E-SERVICES IN MISSION-CRITICAL ORGANIZATIONS: IDENTIFICATION ENFORCEMENT

Carlos Costa, José Luís Oliveira, Augusto Silva
Universidade de Aveiro, DET/IEETA, 3810-193 Aveiro, Portugal

Keywords: E-Services Security, E-Commerce, Digital Credentials, Authentication and Identification.

Abstract: The increasing dependency of enterprise on IT has rise up major concerns on security technology and procedures. Access control mechanisms, which are the core of most security policies, are mostly based on PIN and, some times, in Public Key Cryptography (PKC). Despite these techniques can be already broadly disseminated, the storage and retrieval of security secrets is yet a sensitive and open issue for organization and users. One possible solution can be provided by the utilization of smart cards to store digital certificates and private keys. However, there are special organizations where even this solution does not solve the security problems. When users deal with sensible data and it is mandatory to prevent the delegation of access privileges to third persons new solutions must be provided. In this case the access to the secrets can be enforced by a three-factor scheme: the possession of the token, the knowledge of a PIN code and the fingerprint validation. This paper presents a Professional Information Card system that dynamically combines biometrics with PKC technology to assure a stronger authentication that can be used indistinctly in Internet and Intranet scenarios. The system was designed to fulfill current mission-critical enterprises access control requirements, and was deployed, as a proof of concept, in a Healthcare Information System of a major Portuguese Hospital.

1 INTRODUCTION

Enterprises and organization are increasingly using network-supported services for personal and professional tasks, migrating many of traditional personal interaction to the cyberspace domain. In the past, almost business and social processes were based on paper and physical procedures. Nowadays, these relations are making use of global IT infrastructures, the Internet.

The new environment offers much more quickness, optimization and efficiency of work processes, with huge cost savings. However, it is important to organizations the understanding of new security threads and the design and implementation of secure infrastructures and E-Services. In other hand, in order to be friendly usable, the user comfort and convenience are important factor of success of security technologies.

The consequences of an insecure and inefficient solution can compromise the whole information system with directly and eventually disastrous impact on the respective enterprises. Examples can be the loss of privacy, the exposure to denial of service attacks, the compromise of the data integrity and the invalidation no-repudiation mechanisms. A crescent number of organizations start now to provide their employees and external partners with secure tokens to build several fundamental security services – like authentication. However, none of these security services is effectively achievable if the token owner authentication and identification are not enforced. This last aspect is the major concern for organizations that are dealing with critical information systems.

A variety of security technologies are already available like passwords, physical tokens, biometrics, crypto smart cards and PKC digital signatures. Some of these mechanisms can be used together in order to achieve a higher degree of robustness.

In here we present a model that integrates smart cards, digital credential, biometric fingerprint and user password (PIN), according to the organization access policy. The main goal was the achievement of a flexible and robust security access system to verify and ensure that the users are in fact who they claim. In the developed model, biometrics recognition and password acquisition have been integrated into a Professional Identification Card (PIC) to achieve strong identification and authentication of users.

Costa C., Luís Oliveira J. and Silva A. (2004).
E-SERVICES IN MISSION-CRITICAL ORGANIZATIONS: IDENTIFICATION ENFORCEMENT.
In *Proceedings of the Sixth International Conference on Enterprise Information Systems*, pages 389-396
DOI: 10.5220/0002649103890396

2 PIC IN MISSION-CRITICAL ORGANIZATIONS

As previously mentioned, PIC appears as a core element concerning the migration of entities relations, rights and obligations from the physical world to the cyberspace. Nowadays, the organizations implementation of secure PIC solutions is mainly encouraged by the follow advantages:

- Improvement of business processes (DSI, N/A) (Booz, 2000);
- Provisioning of enhanced security to network and systems (Jones, N/A) (Datakey, N/A);
- Scalability and multi-application flexibility. Support for new applications, dynamically loaded after cards are issued. If the card driver is rich enough, updates and modifications to existent information or functions do not impose card re-issuance;
- Yield costs saving on processes, improves readiness and increases quality and quickness (Booz, 2000);
- Improves user confidence on security mechanisms.

Currently it is possible to identify some core services that can be provided to institutions employees, and implemented upon a professional identification card:

- *Physical Access Control* – Used to restrict and control the access to the physical institution structures;
- *Authentication Token* – The card works as a token that grants access to applications or systems. The authentication is based on some information “securely” stored on the card. The strong authentication is typically based on Public Key Cryptography and Digital Credentials.
- *No-repudiation token* – The card supports digital credentials (certificate + private key) oriented to support digital signatures of documents and actions;
- *Encrypt Token* – The card supports digital credentials (certificate + private key) oriented to support decryption of documents destined to the user;
- *ID Token* – oriented to provide the card owner identification services, including academic and professional licenses. Commonly, this service appears embedded in all cards.

Many of actual PIC implementation combines, in a unique token, several of the above services or functionalities. Namely, it has become usual to find scenarios with demanding security requirements that impose the implementation of most of these services. In areas like healthcare, education, military, justice and the E-Government in general, it is possible to identify some excellent examples of these PIC implementations, from this point forward denominated as “Mission-Critical PIC”.

2.1 Mission-Critical Implementations

Nowadays, there are very powerful tolls concerning the actual migration of traditional society relations to the electronic and virtual world. If, it is not very

Table 1: PIC Mission-Critical Implementations

Examples	**Issued Cards**	**Targets**	**Card-Owner Authentication**	**Services**
USA Department of Defence military cards, (Common Access Card) (DSI, N/A).	13 millions	Active Duty Military, Selected Reserve Personnel, DoD civilian employers, approved contactors	PIN and Biometry	Physical Access to building areas, PKC network Identification and Authentication (I&A), personal identification and electronic commerce functions.
Rabobank Group, the largest Dutch retail bank (Datakey, N/A)	33,000	Internal users and secure online transactions	PIN	Strong Authentication in accessing to centralized application, digital signatures in highest security level transactions and physical access.
Shell Group (petrol) (Jones, N/A)	85,000	internal employees	PIN	Physical Access, network login, no-repudiation of digital transactions, digital signature and encryption Email and documents.
Dutch Judicial Smart Card, implemented under ROBIN project (Norbert, 2003)	12,500	judicial authorized personnel	Fingerprint	Strong Authentication (workstation login and secure access to server, using a Single Sign On system), no-repudiation of digital transactions, digital signature of Email and encryption of networked documents.
Deutsche Healthcare Professional Card (HCP, 1999)	N/A	Physicians	PIN	Strong Authentication, no-repudiation (digital signature) and decryption of documents.

common find examples using theses mechanisms in a regular cybernetic user domain, in the last three years it has possible to identify several mission-critical organizations scenarios where they are in use. A common technical characteristic to these examples is the use of PKI, Digital Certificates and crypto Smart Cards as the key core elements.

In Table 1 some illustrative examples are listed, in distinct society areas, where mission-critical PIC are fundamental technologies. However, some other critical scenario could be identified like, for instance, the education sector (Lutz, 2002) or National Critical Infrastructures (Booz, 2000).

2.2 PIC Services

Considering the card identification service it is possible to isolate two functional approaches. First, the surface card user elements – name, photo, number, issue date, validation, etc. – are typically used to physical conventional ID purposes. Second, the internal card elements are used to provide identification to applications or systems, based on ID elements securely stored inside the card.

Considering the security services that were identified previously in this session, physical access control and the basic authentication token security services are based on primitive and weak structure and will be excluded from our analyses. In almost all of these services implementations, the PIC works as a basic access token element. Looking more in detail to the remaining security services, the strong authentication, no-repudiation and encryption/decryption, it is possible to identify two structural key points: the usage of public key cryptography and digital signatures to implement these services. Typically, the implementation of these services are based on three distinct digital credentials securely stored inside de PIC, which means that, at least, six different storage containers are required (3 to digital certificates and 3 to private keys).

From Figure 1, it is possible to identify several relationship processes inherent to Mission-Critical PICs, with the card as core element. The PIC can interact with application systems to provide security services or with other cards in the context of services like mutual authentication. For instance, in the healthcare sector, many operations demand the mutual authentication between patient cards and professional cards (HCP, 1999). On the other hand, the PIC must establish a relation with the professional, enforcing that cardholder and card-owner are the same.

2.3 PIC Technologies

Most of the current electronic applications are supported by well-known security protocols, like SSL or S/MIME, that rely on strong cryptography, particularly the Public Key Cryptography (PKC). These cryptographic algorithms can be implemented either in software or in hardware devices and their management is supported by a Public-Key Infrastructures (PKI) (Johner, 2000).

The core solution of PKC consists of a pair of complementary (asymmetric) cryptographic keys: the public key and the private key (Menezes, 1996). The PKC usability is based on two key points. First, it is essential that private keys of individuals are stored and maintained secret by the user, which involves securing the private key(s) using protected containers and passwords. However, the best way to do that is by storing it in the protected chip of a smart card. Second, the register and distribution of public keys must be maintained and administered by a trusted third party. The use of Digital Certificates issued by certification authorities is, actually, the best vehicle to do that.

Actually, the huge majority of recent Mission-Critical PIC solutions are making use of PKC services and credentials, stored inside crypto smart cards. Storing digital credentials (digital certificate and private key) on a secure token like a crypto smart card solves the storage problem offering yet a superior transport mechanism with secure protection (Marvie, 2000). Cards with embedded public key capabilities do not give access to the sensible PKC private key at all. The success of the *Card Holder Verification* (CHV) process uniquely grants the access to internal cryptographic functions that handle internally the private key.

The nowadays-electronic world economy tells us that PKC is the most accepted and used mechanism in electronic transactions to implement security and access control services. However, even this system can be insufficient in specific applications. In information systems that are dealing with very sensible information it must be guarantied that the legitimate card owner (PKC-private key) is himself on the communication end-point. This central issue is the avoidance of illegitimate use or delegation of access permission to third persons. For instance, in health care environments, where legal issues such as the patient data privacy have to be respected, the "share" of PIN between professional individuals cannot be tolerated.

2.4 PIC Owner Authentication

Security assurance in most of the current commercial transactions is typically provider-oriented, i.e. the service provider just imposes its security policy to the user that has to assure that its own secrets are preserved. Although for most of the scenarios this solution is acceptable, since the disruption of secrets only affects the owner-provider relation, there are situations where the loss of privacy involves third persons, like the patients in the healthcare scenario.

One of the most important issues related with this mixed technology (PKC + smart cards) is the implementation of an effective verification process of the cardholder, which works as second authentication factor (Figure 1). In most of the application scenarios the PIN presentation is satisfactory enough to provide that guarantee. However, the implementation of biometric techniques to control the access to the reserved card data or capabilities is, in focused scenarios, an essential authentication element to prevent the delegation of card to third parties (and enforce a strong identification).

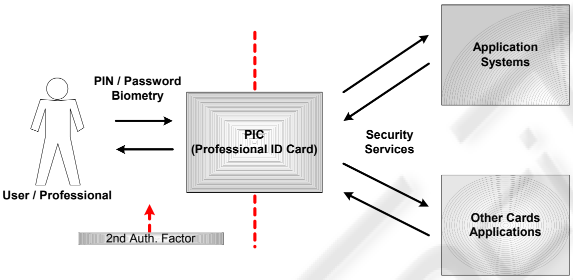

Figure 1: PIC Services

On other hand, to the same service, the second authentication mechanism can change according with access environment. For instance, the PIN mechanism can be enough inside the institution access. However, in an external access it may be a weak solution because the physical employee identification factor disappeared.

In fact, in Mission-Critical PIC implementations, the second authentication factor appears as the most important aspect and a fundamental requirement to the implementation of PIC services. This means that, if the system cannot guarantee that PIC legitimate owner exclusively uses them, none of implemented secure services (strong authentication, no-repudiation and decrypt messages) makes sense. In fact, this second factor must both authenticate and enforce the identification of PIC holder.

Nowadays many of implanted access control systems are still based on the "*what he knows*" mechanisms, which provide a cheap security solution that is good enough for several network and application needs. However, this authentication policy is inadequate for the nowadays high-demanding security environments. The PIN elements are very predictable, usually changed with very low frequency and they can be illicitly acquired by direct covert observation. In this way, there is no effective protection against repudiation by the user ID owner. In other hand, there are scenarios where the access authorization cannot be delegates to other persons.

2.4.1 Biometry

Comparatively to the previous "*what he knows*" access mechanism, biometrics devices appear as a much more accurate and reliable user authentication method. The user is recognized based on "*what he is"*. The biometrics is actually playing an important role in systems security allowing the identification of a person based on his or her physiological or behavioral characteristics (Riha, 2000). The user's physical characteristic is acquired and converted to a bit stream, usually denominated as a *template*.

The biometric authentication procedure can be divided into three parts: 1) In the *enrollment* the user templates is extracted from individual in question; 2) The extracted master template is *stored securely* for future reference; 3) During *verification* time the master templates is compared with a live template captured from candidate individual to identification.

The biometrics key point is that it work well only if the verifier can ensure two things. First, that live biometric template came from the person at the time of verification**.** Second, that this biometric template matches with the master biometric, previously and securely stored. Some benefits of biometrics over password are that the biometric cannot generally be lost, forgotten, or written down and it is much more attractive either to developers and users. Unfortunately the reality is not so easy (Ratha, 2001). In order to be useful, biometrics must be stored and accessible on some secure place, and here begins the first problem. The type of identity recognition model determinates the storage option. If the template matching process is made on the server side, they are typically stored in a central database. However, if the matching is made on client side the templates are typically stored in a secure hardware token, like a smart card.

We see little advantage for the user in adopting systems that require a biometric to be passed over a network like any other shared secret. Moreover, actually the ideal use of biometrics is in the replacement of a PIN or password in situations where the connection from the reader to the verifier is secure (Grant, 2001) like, for instance, when a biometric unlocks a private key on a smart card (Castle, 2001). A clear advantage of this last application scenario is that the owner retains always the control of his biometric template. Furthermore, the storage and matching of the master template can be made inside this tamperproof device, providing a more secure application environment – the master biometric template never leaves the protected user token.

3 A PIC HOLDER AUTHENTICATION MODEL

As we have already highlighted, particularly in mission-critical PIC systems, that is crucial to have mechanisms for differentiating between the authorised card user and someone else that has obtained this identification and is making illegitimate use of it – this can be achieved, most of the times, with the right owner permission or delegation. In other hand, it is equally important to give emphasis to separate authorization trust level according with organization security policies. In this last case, one the most important elements is, for example, the user access provenience or platform.

Many times, common sense puts the access provenience problematic in the indoor versus outdoor scenario. However, it is possible to have, different trust level inside the institution walls. In any case, must be always a central application system to analyse and define the trust level according with pre-defined security policies, i.e. the type of second authentication factor demanded to the end user.

In a trusted or controlled access zone, it is easy to detect this PIC illegitimate use, however the same could not be guaranteed, for instance, in a remote access. What we want to obtain is the implementation of a recognition model to strongly enforce identity of authorised user from distrusted access scenarios like a physically uncontrolled installation and, at the same time, continuing to allow the usage of single PIN/card pair in trusted access areas (although the strongest control can be practicable anywhere if desirable).

In summary, the proposed model imposes different levels of user identification proof, depending on security policies like the access origin, trusted versus uncontrolled. It must guarantee that the authorised person is at the remote access, not being limited to prove that he provided a correct authentication credentials. This is where the biometrics can offer an effective contribution to the problem (Hachez, 2001) (Alliance, 2002), by replacing the pair smart card/PIN by the authentication set smart card-biometry-PIN ("*what you have*"-"*what you are*"-"*what you know*").

3.1 Model Architecture

The first important aspect to emphasize is related with the fact that is always the application server that analyses and defines the trust level in every access, i.e. the server forces, or not, the biometric factor. When a user tries to access to the central application, the server generates an access pre-ticket that is sent to the client on-card application (the javacard applet). This ticket includes an internal timestamp element to prevent the capture and reply attacks, a trust flag that defines the necessity of biometric matching mechanism and the challenge-response message to authentication purposes (Figure 2).

The smart card PIN that protects the PKC private key sets, results from the processing of input parameters owned by distinct intervenient elements (user and server) and from a securely protected on-card application stored at issue time. In other hand, making use of an on-card Bio-API (like the Precise BioMatch (Ola, 2003)), the user master template(s) on the smart card is kept protected and totally inaccessible. It is not possible to retrieve, in any circumstances, a previously stored user template. In operation mode, the card hosted client application just has available a BioAPI "verify" function, that accepts as input arguments the live template and the Id of master template to make the matching. If the match fails more that N consecutive times, the respective master template container is locked.

The NIST/Biometric Consortium presented recently a Java Card Biometric API (NIST, 2002). It is a high level and biometric neutral on-card API that supports, among other characteristics, secure template Match-on-Card with resource to Java Card smart cards. As referred, in this way the sensitive user master template never leaves the secure tamperproof token, with evident risk of capture and misuse. Considering this, we are currently exploring these new functionalities, in the second development phase, including the migration of file-oriented crypto smart cards to java cards technology and the development of applications in Java language (Microsystems, 2001), named cardlets, that are stored and executed inside smart card environment. This way, the presented model is very simplified, reducing the risk attack to the physical layer.

Returning to the model architecture (Figure 2), the second core element is the bypass to the matching process dependent on the kind of the trust policy included in the issued server pre-ticket. As referred, the evaluation of this situation is made by the server side, which will check the IP address and platform of client workstation in the trusted access list. If the client, for instance, is not in the private departmental network, the server sends the encrypted information (timestamp + yes-flag + challenge) demanding the biometric match. Otherwise, the matching is suppressed with the follow message (timestamp + no-flag + challenge). This information is encrypted with the server private key and the java card routine makes use of server public key to decrypt the message and determine the matching procedure to execute.

The other achieved goal of the proposed model is related with the risk of forging user identification. Now it is restricted to the conjugation of three factors: the token possession, the user password knowledge and the physical capture and forging of biometric element.

3.1.1 E-Service Model Workflow

In Figure 2 it is presented a flowchart with the model architecture workflow to the authentication service. However, this flowchart could equally represent the two other PIC security services presented before (no-repudiation and decryption facilities) replacing the challenger with a doc-data or a session key.

When the user needs to use any of the services (*ServerApp*) which security credentials are stored inside the PIC (*ClientApp*) the following steps will be taken:

1 The user holds a PIC smart card containing the cryptographic keys and their biometric template data.

2 The *ServerApp* send a ticket to the *ClientApp*.

3 The user inserts their PIC into a reader and provides his password.

4 If it is not a trusted access (depends on *ServerApp* policy), then the *ClientApp* must:

4.1 Read the user fingerprint;

4.2 Compare this live template with the card owner template;

4.3 If it does not match, the access is denied;

5 The user's password is used to generate the smart card PIN to grant access permission to private key functions.

6 The unlocked private key on the smart card is used to sign or decrypt the message data. The output message is encrypted with server public key and then sent back to the *ServerApp*.

7 The *ServerApp* decrypts the received message using the user public key and process data according to the specific application proposal (signed challenger to authentication, signed document to no-repudiation, or decrypted session key to decipher private documents).

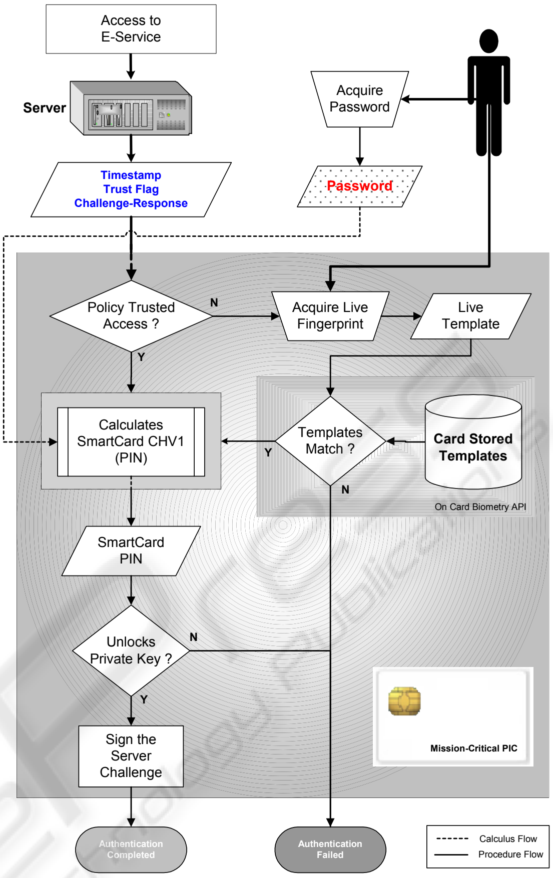

Figure 2: Model Architecture Workflow to an Authentication Security Service

3.2 Deployment Scenario

The proposed control access system have been implemented and deployed in an information system with sensitive data, the CHVNG Cardiology Department Healthcare Information System (HIS) that integrates 45.000 electronic patients' records (EPR) and a Picture Archiving and Communication Systems (PACS). For this particular environment, we have developed a healthcare PIC, denominated Healthcare Professional Card (HPC).

The HPC was implemented over a Web-based HIS that uses *XML/XSL* technology for dynamic content creation and formatting (Bexiga, 2003), according to the user terminal and to his access privileges (Figure 3). This HPC provides access control to the institution's spaces, and indoor and

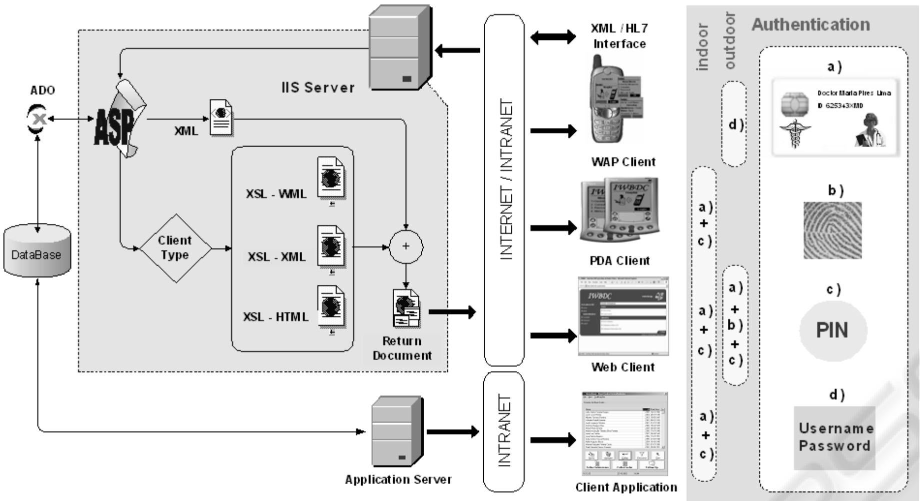

Figure 3: A PIC Deployment Scenario in a Healthcare Information System

outdoor access control (Web) to the HIS and to the PACS (Costa, 2003a) (Costa, 2003b).

In the Web-based access platform we realize that, inside the institution the professional is authenticated through an HPC-PIN pair (‘*a*+*c*’ in Figure 3), but to obtain a similar access level from a remote access our system can impose the use of the HPC-PIN and fingerprint validation (‘*a*+*b*+*c*’). Our main goal is to assure that clinical persons, such as physicians, do not delegate access control on other persons.

The implementation of this smart card system was ruled by the major standards and industry initiatives. The physical level and lower layer protocols of smart cards are defined by the formal standard ISO 7816 (ISO-7816, 1997) in a way that can accommodate components manufactured by different suppliers. The application level was based upon the Schlumberger Cyberflex Access SDK 4.3 (SchSDK, 2002) and PC/SC (PC/SC, 1997). The product was built over a GemPC-Touch reader (fingerprint + card) using Schlumberger Cryptoflex-16k and Cyberflex-32k smart card. The healthcare professional digital certificates and respective private key are stored following a full compliance with PKCS #11 (PKCS11, 2001) for compliance with Netscape products.

4 CONCLUSION

Current enterprise’s dependency on IT is putting major requirements on security solutions namely on access control mechanisms. These are several approaches mostly based on PIN and in Public Key Cryptography (PKC). Despite these techniques can be already broadly disseminated, the storage and retrieval of security secrets is yet a sensitive and open issue for organization and users. Smart cards allow storing digital certificates and private keys. However, in organizations where users deal with sensible data and it is mandatory to prevent the delegation of access privileges to third persons the access to secrets must be enforced by a three-factor scheme: the possession of the token, the knowledge of a PIN code and the fingerprint validation.

We presented a model that integrates smart cards, digital credential, biometric fingerprint and user password (PIN), according to the organization access policy. Our main goal was the achievement of a flexible and robust security access system to verify and ensure that the users are in fact who they claim and that avoids the delegation of authority. As a result we build a Professional Information Card system that assure stronger authentication and that can be used indistinctly in Internet and Intranet scenarios. The system was designed to fulfill current mission-critical enterprises access control requirements, and was deployed in a major Portuguese Hospital.

REFERENCES

Alliance, S., 2002. Smart Cards and Biometrics in Private-Sensitive Secure Personal Identification Systems. Smart Card Alliance. www.smartcardalliance.org

Bexiga, A. and Augusto, F., 2003. IWBDC - Interface WAP para Base de Dados Clínica. Revista do DETUA. 827-841. vol.3, issue. 8

Booz, A. and Hamilton, November 2000. Federal Deposit Insurance Corpotation (FDIC) Deploys Smart Cards & PKI to Internal Staff. Smart Card Alliance. http://estrategy.gov/smartgov/information/fdic_case_study_full.pdf.

Castle, T., 2001. Online Authentication Using Combined Smart Card and Fingerprint Recognition. Centre for Applied Reseach into Education Technology - University of Cambridge.

Costa, C., et al., 2003. An Integrated access interface to multimedia EPR. CARS2003. London - UK

Costa, C., et al., 2003. A New Concept for an Integrated Healthcare Access Model. Health Technology and Informatics - IOS Press. 101-106,95,

DataKey and DSI, S., Largest Dutch bank deploys 33000 smart cards to authenticate internal users and secure online transactions. Smart Card Alliance. www.smartcardalliance.org.

DSI, S. and Virginia, U., Department of Defense to issue up to 13 million. Common Access Cards for smart card-enabled PKI. Smart Card Alliance. www.smartcardalliance.org.

Grant, M. and Pai, G., 2001. Biometrics Authentication and Secure Processing in Networked Embedded Systems. Departement of Electric and Computer Engineering -University of Virginia.

Hachez, G., et al., 2001 October. Biometrics, Access Control, Smart Cards: A Not So Simple Combination. Security Focus Magazine. issue.

HCP Deutsche - Specifications Ver 1.0. National Association of Office Based Physicians and German Medical Association. 1999www.hcp.de

ISO-7816, 1997. ISO 7816 Identification Cards - Integrated circuit(s) cards and terminals. http://www.scia.org/aboutSmartCards/iso7816_wimages.htm.

Johner, H., et al., 2000 February. Deploying a Public Key Infrastructure. IBM. http://www.redbooks.ibm.com.

Jones, M., et al., Shell Group's info security initiatives center around 85000 smart cards with PKI and single sign on. Smart Card Alliance. www.smartcardalliance.org.

Lutz, S. and Thomas, H., 2002. PKI based Access Control with Attribute Certificates for Data held on Smartcards. Technical University of Berlin Research Center for Network and Multimedia Technology.

Marvie, R., Pellegrini, M. et al, 2000. Value-added Services: How to Benefit from Smart Cards. GDC2000. Montpellier, France

Menezes, A. J., et al., 1996. Handbook of Applied Cryptography. CRC Press.

Microsystems, S., 2001. Java Card 2.1.2 - Development Kit User´s Guide.

NIST/Biometric, 2002. Biometric Application Programming Interface (API) for Java Card. NIST/Biometric Consortium Biometric.

Norbert, P., Practical Deployment of Biometrics and IT Security,2003,

Ola, S., et al., 2003. Precise BioMatch™ Fingerprint Technology. Precise Biometrics. www.precisebiometrics.org

PC/SC, 1997. PC/SC Specifications 1.0. ("Interoperability Specification for ICCs and Personal Computer Systems"). http://www.pcscworkgroup.com/.

PKCS11, 2001. PKCS #11 v2.11: Cryptographic Token Interface Standard, revision 1. RSA Laboratories.

Ratha, N. K., et al., 2001. Enhacing security and privacy in biometrics-based authentication systems. IBM Systems Journal. 614-634,40, 3

Riha, J. and Matyas, V., 2000. Biometric Authentication Systems. Masaryk University Brno. http://citeseer.nj.nec.com/riha00biometric.html

SchSDK, 2002. Cyberflex Access Cards Programmer's Guide. Schlumberger.