On Secure e-Health Systems

Milan Marković

Banca Intesa ad Beograd, III Bulevar 1c,
11070 Belgrade, Serbia
Milan.markovic@bancaintesabeograd.com

Abstract. This paper is devoted to e-healthcare security systems based on modern security mechanisms and Public Key Infrastructure (PKI) systems. We signified that only general and multi-layered security infrastructure could cope with possible attacks to e-healthcare systems. We evaluated security mechanisms on application, transport and network layers of ISO/OSI reference model. These mechanisms include confidentiality protection based on symmetrical cryptographic algorithms and digital signature technology based on asymmetrical algorithms for authentication, integrity protection and non-repudiation. User strong authentication procedures based on smart cards, digital certificates and PKI systems are especially emphasized. We gave a brief description of smart cards, HSMs and main components of the PKI systems, emphasizing Certification Authority and its role in establishing cryptographically unique identities of the valid system users based on X.509 digital certificates. Emerging e-healthcare systems and possible appropriate security mechanisms based on proposed Generic CA model are analyzed.

Keywords: E-healthcare systems, Multilayered security systems, PKI systems, smart cards.

1 Introduction

The low-cost nature of the Internet coupled with the ease of making transactions has led to an explosive growth in e-business but trust in this medium is still a major concern. E-security is the foundation that enables trust in e-business [1], [2]. In this sense, main cryptographic aspects of modern TCP/IP computer networks are: digital signature technology based on asymmetrical cryptographic algorithms, data confidentiality by applying symmetrical cryptographic systems, and Public Key Infrastructure (PKI) systems.

The Internet is also changing the way the healthcare industry does business. It offers astounding opportunities to share information between healthcare professionals and to reduce the costly paper trail. However, organizations must create secure architecture to protect the privacy of patient records since main security requirements in healthcare, as well as in emerging mobile healthcare, systems include privacy and integrity of information related to patients. Such information includes information related to person, medical service given, and e.g. social status, and should be kept out of reach of unauthorized persons. Healthcare security benefits are: protect patient confidentiality from network-based violations, securely provide information to remote

J. Domingo-Ferrer and L. Franconi (Eds.): PSD 2006, LNCS 4302, pp. 360 – 374, 2006.

physicians, partners, and branch offices, and comply with government regulations on network security.

This paper is devoted to e-healthcare security systems based on PKI systems. We signified that only a general and multi-layered security infrastructure could cope with possible attacks to e-healthcare systems. We evaluated security mechanisms on application, transport and network layers of ISO/OSI reference model and gave examples of the today most popular security protocols applied in each of the mentioned layers. These mechanisms include confidentiality protection based on symmetrical cryptographic algorithms and digital signature technology based on asymmetrical algorithms for authentication, integrity protection and non-repudiation.

2 Multilayered Security Infrastructure in e-Healthcare Systems

Like in all the other electronic business systems, key security features that should be included in modern medical computer networks are: user and data authentication, data integrity, non-repudiation, and confidentiality. This means that in secure e-healthcare systems, the following features must be realized:

- strong user authentication both for doctors and other medical employees, as well as for patients,
- integrity of medical data transferred either via wired or wireless IP networks should be ensured and
- the non-repudiation function should be implemented.

These features are to be implemented by using digital signature technology based on asymmetrical cryptographic algorithms. Besides, the confidentiality and privacy protection of transferred data must be preserved during whole transmission and they are to be done by using symmetrical cryptographic algorithms. Also, strong user authentication techniques based on smart cards are to be implemented.

In this Section, we will give the overview of modern security mechanisms with particular emphasis on their use in medical electronic business systems and classical and mobile healthcare systems. The considered security mechanisms are based on PKI systems, digital certificates, digital signature technology, confidentiality protection, privacy protection, strong user authentication procedures and smart card technology. An overview of these techniques is given in [3].

In order to preserve the potential malicious attacks to the particular network, the multilayered security architecture has to be implemented. Modern computer networks security systems consist of security mechanisms on three different ISO/OSI reference model layers:

- Application level security (end-to-end security) based on the strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards),
- Transport level security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure,
- Network IP level security providing bulk security mechanisms on network level between network nodes – protection from the external network attacks.

These layers are projected in a way that a vulnerability of the one layer could not compromise the other layers and then the whole system is not vulnerable.

2.1 Application Level Security Mechanisms

Application level security mechanisms are based on asymmetrical and symmetrical cryptographic systems, which realize the following functions:

- Authenticity of the relying parties (asymmetrical systems),
- Integrity protection of transmitted data (asymmetrical systems),
- Non-repudiation (asymmetrical systems),
- Confidentiality protection on application level (symmetrical systems).

The most popular protocols in domain of application level security are: S/MIME, PGP, Kerberos, proxy servers on application level, SET, crypto APIs for client-server applications, etc. Most of these protocols are based on PKI X.509 digital certificates, digital signature technology based on asymmetrical algorithms (e.g. RSA) and confidentiality protection based on symmetrical algorithms (e.g. DES, 3DES, IDEA, AES, etc.) [4]. Most of the modern application level security protocols, such as: S/MIME and crypto APIs in client-server applications are based on digital signature and digital envelope technology.

In modern e-commerce and e-business systems, asymmetrical algorithms (e.g. RSA) are mainly used according to PKCS#1 standard. PKCS#1 standard [5] describes a method for encrypting data using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, according to the syntax described in PKCS#7 standard. There is a lot of work on optimization of RSA algorithm implementation in hardware security module (HSM) based on signal processor [6], [7], [8], [9]. For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key operation of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS#7 to yield a digital signature. For digital envelopes, the content to be enveloped is first encrypted by a symmetric encryption key with a symmetric encryption algorithm (such as DES, 3DES, IDEA, AES, ...), and then the symmetric encryption key is encrypted with the RSA public key of the intended recipient of the content. The encrypted content and the encrypted symmetric encryption key are represented together according to the syntax in PKCS#7 to yield a digital envelope.

Security systems on application level consist also of the user authentication procedure which could be one, two or three-component authentication procedure.

2.2 Transport Level Security Mechanisms

Security mechanisms on transport level generally include confidentiality protection of transmitted data based on symmetrical cryptographic algorithms. These systems are mostly based on establishing the cryptographic tunnel between two network nodes on transport level. The establishment of the tunnel is preceded by strong authentication procedures. In this sense, the systems are based both on symmetrical algorithms for realization of cryptographic tunnel and a bilateral challenge-response authentication procedure based on asymmetrical algorithms and PKI digital certificates for authentication of the nodes and for establishing the symmetrical session key for this tunnel session. The transport level security system is mostly used for communication protection between client with Internet browser programs (Internet Explorer, Netscape Navigator, etc.) and WEB server, and the most popular protocols are: SOCKS (used earlier), SSL/TLS and WTLS. Between them, the most popular is SSL (Secure Sockets Layer) protocol (or Transport Layer Security (TLS)), which is used for protection between client browser program and WEB server. Furthermore, the SSL is the most popular and the far widest used security protocol today.

SSL protocol consists of two phases: authentication phase with bilateral exchanging of PKI digital certificates of the WEB server and the client (optional) and establishing the symmetrical session key and secure communication based on symmetrical algorithm and established session key (cryptographic tunnel). SSL protocol is placed just below the application layer of the ISO/OSI reference model and just on top of the TCP/IP layer (transport layer). This means that the SSL is not necessarily used only under the HTTP protocol but could be used also under some other application level protocols, such as: POP3, SMTP, etc.

WTLS (Wireless Transport Layer Security) protocol is a kind of wireless version of SSL protocol and serves for transport level protection between microbrowsers on WAP (Wireless Application Protocol) enabled GSM mobile phones and WAP servers, based on the same principles and functionality as the SSL protocol. This way, WTLS protocol is intended to use for secure communication in wireless networks (GSM), and is implemented in most of microbrowsers and WAP servers. WTLS protocol uses special digital certificates for wireless communication (WAPCerts).

2.3 Network Level Security Mechanisms

Network level security mechanisms include security mechanisms implemented in communication devices and firewalls, as well as operating system security mechanisms, etc. These methods represent the basis for realization of Virtual Private Networks (VPN). Security protection is achieved by encrypting the complete IP traffic (link encryption) between two network nodes. The most popular network layer security protocols are: IPSec (AH, ESP, IKE), packet filtering and network tunneling protocols, and the widest used is IPSec. Like transport level security protocols, IPSec consists also of network node authentication based on asymmetrical cryptographic algorithms and link encryption based on symmetrical algorithms. IPSec represents a group of protocols consisting of Authentication Header (AH), Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE) protocols in transport and tunnel modes. AH is used for authentication IP packets, ESP is used for encryption and authentication the payload of the IP packets and IKE is used for authentication of the communication nodes and IPSec session key establishment. The most secure IPSec protocol is ESP in tunnel mode, since attacker does not know internal addresses (source and destination) – only addresses of IPSec gateways could be seen externally.

Firewalls also belong to network security mechanisms and could be computers, routers, workstations. Their main characteristics are to define which information and services of internal network could be accessed from the external world and who from internal network is allowed to use information and services from the external network. Firewalls are mostly installed at breakpoints between insecure external networks and secure internal network. Depending of the needs, firewalls consist of the one or more functional components from the following set: packet filter, application level gateway, and circuit level gateway. In this sense, there are four traditional examples of firewalls: Packet Filtering Firewall, Dual-Homed Firewall (with two network interface), Screened Host Firewall, Screened Subnet Firewall (with DeMilitarized Zone (DMZ) between internal and external networks). Nowadays, firewall devices are in fact multifunctional devices that include very sophisticated security mechanisms, such as: several firewall interfaces allowing more detailed secure separation of the network, antivirus, Intrusion Prevention, content filtering, VPN concentrator functionalities, etc.

3 PKI Systems

Public-key cryptography uses a combination of public and private keys, digital signature, digital certificates, and trusted third party Certification Authorities (CA), to meet the major requirements of e-business security. Before applying the security mechanisms you need the answers for the following questions: Who is your CA? Where do you store your private key? How do you know that the private key of the person or server you want to talk to is secure? Where do you find certificates?

A Public Key Infrastructure (PKI) provides the answers to the above questions. In the sense of X.509 standard, the PKI system is defined as the set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography.

PKI system provides a reliable organizational, logical and technical security environment for realization of the four main security functions of the e-business systems: authenticity, data integrity protection, non-repudiation and data confidentiality protection. PKI systems are based on digital certificates as unique cryptographic based electronic IDs of relying parties in some computer networks.

PKI system consists of the following components: Certification Authority (CA) – responsible for issuing, renewing and revoking certificates, Registration Authorities (RAs) – responsible for acquiring certificate requests and checking the identity of the certificate holders, Systems for certificate distribution – responsible for delivering the certificates to their holders, Certificate holders (subjects) – people, machines or software agents that have been issued with certificates, CP, CPS, user agreements and other basic CA documents, systems for publication of issued certificates and Certificate Revocation Lists (CRLs), and PKI applications (secure WEB transactions, secure E-mail, secure FTP, VPN, secure Internet payment, secure document management system – secure digital archives, access control system, etc.)

The method defined in X.509 for revoking certificates involves the use of a certificate revocation list (CRL). This list identifies revoked certificates and is signed and timestamped by the CA. Normally, each certificate is identified by a unique serial number that is assigned when the CA issues it. The CA publishes the CRL, at regular intervals, into the same public repository (e.g. LDAP) as the certificate themselves (only certificates with owner permissions could be published).

There are several types of CA: corporate CAs, closed user group (CUG) CA, CA of vertical industries, and public CAs. Regarding the implementation approach, CAs could be divided to: outsourced CA – when some organization use certification services from the earlier established CA, and insourced CA – when some organization establishes its own CA services (bought on the market or inhouse developed). In all cases, all CA organization mostly used the CA software-hardware technology from the established CA technology vendors, such as: Entrust, Cybertrust, Cryptomathic, Utimaco, SmartTrust, RSA Data Security, etc.

In the following, a brief description is given of the generic model of the Certification Authority software-hardware system which is realized as a web multitier architecture. The described system is similar to the most modern and most secure PKI systems today. Also, some possible variants of system realization depending on the set of the requests that should be fulfilled are discussed. This generic CA represents a solution which could be fully customized to be adapted to the customer requirements.

3.1 Main Features of the Generic CA System

The generic CA is a WEB-based Certification Authority system which could support both closed PKI systems with strictly defined users of usually only one or two different user profiles, as well as public PKI systems with more user profiles and more different ways of user registration. The generic CA system represents the public CA system fully customizable to the particular requests of different users. Main features of the generic CA system are the following:

- The system fulfils all worldwide PKI standards and could be customized according to both adding new features and customizing the applied cryptographic algorithms.
- The generic CA is WEB multitier CA application which is based on smart cards for users.
- Generic CA system supports different database servers, such as: MS SQL Oracle and IBM DB2.
- The generic CA supports a working system with one asymmetrical keypair, with two keypairs and combined system.
- The generic CA supports a hierarchical PKI structure and has the off-line Root CA and more on-line Intermediate CAs. As an example, each user profile should have its Intermediate CA server.
- The generic CA supports different ways of the user registration, such as: through registration authorities (RA) and RA operators (RAO), as well as directly (for specific user profiles) via WEB CA server.
- The generic CA has implemented a procedure of distributed responsibilities (secret sharing, necessity of presence of number of specific users) in sense of creating the Root CA asymmetrical private key for generating the new Intermediate CA certificate.
- The generic CA has a support for life cycle certificate management (renewal, suspension, revocation).
- The generic CA has possibilities for electronic personalization of the smart cards and this could be done by client themselves, RAO or CA Operators (CAO).
- The generic CA system has a support for printing PIN code (lettershop) for accessing the cards which should be sent to the user separately from the smart card.
- The generic CA system provides the printing of different reports depending of the user needs.

3.2 System Architecture of the Generic CA System

A system architecture of the described generic CA system is given on Fig. 1. What missing on the Fig. 1 are application servers from different business processes which use the generic CA system. For example, WEB server in DMZ zone could be a business WEB server which will eventually realize strong authentication procedure of the users with smart cards, issued by the described generic CA system.

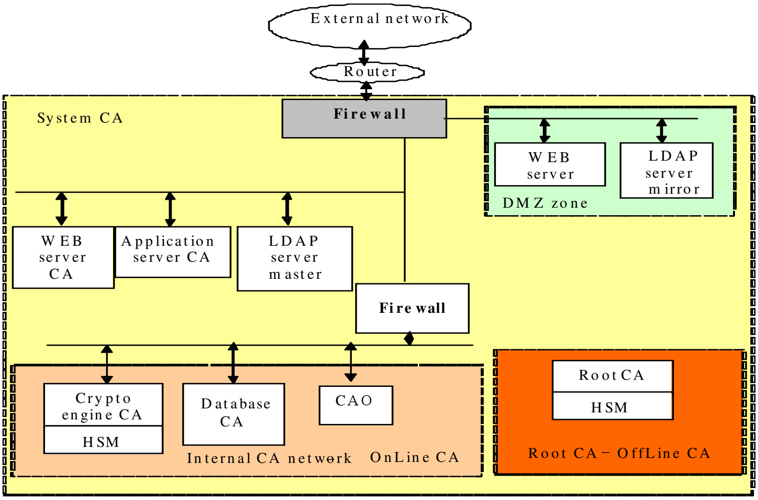

Fig. 1. A simplified network configuration of the generic CA system

As it could be seen from the Fig. 1, the generic CA system consists of OnLine and OffLine parts. OffLine part represents RootCA which is used only in rare cases when the Root CA asymmetrical private key should be activated for a purpose of generating a new Intermediate CA certificate in the hierarchical structure shown on Fig. 2, which is the most popular PKI structure in the modern PKI systems. Root CA is located in totally separated room from the rest part of the CA where there exist a vault in which individual activation parts of the Root CA asymmetrical private key are securely stored. These parts are used according to the defined procedure of “distributed responsibilities” (or “secret sharing”) in cases of generating new Intermediate CA certificates (this procedure is called “CA ceremony”). Eventually, the Root CA could be also in the same room (if necessary) as the OnLine CA but, as mandatory request, outside the LAN network and with mandatory vault for storing the activation parts of the Root CA private key.

In the CA ceremony procedure, it must be present a corresponding minimum number of special CA employees (custodians) who have access to the corresponding individual activation parts, stored on smart cards in special separated boxes of the vault, for activating the private key. Namely, a corresponding pre-defined number of smart cards must be present in order to activbate the Root CA private key in HSM device of the Root CA server, fully in accordance with General and Internal CA practices. After that, a new Intermediate CA asymmetrical keypair is generated and the Intermediate CA certificate is created (digitally signed) by a digital signature applying the Root CA private key in the Root CA's HSM. The encrypted private key and certificate of the Intermediate CA will be programmed (or generated directly onto

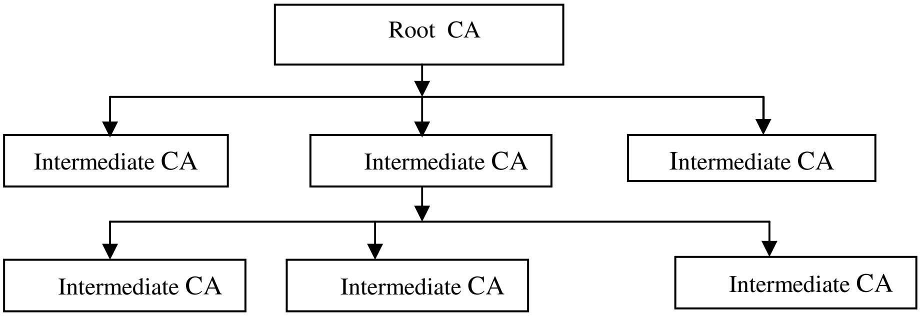

Fig. 2. Modern hierarchical structure of the Certification Authorities

the Intermediate CA's HSM) into the new smart card (Intermediate CA smart card) which will be installed into the HSM device of the new Crypto Engine server, intended for use as an OnLine CA for this Intermediate CA system. After that, Root CA private key will be deactivated from the Root CA HSM device and the smart cards with activation parts of the Root CA private key will be returned to the vault. As it could be concluded, it is possible that more Intermediate CA simultaneously work in OnLine working mode, i.e. that more Intermediate CA Crypto Engine servers are activated in the OnLine working mode for digital certificate generation (e.g. Intermediate CA for different kind of medical institutions). OnLine and OffLine parts of the generic CA system should support the use of the HSM modules, see Fig. 1.

In DMZ zone, besides WEB server, there is a LDAP mirror server which serves for publishing the CRL and ARL lists, as well as for eventual publication of issued digital certificates. This server is a copy of the master LDAP server which is located in the internal zone.

The generic CA system supports different methods for user registration, and the system is fully flexible to support different requests regarding ways of user registration according to the adopted documents (Certificate Policy and CPS) which defines the appropriate user profiles (both for individuals and legal persons). The system supports the issuing of digital certificates on different media (smart cards, mini CD, etc.) and enable functioning in the system with one or two asymmetrical keypairs. In the generic CA system, the certificate life-cycle management is implemented and comprises of the following procedures:

- Certificate renewal,
- Certificate suspension and reactivation,
- Certificate revocation.

These functions are implemented in accordance with Certificate Policy and Certificate Practise Statement of this CA system. In this case, the user will be enabled to make certificate renewal by himself, while the suspension and revocation will be done exclusively by the RAO and CA employees, according to the written procedure in Certificate Policy and CPS.

It should be mentioned that described architecture of the Generic CA system could be one example of possible realization of modern CA system and that actual implementations are more or less different depending on the way of key generation for users, the way of distribution keys and certificates, as well as on ways of CRL publishing. However, although there are differences, basic principles and concepts of the modern certification authorities are the same as in the described example. In this sense, the described Generic CA system could be a good candidate for establishing some e-healthcare PKI systems.

4 Smart Cards and Hardware Security Modules

Software only security solutions are not safe and are very vulnerable to some attacks (e.g. Trojan horse). There are several reasons why SW only security systems are not suitable: certificate and private key are stored on conventional media which is not secure, consumers are tied to their PC and are thus not mobile, and consumers are to manage certificates, which is not simple.

Hardware security modules (HSM) represent very important security issue of the modern computer networks. Main purposes of the HSM are twofold: increasing the overall system security and accelerating cryptographic functions (asymmetric and symmetric algorithms, key generation, etc.). HSMs are intended mainly for use in server applications and, optionally for client sides too in case of specialized information systems (government, military, police) [10]. For large individual usage, smart cards are more suitable as hardware security modules. However, for large usage, the best approach is in the combination of SW and smart card solutions for the best performance. Namely, smart card increases security and SW increases the total processing speed. In this sense, the most suitable large-scale solution consists of: SW for bulk symmetric data encryption/decryption plus hash calculations and smart card for digital envelop retrieval and digital signature generation. In modern and most secure PKI systems, two asymmetrical keypairs are used: one for digital envelope retrieval and the other for digital signature generation. In short, smart cards are credit-card sized plastic card with an embedded computer chip. There are several types of smart cards. Regarding the processing power, smart cards could be divided into the following categories: memory cards – containing a memory chip only with non-programmable logic, microprocessor's chip card with internal memory, microprocessor's chip card with internal memory including additional PKI capabilities (with additional RSA, 3DES, and RNG (Random Number Generator) coprocessors – called PKI smart cards). Regarding the physical contacts of the chip, smart cards could be: contact cards – chip with electrical interface, contactless cards – chip with electromagnetic interface, combo cards – with two chips: one with contact and one with contactless interface, and dual interface chip cards - with chip that have two interfaces: electrical and electromagnetic. Regarding the chip operating system, smart cards could be: proprietary operating system smart cards (with a single or multiple (MULTOS) application capabilities), and JAVA smart cards. Also, smart cards could be divided regarding the power of the implemented microprocessors (8-bit, 16-bit or 32-bit) or regarding the amount of the available memory (EEPROM) (16 KB – 128 KB).

Today's PKI smart cards are still mostly based on 8-bit microprocessors (based on the well-known Intel 80C51 microcontroller) with smaller amounts of 16-bit and 32-bit microprocessors. However, it is clear that 8-bit smart card microprocessors will be forgotten very soon and that the market will move toward more powerfull microprocessors. Also, there is a clear move toward JAVA and Multos multiapplicative smart cards instead of previously used proprietary OS – one application smart cards. JAVA and Multos smart cards enable both multiapplication and easier customization of the existing applications. Smart cards used in PKI systems provide a secure and portable way to store the private cryptographic keys and corresponding X.509 digital certificates. The smart card enhances the PKI security by enforcing an extra authentication layer at the end-user level. This extra authentication layer, coupled with the fact that cryptographic keys generated on the card never leave the card, adds an important additional security layer which increases the security of the overall solution. Actually, PKI smart cards with two X.509 digital certificates and two private asymmetric keys stored (for digital envelope retrieval/identification and for digital signature), where signature keypair is generated on the card, represents the most up-to-date security solution for large scale users which provides all four mentioned main security functions in modern information systems: authentication (X.509 digital certificate), data integrity (digital signature), non-repudiation (digital signature by asymmetric key generated and stored on the card), and confidentiality (based on asymmetric private key for digital envelope retrieval). Also, it should be emphasized that today mostly smart cards are certified according to the EAL4+ certification (certification includes: smart card (chip), chip operating system and PKI application on the card) which is a necessary condition for Secure Signature Creation Devices (SSCD) according to EU Electronic Signature legislation.

5 e-Healthcare Security Mechanisms

This Section deals with the basics of security mechanisms in e-healthcare systems. Key players in healthcare systems are: medical organizations (hospitals, clinics, pharmaceutical organizations), insurance organizations, healthcare professionals (doctors, physicians, nurses, pharmacists, etc.), and patients – end users. Most modern healthcare systems are information systems based on TCP/IP computer networks and they work fast move toward the electronic business in healthcare industry – electronic healthcare (e-healthcare). In this environment, security mechanisms for e-business must be implemented with necessary adaptation to the healthcare environments. There are a lot of technical and security issues for these systems that include, between the others: electronic patient record or electronic health record (EHR) must be fully private, central database of patient electronic records must be enabled for use from all players (medical organizations, professionals, insurance, patients), privacy protection of the patient records, secure communications between all players in the system, electronic order entry, enabling mobile healthcare, HIPAA compliance [11], etc. Thus, security mechanisms that are necessary to be implemented in these e-healthcare systems are: strong user authentication procedure, digital signature technology, confidentiality protection of data in the system on the application, transport and network layers, privacy protection of the patient personal data, strong protection of the central healthcare database based on multiple firewall architecture, and PKI systems, which issue X.509 digital certificates for all users of the system (healthcare professionals and patients) - digital identities (IDs) for the users.

5.1 Strong User Authentication

There are several types of user authentication procedures that could be based on the following components: Username/Password – PIN code – something that user know, hardware token – something that user has, and biometric characteristic (e.g. fingerprint) – something that user is.

Regarding the above components there are several types of authentication procedures which combine some of them, such as:

- Username/password based authentication – weak authentication,
- Username + dynamic password (one-time password) obtained by appropriate hardware token – stronger than previous one but not in the class of strong user authentication procedures,
- Username + dynamic password obtained by appropriate hardware token + challenge-response procedure – strong user authentication procedure,
- Username/password or PIN code + PKI smart card + bilateral challenge response procedure based on PKI X.509 digital certificate and asymmetrical cryptographic techniques – strong user authentication procedure (stronger than the previous one),
- Username/password or PIN code + PKI smart card + biometric characteristic checking + bilateral challenge response procedure based on PKI X.509 digital certificate and asymmetrical cryptographic techniques – the strongest user authentication procedure.

In other words, the class of strong user authentication procedures consists of the two or more component authentication procedures and a use of the bilateral challenge-response procedure.

Modern e-healthcare information systems must be based on the strong authentication procedure.

5.2 Digital Signature Technology

It should be pointed again that the state-of-the-art solution for all the mentioned three security functions: authenticity, data integrity and non-repudiation, could be today achieved only by use of the PKI smart cards with digital signature generation on the card with signature private key generated on the card and never leaves the card. In the modern e-healthcare systems, healthcare professionals, as well as the patients, should use the smart cards as the hardware tokens for creating digital signature. More and more EU countries demands that the signature made with e-healthcare PKI card must be qualified electronic signature according to the EU Electronic Signature Legislation.

5.3 Confidentiality Protection

Since data that is transmitted through the particular e-healthcare system contain very sensitive, often personal patient's data, its confidentiality must be fully preserved. This should be done by using digital envelope technology based on symmetrical and asymmetrical cryptographic techniques and PKCS#7 file format. This technology is based on digital certificate, symmetrical algorithms for encryption of data and asymmetrical algorithms for protection of symmetric key which is sent together with encrypted data. This technology is mainly used for application level protection and it mainly represents the protection from internal attacks to the system.

However, the transport and network level protections should be also used in the system in order to prevent external attacks. Namely, besides the application level protection based on digital signature and envelope technologies, that are based on the end users smart cards, the transport level (SSL) and network level (IPSec/VPN) security mechanisms should be used. In other words, it is strongly recommended that security mechanisms on more than one level are to be used. In this sense, the application level protection should be mandatory in combination with one or two additional level protections, transport or network based, depending of system characteristics, type of application and connections, required system throughput, other technical requirements, etc.

5.4 Privacy Protection of the Personal Patient Data

It is already emphasized that the main issue of the e-healthcare system is to protect privacy of the patient personal medical data – now processed and stored in the electronic form. This means that the data should be protected on the whole processing path in the system, i.e. from the medical professional workstation to the central database. In other words, unauthorized access to the data should be protected in the entire e-healthcare system.

5.5 Protection of the Central Database

As we already mentioned, the central e-healthcare database should be maximally protected from internal and external attacks. Normally, the new designed e-healthcare application should be multi-tier (three or more tiers) applications that could be WEB based or client-server based applications. Modern trends move toward web based applications with pretty thin clients [12]. Client's part of the application should prepare data (e.g. offline) which includes applying of the appropriate security mechanisms (digital signature and digital envelope based on smart cards) and send this data (in online mode) through web browser interface to the web site (e.g. e-healthcare WEB portal) on the central (or other) location. Before sending data to the web portal, the enduser must authenticate himself on the web portal by using the strong authentication PKI procedure based on smart card and digital certificates. Modern trends move toward establishing web portal for different medical organizations (or for central point) with single-sign-on capabilities of end-user authentication. This means that administration of the valid users should be centralized and that users cannot do any action if they are not strongly authenticated before through adequate single-sign-on function.

A possible example of Generic model of the central e-healthcare site is proposed on Fig. 3. In this model, we could see four different parts of the central medical site:

- External part for accessing the system which is on the one side of Firewall (connected to one particular interface of the firewall),
- DMZ – DeMilitarized Zone with some general purpose servers, such as: mail, ftp, http, as well as with the WEB e-healthcare portal,

- Internal zone with different applications servers – middle tiers of different multitier medical applications, and
- Most secure internal zone where the most sensitive parts of the system (e.g. central EHR database) are located.

In this model, multiple firewall architecture is applied. Between the external part and one or more DMZs, the commercial firewall (mostly based on packet filtering techniques) could be applied. However, for the protection of the most sensitive part of the system – the central database, some firewall of the application proxy level gateway type should be applied, e.g. [13], [14]. The best protection will be achieved if this second firewall will be the proprietary made firewall – and not a commercial one.

5.6 e-Healthcare PKI Systems

To enable application of the all previously mentioned security mechanisms, the appropriate PKI system must be established in advance. The e-healthcare PKI system has the following characteristics: it is based on X.509 digital certificates as digital IDs for valid users of the system, central point of the PKI system is Certification Authority (CA), and CA issues digital certificates on smart cards (patient and healthcare professionals' smart cards). In integrated e-healthcare medical systems, the CA could be truly centralized, centralized with hierarchical CA structure or decentralized. In the truly centralized system, there is only one CA (most often at some state healthcare authority) who issues all digital certificates for all kind of end-users (patients, healthcare professionals, insurance employees, etc.). In this system, individual medical organizations are not independent in defining its own PKI policy but must conform to the global healthcare PKI policy.

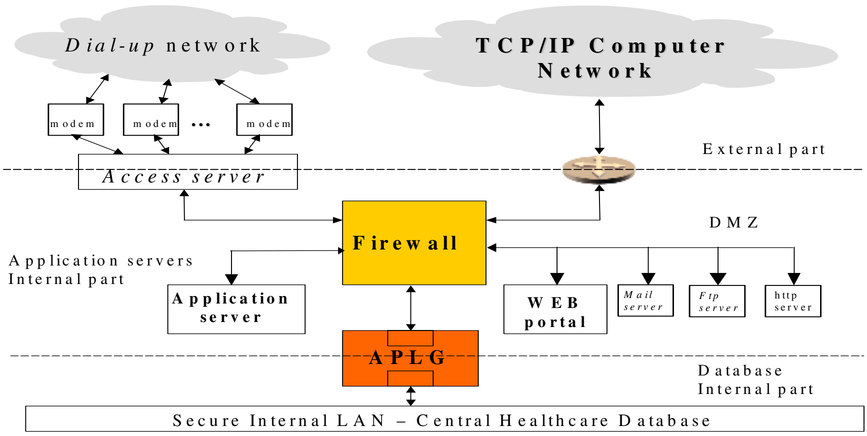

Fig. 3. A generic model of the central (or other) healthcare site

In the centralized system with hierarchical CA structure, there is a root CA at the healthcare authority and several levels of intermediate CAs. These intermediate CAs will be for different kind of end users and for individual medical organizations (e.g.

some clinic that has a large information system). The advantage of this architecture is that medical organizations are independent in creation of their own PKI subsystems and that each of the users group is under the one certificate management system. However, since all of the intermediate CAs is under the one centralized root CA, compatibility of communications between parties belonging to different intermediate CAs is completely achieved. Decentralized CA structure could be used in the case that all medical organizations have their own PKI subsystem, independent of some centralized authority. This system provides independency but there is an issue regarding the communications between parties that does not belong to the same CA. In this case, this could be only achieved by applying the cross-certification procedure between the CAs. The trend is that modern e-healthcare information systems are based on the centralized PKI system with hierarchical security infrastructure and digital certificates stored on smart cards.

6 Conclusions

In this paper, the modern computer security systems are analyzed and their possible application in e-healthcare systems is emphasized. It is concluded that only multilayered security architecture could cope with potential internal and external attacks to the modern computer networks and e-healthcare systems. The most frequently used security mechanisms on the application, transport and network layers are analyzed. It is concluded that more than one layer should be covered by the appropriate security mechanisms in order to achieve high quality cryptography protection of the e-healthcare system. It is also concluded that, between many specific conditions in the e-healthcare systems, application of security mechanisms should be considered on the client side, communication side and central database side, and that, in each of the sides, appropriate security measures should be applied. Central points of e-healthcare systems are smart cards for end users (citizens, healthcare professionals, etc.) that could be used for applying digital signature and digital envelope technology and the central PKI system. Smart cards must be used by doctors and other healthcare professionals. For patients, main point is that data should be protected from unauthorized use (privacy protection) and thus it is not mandatory to use PKI smart cards for patients. However, in order to enable some future advance features, as well as the qualified signature, it is strongly recommended that PKI smart cards be used for patients too.

References

1. Oppliger, R.: Internet and Intranet Security, Artech House, (1998), ISBN 0-89006-829.
2. Ford, W., Baum, M.S.: Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Second Edition, Prentice Hall PTR, Upper Saddle River, NJ 07458, (2001).
3. Marković, M.: Cryptographic Techniques and Security Protocols in Modern TCP/IP Computer Networks, Short-Tutorial, in Proc. of ICEST 2002, Oct. 1-4, (2002).

4. Schneier, B.: Applied Cryptography, Second Edition, Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc., New York, Chichester, Brisbane, Toronto, Singapore, (1996).
5. RSA Laboratories: PKCS standards.
6. Marković, M., Unkašević, T., Djorđević, G.: RSA algorithm optimization on assembler of TI TMS320C54x signal processors, in Proc. of EUSIPCO 2002, Toulouse, France, Sept. 3-6, (2002).
7. Unkašević, T., Marković, M., Djorđević, G.: Optimization of RSA algorithm implementation on TI TMS320C54x signal processors based on a modified Karatsuba-Offman's algorithm, in Proc. of ECMCS'2001, 11-13 September, Budapest, (2001).
8. Djorđević, G., Unkašević, T., Marković, M.: Optimization of modular reduction procedure in RSA algorithm implementation on assembler of TMS320C54x signal processors, DSP 2002, July, Santorini, Greece, (2002).
9. Marković, M., Đorđević, G., Unkašević, T.: On Optimizing RSA Algorithm Implementation on Signal Processor Regarding Asymmetric Private Key Length, in Proc. of WISP 2003, Budapest, Sept. 2003, (2003), 73-77.
10. Marković, M., Savić, Z., Obrenović, Ž., Nikolić, A.: A PC Cryptographic Coprocessor Based on TI Signal Processor and Smart Card System, Communications and Multimedia Security Issues of the New Century, R. Steinmetz, J. Dittman, M. Steinebach, (Eds.), Kluwer Ac. Publishers, (2001), 383.393.
11. Healthcare Insurance Portability and Accountability Act: HIPAA Requirements for Technical Security, Services and Mechanisms, (1996).
12. Oppliger, R.: Security Technologies for the World Wide Web, Artech House, Boston, London. (2000).
13. Savić, Z., Nikolić, A., Marković, M.: Cryptographic proxy gateways in securing TCP/IP computer networks, In Proc. of Information Security Solution Europe, ISSE 2001, London, UK, (2001).
14. Savić, Z., Marković, M.: Development of Secure Web Financial Services in Serbia, in Proc. of ISSE 2003, Vienna, Austria, October 7-10, (2003).