receipt is forwarded to the sender. In the case of positive checks, the receiver's PEC domain stores the message in the recipient's mailbox and notifies the sender by means of a signed and verifiable receipt.

The Italian Regione Marche administration has operated a Web portal, called *Raffaello Mail* that includes, among several services, also a CE (PEC compliant) service. Through the *Raffaello Mail* portal, citizens are able to receive and to send

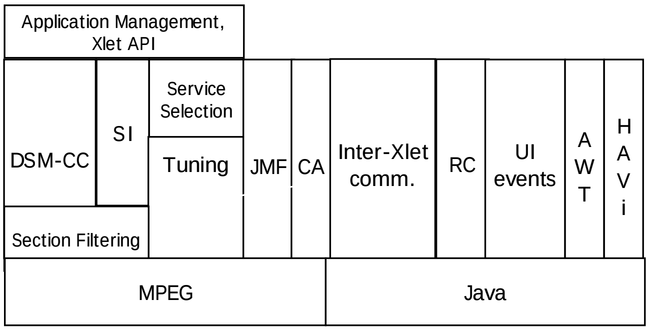


Fig. 4. Overview of the main MHP software stack components

E-mails from and towards addresses belonging to several CE providers (e.g. public agencies and administrations). Authenticated access to this portal is performed using a specific smart card, the *Raffaello* card, issued by the administration of Regione Marche. The CE over DTT service described in the following aims at extending the context of use of the *Raffaello* card to DVB-T STBs equipped with smart card readers, by implementing suited software APIs to extend the MHP support to RSCs.

III. DVB-T Set Top Box Middleware Architecture

In DVB-T STBs, the middleware can be thought of as an operating system, that has to manage the available hardware and software resources, to handle service selection and MPEG decoding functions, and to execute all the operations related to Xlets and user interaction, by means of the MHP framework. All these aspects are strictly related and interoperating. Although MHP, that has a very strong basis in Java technology, is the element which mostly characterizes STB middleware, those parts that relate to MPEG are equally important, and must be integrated into, or interfaced to, the MHP implementation.

The MHP software stack is a complex and modular architecture, whose components can be built on top of one another: standardized APIs may be used internally, to exploit the dependencies among the various components. A graphical overview of the main components in an MHP software stack is provided in Fig. 4.

The basic MHP APIs can be split into two main sets, one containing the components related to MPEG streams, the other providing services built directly on top of the standard APIs that are included in any Java platform. A detailed discussion of the MHP middleware structure can be found in [18].

The core of the MPEG-handling APIs is DAVIC's MPEG API, that collects the basic components describing MPEG services and streams. The Java APIs include graphics components (AWT, HAVi and DVB UI), a User Interface events component, an inter Xlet communication API (typically built on a proprietary API) and the Return Channel component. In STBs implementing a Public Switched Telephone Network (PSTN) return channel interface, this is considered a scarce resource and handled by means of the DAVIC resource notification API. It may not be the case when using an ADSL return channel interface. The Conditional Access (CA) component, used to access and decode scrambled elementary streams, directly interfaces the MPEG decoder, mainly because of efficiency issues, as most of the work is carried out in hardware. Another basic component, though not shown in Fig. 4, is the Resource Manager, that provides the other components a framework for sharing scarce resources; it is exposed to applications and other components through the DAVIC resource notification API.

The Interactive Broadcast and Internet Access profiles of MHP include support for using a return channel interface in the receiver, through an MHP application; basically, this is similar to accessing an IP connection in a classic Java application. The MHP 1.0.x specification requires support for HTTP 1.0 and DNS over the return channel, on top of the basic TCP and UDP protocols, but anything else is optional. MHP 1.1 adds support for HTTPS (i.e. Secure HTTP), but it does not include any other protocol, such as SMTP or FTP. In order to establish return channel connections, the MHP middleware stack calls the standard *java.net* API; however, this API assumes that a permanent network connection is available, but this may not be always the case when dealing with a STB, according with the return channel interface it may provide. To face these situations, MHP defines some extensions to the *java.net* API in the *org.dvb.net.rc* package, by means of which Xlets can set up a PSTN modem and connect to a service provider. PSTN modems, being a scarce resource, must be reserved for connection before they can be used; on the contrary, always-on interfaces are treated as IP connections that applications can access when needed.

MHP 1.1, originally published in June 2001, introduced smart card reader APIs, to support a low level communication with smart cards, and the Internet Access Profile, a set of Java APIs to support Web browsing and E-mail clients. As many T-based services, such as T-Government and T-health, may require identification and authentication of end users, MHP 1.1.2 adds further features, to access smart cards for encryption (private keys reside inside the smart card and never enter the MHP terminal) and user authentication. In MHP 1.1, the smart card reader API was based on the Open Card Framework (OCF); later, MHP 1.1.2 has replaced it with Security And Trust Services API (SATSA) [19], learning from the experience gained by the use of Java in mobile terminals. Moreover, OCF did not pass conformance tests, and presented an unclear and questionable Intellectual Property Right (IPR) policy. MHP 1.1 only provides optional support for the SATSA-APDU package, as stated in the ”11.9.4 Not-CA smart card API” section of the ETSI TS 102 812 v1.3.1 specification, that defines the later MHP 1.1.2. The SATSA-APDU Optional Package enables MHP applications to communicate with a smart card by exchanging Application Protocol Data Units (APDUs) defined in [20]. An APDU is a short message encoded as a byte sequence; SATSA-APDU enables an Xlet to exchange APDU messages with a card application.

IV. Security Capabilities in MHP

The advent of interactivity through DTT has radically changed the traditional TV broadcasting service: the final result is that the DTT architecture can be considered as a Service Oriented Architecture (SOA), according with the scenario previously outlined (see Fig. 1).

DVB MHP has defined a security model in [21] Annex 5, that MHP applications must comply with. This model ensures smooth MHP operations when supporting privacy, guarding the MHP implementation against a number of security problems, without preventing the possibility of efficiently implementing reasonable business models, such as T-commerce services. In essence, signing MHP applications provides a guarantee that the applications themselves and their data have not been modified after signing; the associated certificate carries details about the entity that signed the application. The receiver can use the authentication information to determine what privileges it has to ensure to the application during its execution, through a fine-grained control of the available resources, provided by the STB middleware.

It is necessary to remark that this kind of authentication is useful only to preserve the STB and the end user against possible hostile applications; it does not provide a technically viable mechanism for content protection in a unidirectional broadcast environment such as the DVB-T one. A T-government service, like the CE one, needs further capabilities, such as a secure bidirectional information exchange, i.e. the possibility of establishing a secure return channel connection through the Internet, towards the services exposed by remote servers of public administrations or certified private entities. In this sense, a general purpose security framework for the return channel connection can be provided by the TLS protocol [22], which requires the MHP stack to implement several cipher suites, such as Rivest-Shamir-Adleman (RSA), Message Digest 5 (MD5), Secure Hash Algorithm (SHA-1), and Data Encryption Standard (DES). A more detailed description of the required suites is given in Table I.

MHP does not mandate the whole TLS implementation: the TLS server side, the compliance with Secure Socket Layer (SSL) 3.0, and the TLS client authentication are not required. Before a TLS connection can be established, to provide secure transactions of sensitive data, MHP has to ensure that the list of certificates sent by a server contains at least one trusted certificate. Assuming that the MHP application knows which server it has to connect to, there is at least one certificate against which the application can check that a given certificate chain contains the expected certificate, that is already known and trusted.

The MHP specification describes how to install the certificates at the receiver; they should have a name in the format *dvb.tls.organization_id.application_id.x*, where *x* is an optional string to discriminate certificates, when necessary. In DVB-Java, TLS certificates are placed in the application base directory. When no TLS certificates are sent together with the application, the MHP stack implementation will allow any connection to be established, to any server. The application can use the Java Secure Socket Extension (JSSE) API to retrieve the certificate chain and check it contains what the application requires. In such a case, both the name and public keys need to be checked by the application, to trust the remote server. An unsigned application may not use the return channel interface; by default, a signed application may not access the return channel interface, unless otherwise specified by the permission request file.

It is important to stress that even if applications use TLS, data may be not encrypted during transfer. As a matter of fact, it is possible that confidential data are transmitted in clear: among the cipher suites required by MHP (see Table I), TLS_RSA_WITH_NULL_MD5 and TLS_RSA_WITH_NULL_SHA do not use encryption, and an MHP STB may have these options selected by default. Under these conditions, a TLS server could ask and obtain to set up an unencrypted session with a STB: it is a quite common case, as establishing a ciphered connection may be resource-consuming for a server. So, if data confidentiality is required during transfer, in order to prevent unencrypted sessions it is preferable to disable the two options at the decoder, as shown by the code extract reported in the following. In the case the server does not negotiate a cipher suite including encryption, the connection set up will fail, and no data will be transferred.

```
sslSocket.setEnabledCipherSuites(new String[]
{
  "TLS_RSA_EXPORT_WITH_DES40_CBC_SHA",
  "TLS_RSA_WITH_DES_CBC_SHA",
  "TLS_RSA_WITH_3DES_EDE_CBC_SHA",
  "DVB_RSA_WITH_3DES_EDE112_SHA"
 });
```

V. User Authentication in MHP

Public administrative services available through on-line platforms require access procedures that should be secure, easy to use, and as much general purpose as possible. In order to favour the convergence among digital identification solutions similar to EIC, the NSC standard has been released. The NSC standard acts as a reference when a multi-service card, like an RSC, is to be issued by a local or national administration. By means of an NSC/RSC, it is possible to provide health, bank, postal services and others, to remote users, and univocally identify each user by means of their digital signature.

The use of NSC/RSC for delivering public services over the DVB-T platform highlights the problem of integrating smart cards (the physical support for NSC/RSC) and MHP DVB-T receivers. Almost all the commercial STBs provide at least one smart card reader slot: this is “historically” due to pay-per-view programs and CA systems. CA card readers are in any way compliant with the physical and electrical standards of NSC/RSC, i.e. under a hardware standpoint. The situation is different when dealing with the software interface to NSC/RSC smart cards, which is different from that necessary to communicate with CA smart cards. The former has to comply with the ISO 7816-4 standard [20]. This standard describes the commands, the messages and the answers exchanged between the smart card and the Card Acceptance Device (CAD, commonly known as card reader), the logical structure of files and data stored in the smart card

TABLE I
CIPHER SUITES SUPPORT REQUIRED IN MHP

Cipher Suite	Key Exchange	Cipher	Hash	MHP Status
TLS_NULL_WITH_NULL_NULL	Null	Null	Null	Required
TLS_RSA_WITH_NULL_MD5	RSA	Null	MD5	Required
TLS_RSA_WITH_NULL_SHA	RSA	Null	SHA-1	Required
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	DES40_CBC	SHA-1	Required
TLS_RSA_WITH_DES_CBC_SHA	RSA	DES_CBC	SHA-1	Required
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES_EDE_CBC	SHA-1	Required

memory, and the mechanisms to protect the access to them. Moreover, the standard [20] defines the cryptographic primitives to cipher the communications between the smart card and the CAD terminal (Secure Messaging). SATSA, selected as the reference environment for smart card interfacing, is perfectly compatible with MHP, and has the advantage to make complex low level communications transparent to software developers.

The RSC issued by the Regione Marche administration is called *Raffaello* card. It can be classified among the possible strong authentication solutions, and allows the user to access some of the informative services provided by Regione Marche administration in a secure way, i.e. it assures the user's identity, and the fact that the operations associated to the user's specific privileges are executed by that user only. The *Raffaello* card is consequently an identification device for remote services, being associated to an authentication certificate, issued by a public Certification Authority, that has five years validity. By using the *Raffaello* card, and its associated Personal Identification Number (PIN), each user can access available public administration services, without the need of providing a username and a password for each service, but simply by inserting their card in a proper reader. The user's private PIN is the Security Data Object used to access the protected file, called *C_CARD* Elementary File (EF), located inside the Data Folder DF1. As shown in Fig. 5, it is an Elementary File stored in the standardized file system structure of the NCS, that contains all the data necessary to identify the user, and to provide personalized services. The authentication certificate profile is based on the IETF standards [23], [24]; the *common_name* subject of the certificate is requested by national regulations, to provide strong user authentication. This field comprises the citizen tax identification number, the smart card ID and the hash calculated over the Personal Data EF. Automatic reading of this field, and its use during the transactions, avoids typing the user data by means of the STB remote control keys. Reading that field is made possible by the SATSA-APDU, an extension of the Generic Connection Framework (GCF). Using the GCF, an Xlet requests a connection from a *factory* Java class, the *javax.microedition.io.Connector*; if the connection is established, the *Connector* hands the Xlet an object able to exchange data over the connection, as shown by the following code sample:

```
...
String urlConnection = "apdu:0;target=CXS";
try
{
connection =
 (APDUConnection)Connector.open(urlConnection);
}
...
```

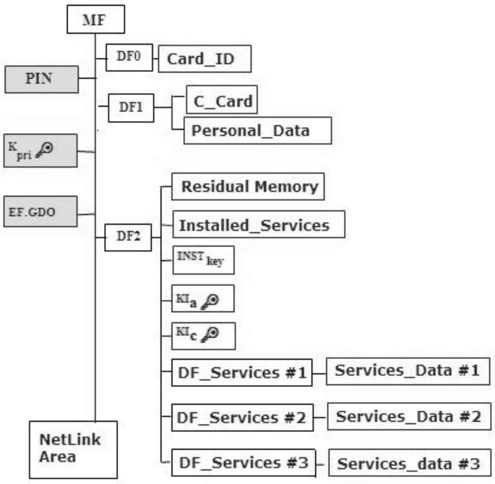


Fig. 5. Standardized file system structure of an NCS

In SATSA-APDU, the Xlet passes a *locator* string, carrying an Application ID (AID), to the Connector's *Open()* method, which returns an *APDUConnection* that can be used to communicate with the card application. The vast majority of the card issued in Italy are compliant with the standard, but are not Java cards. Although an AID could be, in theory, set also on these cards, this is not mandatory. Any *Connector.open(”apdu...;target=a0.00...”)* method issued towards such cards returns a *ConnectionNotFound* exception. This is because the card has neither an AID set, nor it is a Java Card with such a listening application. The solution consists in defining a new target, namely CXS, for the *Connector.open()* method, as *Connector.open(”apdu:0,target=”CXS”)* in the sample code. In this case (target = CXS), and only in this case, if we catch a ”*NoCardApplication*”, instead of a *ConnectionNotFound* exception, the SATSA layer can successfully return an *APDUConnection* object. At this point, the MHP application may continue to exchange APDUs (*exchangeAPDU()*) and eventually close the connection.

VI. CE OVER DVB-T: A CASE STUDY

The aim of the project described in this section, and represented by the *RaffaelloMail*-Xlet, is to migrate a CE service, currently available on a Web platform, to DVB-T, so that users can issue requests for certificates to a local

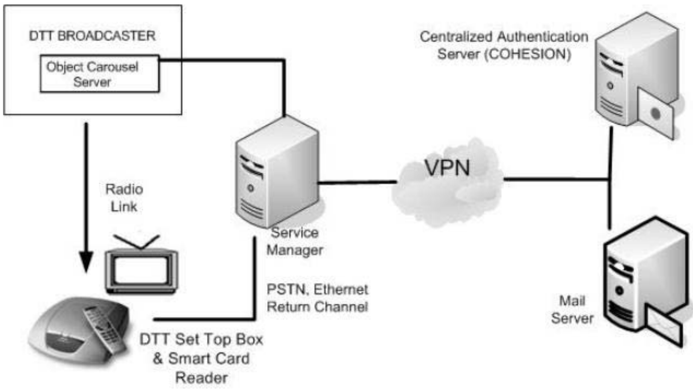

DTT BROADCASTER
Object Carousel Server
Radio Link
Service Manager
VPN
Centralized Authentication Server (COHESION)
PSTN, Ethernet Return Channel
Mail Server
DTT Set Top Box & Smart Card Reader

Fig. 6. Overview of the technological infrastructure involved in the *RaffelloMail*-Xlet project

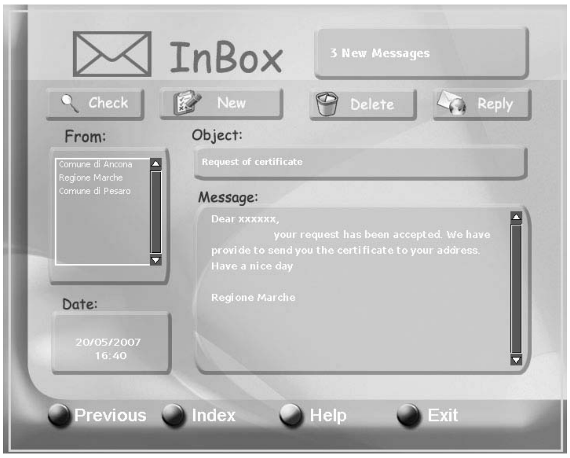
public administration, by means of their home STBs, in a Trust Access modality. Trust Access modality supplies Internal Security Services based on user's identity, with related roles and privileges, to allow a controlled access to Web based services. In practice, the identities of the communicating user and institution are ensured, respectively, by a strong authentication procedure over the DTT platform, through the *Raffaello* RSC, and by an informative and service infrastructure partly already available at the Regione Marche institution. More specifically, the final scenario can be classified as a SOA scenario, where different subjects and different technologies are integrated, as shown in Fig. 6.

In the SOA scenario, the user performs authentication using his *Raffaello* card, through the interaction with the MHP *RaffaelloMail*-Xlet graphic user interface (GUI). Once entered a page called Authentication Page, the user is requested to insert his RSC into the STB card reader, and to type the corresponding PIN, by means of a virtual keyboard shown by the application on the screen. The Xlet can verify if the typed PIN is correct or not, by questioning the *Raffaello* card. In the positive case, the Xlet will start a handshake procedure to establish a TLS communication session over a PSTN or Ethernet interface, with an external Web server called Service Manager, that acts as a Content Management Service (CMS), to handle the interaction of the STB with the Internet world. The handshake process is transparent to the user, and completely managed by the Xlet through proper Java instructions.

Once the secure connection is established, the Xlet transfers the user's identity data, read from the *Raffaello* RSC, to the Service Manager. The Service Manager establishes a VPN connection to the Authentication Server Cohesion [25], by invoking a particular synchronous WebService. Cohesion represents the core element to access all the available authenticated services offered by the Regione Marche administration, and supported by means of the *Raffaello* RSC. Cohesion checks the user's rights of accessing the *Raffaello Mail* Service, by addressing a query to the User Profiles Database of the RSC project, and gives back the corresponding Simple Object Access Protocol (SOAP) answer. The Service Manager processes the SOAP answer, formats it in a suited XML syntax for the *RaffaelloMail*-Xlet, and transmits it back to the STB, again over the secure TLS connection set up during the initial phase. These formatting operations are necessary to ensure a correct exchange of data between the Service Manager and the user side, represented by the STB and the MHP application. As discussed in [7], Web contents need proper transcoding in order to be accessible on the DTT platform.

The *RaffaelloMail*-Xlet parses the received XML file. In the case the SOAP answer was positive, the user is authorized to send an E-mail for requesting his certificates to the public administration. In order to simplify the process of writing texts by means of a remote control, the Xlet provides the user with a wizard procedure, to guide him in filling in all the empty and editable fields in the GUI. Given the specific context of application, there are some limitations on the number of fields that may be edited by the user, and on the textual information the user can type, with respect to a traditional E-mail written through a Web interface. The user cannot select the recipient of the certified E-mail message arbitrarily: he is allowed to make a selection in a preconfigured scrolling list, which corresponds to the public list of the trusted certified institutions, recognized and regularly updated by the Regione Marche administration. Depending on the selection performed, the user can choose the type of certificate he needs in a limited set of options, then enter the Editor Page. In this MHP page, thanks to editing functionalities developed ad hoc, the user can write, rather quickly, the text of the E-mail by pressing the remote control keys.

Finally, once the SEND button on the GUI is pressed, the *RaffaelloMail*-Xlet starts another set of workflows to transfer the edited contents to the Service Manager, that, in its turn, contacts the Certified Mail Server. If no problems arise, the Mail Server, complying with the rules of a CE System, transfers the E-mail to the right recipient. Also in this case all the data exchanged pass through a secure connection. In the case the whole authentication procedure fails, or the STB is not able to connect to the Cohesion server through the Service Manager, a message will be shown to the home user, and the Xlet will pause in the Authentication Page. A similar procedure is performed when the user wants to check his InBox through the *RaffaelloMail*-Xlet. A screenshot of the interactive application GUI, through which the user can check incoming mails, is shown in Fig. 7. As in a traditional E-mail service, attachments could be sent to the user, together with the mail body. Limitations on the nature of the attached files are obviously due to the specific platform on which the service is provided. As a consequence, when dealing with CE over DVB-T, the only attachments which may be properly displayed by the final user are text and image files, the latter according to the formats admitted by MHP (i.e. JPG, PNG, BMP). Restrictions on the greatest admitted dimension for the received mails and attachments exist, usually stronger than those imposed by E-mail servers on the Web. They are basically due to the technological limitations of the STBs available on the market, which are expected to improve in the future. As a



3 New Messages

From:

Comune di Ancona
Regione Marche
Comune di Pesaro

Object: Request of certificate

Message:

Dear xxxxxx,
your request has been accepted. We have provide to send you the certificate to your address.
Have a nice day

Regione Marche

Date: 20/05/2007 16:40

Fig. 7. A screenshot of the *RaffaelloMail*-Xlet GUI: the InBox page

final remark, latencies in the order of some seconds may be experienced by the user, when the MHP application performs the authentication process. They are associated to the instructions executed in order to query the RSC for user's private data. Even though a latency of some seconds may appear quite annoying, it is important to remember that such operations are executed only once, during the secure connection setup phase; moreover, latencies of similar amount have been obtained by testing the application on different STBs, thus indicating they are associated to processing limitations of the CA modules currently available.

VII. Conclusion

This paper discussed the main issues to face when migrating a Web based certified service, such as Certified E-mail, to the DVB-T platform, in order to exploit the interactive capabilities it offers, through the smart card support provided by MHP. The final aim is to allow the TV user to issue requests for certificates towards institutions of the public administration directly from his home premise, through the DTT STB; any communication session takes place in a secure way, thanks to suited identification, authentication and ciphering mechanisms. The security framework necessary to ensure a certified service is established by means of suitable APIs, through which DTT STBs can interface Regional and National Services Cards, to provide user identification and authentication. A case study involving the centralized authentication framework of the Italian Regione Marche administration, the RSC issued by it, and an interactive MHP Xlet developed ad hoc, has been presented.

References

[1] MHP Specification 1.0.2, TS101 812 V1.2.1, available at: http://www.mhp.org/.

[2] Baldi M., Spinsante S., Falcone D., and Gambi E., "A T-Learning platform based on Digital Terrestrial Television," Proc. of SoftCOM 2006, 14th International Conference on Software, Telecommunications & Computer Networks, Sept. 29 - Oct. 1 2006, Split - Dubrovnik, Croatia.

[3] Demunter C., "The digital divide in Europe," EUROSTAT European Communities 2005, Catalogue Number KS-NP-05-038-EN-N (available at: http://epp.eurostat.cec.eu.int/cache/ITY_OFFPUB/KS-NP-05-038/EN/KS-NP-05-038-EX.PDF, retrieved on Apr. 2007).

[4] Elias M., Campista M., Moraes I.M., Esposito P.M., Amodei A. Jr., de O. Cunha G., Costa L.H.M.K., and Duarte O.C.M.B., "The Ad Hoc Return Channel: A Low-Cost Solution for Brazilian Interactive Digital TV," IEEE Communications Magazine, Jan. 2007, pp. 136 - 143.

[5] Ma M., Wilkes-Gibbs D., Kaplan A., "IDTV Broadcast Applications for a Handheld Device," IEEE Communications Society 2004, pp. 85-89.

[6] Open Source Object Carousel implementation available at: http://www.cineca.it.

[7] Ferretti S., Roccetti M., Palazzi C.E., "Web Content Search and Adaptation for IDTV: One Step Forward in the Mediamorphosis process Toward Personal-TV," Hindawi Advances in Multimedia, Vol. 2007, pp. 1 - 13.

[8] Ferretti S., Roccetti M., "MHP meets the Web: bringing web contents to digital TV for interactive entertainment," Proc. of the 8th IEEE Int. Symp. on Multimedia, pp. 169 - 176, San Diego, Calif., USA, December 2006.

[9] ISO/IEC 7816 - Parts 1/2/3, "Asynchronous smartcard information," (available at: http://www.ttfn.net/techno/smartcards/iso7816_12.html).

[10] Report: "Progetto CNS" (in Italian, available at: http://www.progettocns.it/cittadino/usaCarta.aspx, retrieved on May 2007).

[11] Gentili M., "Italian Electronic Identity Card: principle and architecture," Proc. of the 27th VLDB Conference, Rome, Italy, 2001.

[12] http://www.cartaraffaello.it/web/ (in Italian).

[13] Herrero C., Cesar P., Vuorimaa P., "Delivering MHP applications into a real DVB-T network: Otadigi," Proc. of the 6th Int. Conference on telecommunications in Modern Satellite, Cable and Broadcasting Service, vol. 1, pp. 231 - 234, Nis, Serbia - Montenegro, Yugoslavia, October 2003.

[14] Postel J., "Simple Mail Transfer Protocol," IETF RFC 821, Aug. 1982.

[15] Legge 15 Marzo 1997, n. 59, "Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa," G.U. n. 63, March 1997 (in Italian).

[16] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa," G.U. n. 42, Feb. 2001 (in Italian).

[17] Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, "Disposizioni per l'utilizzo della posta elettronica certificata," G.U. n. 97, Apr. 2005 (in Italian).

[18] Morris S., Smith-Chaigneau A., "Interactive TV Standards: a guide to MHP, OCAP and JavaTV," Focal Press, 2005.

[19] Security And Trust Services API for J2ME - SATSA 1.0, Java Specification Request JSR 177, July 2004 (available at: http://java.sun.com/products/satsa).

[20] ISO/IEC 7816 Part 4 Smart Card Standard, "Interindustry commands for interchange" (available at: http://www.cardwerk.com/smartcards/ISO7816-4.aspx).

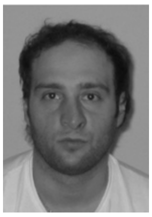
[21] Digital Video Broadcasting (DVB) Document A062, "DVB Commercial Module - Multimedia Home Platform User and Market Requirements: Enhanced and interactive digital broadcasting in the local cluster," Apr. 2001, (available at www.mhp.org/documents/).

[22] Dierks T., Allen C., "The TLS Protocol," IETF RFC 2246, Jan. 1999.

[23] Santesson S., Polk W., Barzin P., Nystrom M., "Internet X.509 Public Key Infrastructure Qualified Certificates Profile," IETF RFC 3039, Jan. 2001.

[24] Housley R., Polk W., Ford W., Solo D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF RFC 3280, Apr. 2002.

[25] Corradini, F., Paganelli, E., Polzonetti, A., Forestieri, L., Settimi, D., "Smart Card Distribution for E-Government Digital Identity Promotion: Problems and Solutions," Proc. of ITI 2006, 28th Int. Conf. Information Technology Interfaces, June 19-22 2006, Cavtat, Croatia.



Giorgio Rascioni received his Laurea degree in Electronic Engineering in 2005, from the Università Politecnica delle Marche, Italy. Since November 2006 he is a Ph. D. student at the same university. His main research activities deal with the development of MHP applications, interactive services over DVB-T/H, and error concealment algorithms for video coding.

Susanna Spinsante received her Laurea degree (summa cum laude) in Electronic Engineering in 2002 from the Università di Ancona, Italy, and a Ph.D. in Electronic Engineering and Telecommunications in 2005, at the Università Politecnica delle Marche. Currently, she is a temporary researcher at the same university; her main research interests are related to security and encryption aspects in communications, MHP applications over DVB-T, coding and audio/video applications.

Ennio Gambi is with the Department of Biomedical Engineering, Electronics, and Telecommunications of the Università Politecnica delle Marche of Ancona, Italy, where he is currently the lecturer for the course of Telecommunication Systems. He is presently working on spread spectrum systems, encryption and authentication algorithms, with particular interest in coding systems and transmission of multimedia signals over wired/wireless LAN.

Carla Alfonsi is with the Regione Marche Public Administration, where she is the coordinator of the *Digimarche.dt* project about the implementation of T-gov services on the DTT platform. She is also full time responsible for the front-office IT systems of the same administration, and temporary lecturer for the courses on data warehouse and data mining at Università di Urbino (Italy).