Trusted Third Party Services for Deploying Secure Telemedical Applications over the WWW*+

Diomidis SPINELLIS[1], **Stefanos GRITZALIS**[1,2], **John ILIADIS**[1], **Dimitris GRITZALIS**[3] and **Sokratis KATSIKAS**[1]

[1] *Dept. of Information and Communication Systems, University of the Aegean*
Samos GR-83200, Greece. email: {dspin, ska}@aegean.gr

[2] *Dept. of Informatics, Athens Technological Educational Institute (TEI)*
Ag. Spiridonos St., Aegaleo GR-12243, Greece. e-mail: {sgritz, jilliad@aegean.gr}

[3] *Dept. of Informatics, Athens University of Economics and Business*
76 Patission St., Athens GR-10434, Greece. email: dgrit@aueb.gr

Abstract

The EUROMED-ETS schema provides a robust security framework for telemedical applications operating over the World Wide Web. It is based on a trusted third party architecture under which certificate authorities store the public-key certificates of participating hospitals and medical practitioners. Digital signatures are used to provide peer and data origin authentication, and, in combination with access control lists, to provide access control. The deployed infrastructure is based on off-the-shelf available clients and servers, and provides functions for electronic registration of participants, session initialisation, user authentication, key generation and personalisation, certificate generation, distribution, storage and retrieval, certificate revocation lists, and auditing. It was found that, as the underlying technologies mature, a Web-based trusted third party architecture provides a viable solution for delivering secure telemedical applications.

Keywords

Information Security, Medical Information System, Healthcare Information System, Trusted Third Party, Digital Signature, World Wide Web.

Acknowledgements: This work was partially funded by the European Commission under the Eurpean Trusyted Services (ETS) Programme (EUROMED-ETS project). The authors would like to thank their project partners for many helpful and constructive discussions.

---

* *Computers and Security*, 18(7), 1999.

+This is a machine-readable rendering of a working paper draft that led to a publication. The publication should always be cited in preference to this draft using the reference in the previous footnote. This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

1. INTRODUCTION

1.1 Security in the Internet and the WWW

Information and Communication Technology applications have rapidly evolved from stand-alone centralised computer systems to open networks and distributed computing environments, establishing communication among different computing systems via local area networks and the Internet. This increasing interconnectivity means that more information is being carried electronically, so that the risk of possible attacks such as eavesdropping, non-authorised access and modification, replay-attack and masquerade [1,2] increases dramatically.

Regarding Internet, in 1990, *CERT* reported 130 security incidents; by 1996, the number of incidents had increased to 2,573 [3]. In these circumstances, when the *Yankee Group* interviewed Information Systems managers about prospective use of the Internet, *9 out of 10* said they would use it if they believe that it was safe. On the other hand, *3 out of 4* said they do not feel confident in Internet security [3]. According to a relevant *Ernst & Young* and *Information Week* survey, 85% of the interviewed Information System managers stated that security risks have increased over the past five years. However, rather than refusing to use Internet, the risks have resulted in a rise in the number of institutions that have appointed a full-time security specialist. As a result of this attitude, *8 out of 10* of the companies interviewed had a full-time security director.

From a technical point of view, most Internet services are based on the *client/server* model. Under this model, one program requests service from another program. A client/server application that has grown to be most popular on the Internet is the *World Wide Web (WWW, Web)*. The Web is a distributed hypertext-based information system developed to be a pool of human knowledge allowing collaborators on remote sites to share ideas and information.

The Web was conceived in 1990 at CERN in order to provide its user community with a friendly way to access global information. Information is displayed on the Web as a set of pages, written in the HyperText Markup Language (HTML) [4]. These pages are usually stored on dedicated computers equipped with software that receives network requests from the *Web clients* and transmits HTML files in response. The term *Web server* is used to describe both the computer and the software that supports the aforementioned process.

Although the Web is one of the most useful applications of the Internet, the designers of it did not adequately consider protection and security when implementing the service; they opted for complete openness. As a result, the demand for security services for potential users has grown rapidly. New applications such as telemedical applications, electronic commerce and business transactions have driven the development of an integrated framework to provide security capabilities on the Web.

The Web security problem consists of three major parts [5]:

- securing the Web server and the data that is on it,
- securing information that travels between the Web server and the user,
- securing the user's own computer.

Accordingly, in many cases we have to address major complementary issues such as:

- identification and authentication between communicating parties,
- information privacy,
- information integrity in terms of origin of data, destination, content and non-repudiation,
- logging and auditing information about the transaction for purposes of non-repudiation, conflict resolution and investigation of misuse.

The obstacles in the way of public and private institutions implementing security, in the "era of Internet and the WWW", are clearly stated in the results of a survey from *InfoSecurity News* [3]. This survey lists the main roadblocks to security according to Information Systems managers. These roadblocks are presented in Table 1.

Roadblock	% reporting
Unclear responsibilities	42
Lack of management support	46
Lack of management awareness	46
Budget constraints	56
Lack of user awareness	73

Table 1: Roadblocks to security

1.2 The EUROMED platform

Telemedicine is the interactive audio-visual communication between healthcare providers and patients or other healthcare providers regardless of geographic distance. EUROMED is a European Commission's funded project with the objective [6] to exploit, combine and support High Performance Computing Networking (HPCN) activities to enhance and standardise visualisation techniques to be used in telemedical applications over Europe. It utilises the Web as the basic navigational medium to remotely access multimedia medical information.

EUROMED's network consists of a number of Internet sites which store patient medical data as well as image processing and archive applications. A physician seeking information to reach diagnosis for a given patient searches the Internet using a Web browser and collects available medical data for this patient. Data may be images coming from different modalities such as X-rays, biosignals, results of biochemical examinations and reports.

EUROMED is based on interlinked HTML pages which allow authorised users to access medical data, input them to Java applications invoked from other pages and archive the results by updating links to the old pages. As a result, it has created three hierarchical infrastructures:

- The *Hierarchical Communications Network (HCN)* using Internet, satellite and telecommunications networks (e.g. ISDN, ATM, etc.) which connects dispersed isolated regions (e.g. the Greek islands in the Aegean archipelago and cities on the Italian mountains with mainland European countries.

- The *Hierarchical Computing Facilities Infrastructure (HCFI),* which includes a range of High Performance Computing (HPC) platforms powerful workstations and PCs, providing heterogeneous computing facilities to every node in the HCN.
- The *Hierarchical Medical Facilities Infrastructure (HMFI),* which consists of specialised clinics, general hospitals and local doctors which can collaborate and facilitate a uniform level of medical practices.

Moreover, EUROMED has developed a hierarchical telemedical Visualisation Suite of packages incorporating, superimposing and enhancing DICOM 3 image modalities such as CT, PET, MRI and supporting techniques such as ultrasound diffraction tomography.

The remaining of this paper is organised as follows: In section 2, the requirements which were placed on EUROMED-ETS (the security-oriented enhancement of EUROMED) by the EUROMED project are described. In section 3, an integrated framework design for secure Web-based telemedical applications is also described. Section 4 contains the steps taken in order to implement a pilot solution. In section 5, the major problems which were faced during the pilot stage are discussed. Finally, section 6 contains concluding remarks and our view of future research directions.

2. EUROMED REQUIREMENTS

According to the Council of Europe Recommendation R(97)5 on the Protection of Medical Data [7] *"... Appropriate technical and organisational measures shall be taken to protect Personal Data processed in accordance with this recommendation against accidental or illegal destruction, accidental loss as well as against unauthorised access, alteration, communication or any other form of processing. Such measures shall ensure an appropriate level of security taking into account, on the one hand, of the technical state-of-the-art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks".*

It is obvious that a system, based entirely on the Web for its functions, is vulnerable to a variety of security threats. In particular, by monitoring communication lines, wiretappers may gain unauthorised access to local or remote medical data, thereby violating the patient's privacy. Malicious users may store false, corrupt or modified data, resulting the false diagnosis of a patient; these users might masquerade as valid local or remote users, causing accountability problems. Finally, an ingenious intruder may substitute a whole site by a masquerade site. EUROMED-ETS should deal with the above major threats EUROMED faces using state-of-the-art technology.

The general requirements which were placed on EUROMED-ETS are the following:

- the public Internet shall be used as the communications infrastructure,
- HTTP and other Web protocols shall be used as the transport mechanism,
- all security mechanisms that will be implemented shall be application-transparent,
- technology that will be proposed must be widespread, as mature as possible and widely accepted,
- the strategies that will be adopted shall provide for the widest possible deployment of the project results,

- proposed solutions must be supported by equipment ranging from a single PC to high performance supercomputer clusters,
- a variety of sites shall be taken into consideration, ranging from large organisations to isolated medical stations,
- sites, regardless of size, power of equipment, or location, shall hold patient or image medical data that need to be made available to other sites in a secure manner,
- no sites other than TTP sites should be required to take over security functions that will be proposed.

With respect to R(97)5, the objective was to guard two major components of security, that is *confidentiality* (information is not made available or disclosed to unauthorised individuals, entities or processes), and *integrity* (the prevention of unauthorised modification of information). EUROMED-ETS deals with the threats EUROMED faces by providing the appropriate services using measures such as *digital signatures* to prove the authenticity and integrity of data, and *encryption* to provide confidentiality.

In the context of providing these measures, technical, organisational, medical and ethical aspects have been considered. The first aim of the security mechanisms was to protect the access of the personal homepage related to the patient, since from the personal home page one can see all relevant medical data. According to the relevant requirements, EUROMED-ETS has concentrated on HCN and HMFI levels of EUROMED's platform.

From a technical point of view, the possible threats to a generic internetworked environment were also taken under consideration. These threats have been assessed [3] and the results of the assessment are described in Table 2.

Internet access	Threats
Leased-line Internet access	Penetration of corporate network by hackers
FTP access, WWW access	Viruses in downloaded software, Trojan horses
E-mail	Tampering, Forgery, Interception
Usenet news	Postings by employees, which reveal corporate information
WWW, FTP and Gopher servers	HTML files tampered with, Access to sensitive files, Exploiting holes that enable intruder to take over server or access corporate network
Dial-in/dial-out	Password protection penetration
Communication with business partners or branch offices over the Internet	Private nature of communications could endanger business if overheard by competitors

Table 2: Assessment of threats in a internetworked environment

3. EUROMED-ETS: AN INTEGRATED FRAMEWORK DESIGN

3.1 Architectural issues

Most of the security problems mentioned above can be solved by applying cryptographic technologies. There are two general forms of key-based cryptographic algorithms [5]:

- *Private key or symmetric algorithms*, which use the same key to encrypt and decrypt the message; the security of a symmetric algorithm rests in the key and therefore the key needs to be secret.
- *Public-key or asymmetric algorithms*, which use a public key to encrypt the message and a private key to decrypt it; the name "public key" comes from the fact that one can make the encryption key public without compromising the secrecy of the message or the decryption key. The secret key must remain hidden in the owner's private domain.

The main advantages offered by public key cryptosystems are: a) their scalability to very large systems, b) the flexibility of authentication, c) the support of digital signatures, and d) the potential of non-repudiation enforcement. Although public-key algorithms make the key management process easier, the need for entities to make their public key widely known poses new problems. The available mechanisms for the publication are insecure. Web pages, white pages directories, finger files, and the Domain Name System are mechanisms commonly considered. However, it is not possible to store a public key using these mechanisms, as the key itself could be modified and the whole process could cause an integrity violation of a user's public key.

The assurance scheme provided will be acceptable when it is based on the use of a public-key *certificate*. This is an information package which includes the user's identity, the user's public key and is digitally signed by a trustworthy entity known as *Trusted Third Party (TTP).* When this scheme is applied to a security infrastructure based on public key techniques, the TTP is known as a *Certification Authority (CA).*

The security solution proposed in this paper is based on secure Web communication and TTP services. The available security concepts and technologies are presented in Table 3. Among them, the mechanisms proposed and utilised by our approach are denoted in italics.

3.2 Responses to threats

Methodologically, the list with the assessed possible threats (see Table 2) has to be followed by a list of techniques addressing/responding to these threats. In our case, this was done before we described the functions needed to support the certification process. The relevant results are briefly described in Table 3.

3.3 Functions for supporting the certification process

The reference framework for CAs specifies a set of functions which support the certification process. Every EUROMED-ETS CA performs the sub-processes identified in the sequel.

Threat	Technique	Policy implications
Penetration of corporate network by hackers	• Host-based security measures, firewall that translates IP address • Password enforcement • Network monitoring	• No ad hoc desktop Internet connections • Guidelines for selecting appropriate passwords • Use of password checking software
Viruses, Trojan Horses	• Antivirus software • Monitoring tools	• Check downloaded files • Install legitimate software
Tampering, forgery, interception	• Secure e-mail with digital signatures	• Users awareness • Users training
Postings by employees revealing corporate information	• Personnel issue	• Use of disclaimers • Limited use of Usenet
HTML files tampered with, access to sensitive files, exploitation of security holes	• Monitoring software • Proper server configuration • Topology placing Web server outside firewall	• No ad hoc public WWW servers • Control who changes HTML files
Penetration of password protection	• Dial-in/dial-out outside the corporate firewall • Use one-time passwords • Use of secure modems	• User awareness • User training
Private nature of communications could endanger business if overheard by competitors	• VPN over the Internet	• Agreement to use encryption • Restricted encryption

Table 3: Threats and methods to respond

Electronic registration

Every user who wishes to communicate with an entity in a specific networking group must register with the appropriate CA. Practically, the first step of the electronic registration process includes the registration request to the CA. The CA will forward this request to the *Registration Authority* (RA). The latter will verify out of band the identification data included in the registration request and if it is valid, it will inform the CA that it can proceed with the issuance of the certificate for that entity. Finally, the CA will generate the certificate and communicate it to the requesting entity. When the entity confirms that it has received and installed a valid certificate, the CA will store that certificate in the Directory maintained by the Registration Authority.

Security services	Security concepts and technologies
Authentication (Peer and data origin)	Digital Signatures
Authorisation and Access Control	*Digital Signatures*, *Access Control Lists*, IPv6 (for Internet-wide authentication), Passwords/passphrases, Biometrics, Tokens
Integrity	*Digital Signatures*, *Check Values*, Antivirus software
Control	Firewalls, Intrusion detection and prevention systems
Confidentiality	*Encryption*, Network address translation, File permissions on host computer
Accountability	Audit trails, Logs, Receipts

Table 3: Security services - Security mechanisms relationship

Initialisation

The first step establishes the details of the session between requester entity and CA. This step allows the requester and CA to synchronise their cryptographic working environments. In other words, both parties interchange information about the selected cryptographic algorithms, cryptographic protocols, certification and key exchange protocols in order to establish a secure communication channel. This phase comprises the *Secure Session Layer* (SSL) handshake [8]. Essentially, the CA public certificate is being communicated to the client in order for it to be able to send, in encrypted form, the symmetric key and the algorithm it has selected for that session.

Authentication

This step entails the appropriate actions for the entity's authentication process. Authentication procedures and mechanisms [9] involve some sort of validation approach to produce evidence or confidence that a reported identity must have been valid. When the authentication process succeeds the authorisation authority informs a CA to issue the certificate with specific granted privileges.

Key personalisation, generation and repository

Key Personalisation is the process of associating a key pair with the registered name of one and only one specific entity. The latter is responsible for the generation of its own keypair; the secret key never leaves the entity’s storage, while the public key is communicated securely, via SSL, to the CA. The public key remains in the local CA repository to be used in the certificate generation process.

Naming

To provide meaningful authentication services each entity in the domain needs to be uniquely identified by a name. If there are many participants, the use of the name may not be enough and a service is required which will guarantee unambiguous names or aliases. It is for this reason that the assignment of names to the entities should be done hierarchically, accordingly to the X.500 specifications.

Certificates: Structure, generation, distribution, storage, and retrieval

Certificates are generated by TTPs with the help of a Certificate Management System software. Certificates are signed using the 1024 bit CA's private key. CAs are responsible for sending copies of the certificates they generate to the appropriate directory server and keeping another backup to the local repository. Accordingly, once a CA generates a certificate, it will provide a copy of it to the user with whom it is associated. The certificate is transferred to the user by means of e-mail. Another option is to notify the user that the certificate has been issued and notify him of a specific URL from which he may download and install his certificate.

It is useful for the CAs to perform management functions on these certificates it generates. In order to provide these services (e.g. notifying a user when a certificate is about to expire or revoking certificates) the CA will use the local repository in order to store and retrieve the certificates it generates. Expired or revoked certificates should be removed from the Directory.

Auditing

To provide additional assurance of the trusted nature of CAs and to provide information to agency personnel conducting internal audits, the actions of each CA should be audited. Audit records and audit trails are generated for events such as user registration, certificate request and receipt, compromised key reports, etc.

Certificate directory management

Directory services are offered by TTPs mainly according to the CCITT X.500-X.521 recommendations [10]. Both physical persons and application entities, including CAs, are mapped to Directory objects. In these objects, certificates are stored together with naming, addressing and other object-specific information.

Although the developed trust model is designed according to the hierarchical trust model, the overall Directory set-up is still an open issue, since it depends heavily on organisational factors that vary across different organisations and countries. From a management point of view, the Directory consists of several certified *Directory System Agent* (DSA) application entities. Each DSA is responsible for the local subtrees of the *Directory Information Tree* (DIT). For both safety and efficiency reasons, it is possible to replicate subtrees across DSAs. The objects contained in each subtree are maintained by authorised managing personnel. The DIT subtrees are updated with certificate information by the TTP CMS software, whenever the latter creates, updates or revokes certificates.

End entities consult the Directory in order to verify names, obtain certificate information, verify authentication information presented by other end-entities, and check for possible revocation of certificates. This communication is done using the *Lightweight Directory Access Protocol* (LDAP) [10] over SSL. For this purpose, the DSAs are themselves certified by a CA, so that they can offer SSL connections.

CRLs: Structure, generation and maintenance, distribution, storage, and retrieval

Certificate Revocation Lists (CRL) include information, such as the CRL issuer's identifier, the serial numbers of the revoked certificates and the date each certificate was revoked. The CRL is signed by the issuer using its private key. CAs generate CRLs that denote which certificates are no longer valid due to compromise or to employee severance. Each CA

generates CRLs for the certificates that it has generated. The CA ensures that the information within the CRL is as current as possible. Therefore the CA updates its CRLs periodically in order to incorporate new information.

Integrity of the root public and private keys

Special procedures are guaranteeing the integrity of the public keys at the top of the trust hierarchy since the trust and integrity of the whole certification process hinges on these public keys. SSL is used to guarantee the integrity of communication when entities look up the root key. Backups of the Root Public Keys, signed with the private keys of the root Administrators, should be handed out to a number of officials.

Date and time stamping services

In many applications time and date stamps must be affixed to documentation to denote when the documentation was received or sent. Certification information is always time-stamped. If the documentation is generated by and sent via electronic means, the date and time-stamp must also be generated and affixed to the document electronically. According to the relevant requirements, time-stamping does not need to be implemented at this stage of development. Our approach claims that the use of DICOM, which has the capability of offering an elementary time-stamping service, may prevent the replay attacks and non-repudiation and thus TTPs need not provide time-stamping services at this stage.

4. IMPLEMENTING THE EUROMED-ETS SOLUTION

4.1 Technical infrastructure

EUROMED-ETS deals with most of the major threats EUROMED faces by providing confidentiality and integrity services, using measures such as digital signatures and cost/ effective encryption techniques. Telemedical applications over the Web are secured with the establishment of TTP services and *Secure Session Layer* (SSL) [8,12], solution which is characterised by its open architecture and its potential to interoperate with a large number of Web tools.

During the pilot implementation of the approach, TTP services were established in four different sites in Europe, namely in ICCS (Athens-Greece), UHM (Magdeburg-Germany), UoA (Samos-Greece) and UniCAL (Calabria-Italy).

The TTP security scheme used by the our Security Architecture consists of the following components [6]:

- *Directory Services* have been used to manipulate and store the identification and authentication information of all the objects which participate in our scheme (e.g. users, servers, workstations).
- *Certificate Servers* provide the necessary certificates X.509v3 [13] to materialise the TTP security scheme.
- *Secure Web Servers* are used as platforms on which the Web-enabled, medical applications of EUROMED run.

The main component, which is secured by the aforementioned EUROMED-ETS security components is the EUROMED-PC software. This is a low cost implementation realisation of

EUROMED for personal computers. Its purpose is to provide telemedical services to areas characterised by low infrastructure in computer or communications technology.

The technical characteristics of the hardware used in the pilot phase were selected in order to fulfil essentially any need that we could possibly come up with, in the course of the research and implementation. High-performance Personal Computers and SunSparc workstations and servers located in four distant regions were communicating through the Internet. The TTP Servers were running on Solaris and Windows NT computers while the client machines were operating under the Windows NT and Windows 95/98. Interoperability between the TTP servers and clients running on these machines was tested thoroughly with success.

The software components of the EUROMED-ETS implementation are depicted Figure 1. A report on these components and their role to the EUROMED-ETS TTP implementation is presented in the sequel.

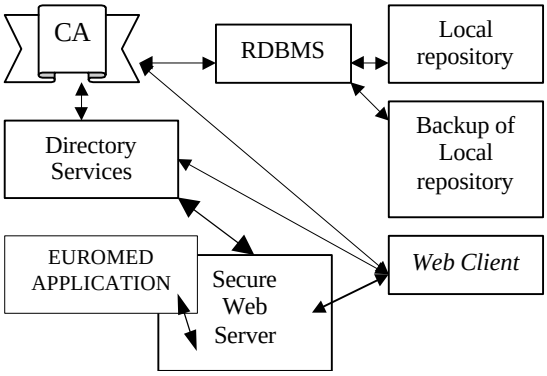

Figure 1: TTP infrastructure

EUROMED application

The EUROMED application, operating on EUROMED-PC, is WebTSN ver.1.0, The medical records kept by this application may be accessed either locally through a Windows application, or remotely; the application interoperates with Web Servers, providing thus an HTML interface accessible to any user who possesses a valid certificate and proper access rights. The database used by the application itself to keep the medical records at a local level is *Local Interbase*.

Web server

Netscape Enterprise v3.0 was chosen as our Web Server. The selection was made between numerous Web Servers. Enterprise v3.0 was the only one, at the implementation time, that offered both advanced Web capabilities and the SSLv3 encryption scheme. Moreover, its functions and especially the administration menus and operations are tightly integrated with those of the other Servers we have chosen to use in the pilot. Besides that, it provides LDAP integration, so that the users and access rights can be stored directly to an LDAP Directory. This protocol is specifically targeted at management and browser applications that provide simple read/write interactive access to the X.500 Directory while not incurring the resource requirements of the *Directory Access Protocol* (DAP).

Certificate server

Similarly, Netscape's Certificate Server v1.01 was chosen as a CA for the pilot. It can issue certificates for SSL-based authentication, S/MIME and object signing. It supports all the standards that were included in our CA requirements (e.g. X.509v3, SSLv3, PKCS and LDAP). It provides full LDAP integration, that is the certificates and other user data may be published directly to an LDAP Directory. Moreover, the Web-based certificate management enables a certificate issuer or a CA administrator to execute jobs remotely. The local database used by the Certificate Server in order to store the issued certificates was Informix OnLine 7.2, a cut-down version included in the Netscape Certificate Server package.

Directory server

The Directory Server used was Netscape's Directory Server v1.02. It supports LDAPv2 [11,14]. In addition, it supports referrals, as they have been introduced to the LDAP protocol [15]. Furthermore, it allows administrators to extend the directory schema to keep track of new information. Finally, it keeps error, access and change logs with varying administrator-controllable levels of detail.

Web client

Netscape Navigator and the Netscape Communicator were used as clients. It should be mentioned that only the latter is equipped with an integrated LDAP search tool which can be used separately from the browser. Navigator has no such tool, but one may use the Web Directory Gateway available by Netscape Directory Services 1.02 in order to query the Directory.

Management and testing tools

Other tools used were: a) LDAP tools by Netscape (command line and Communicator incorporated versions), b) SSLeay [5,16] (it was used to check interoperation between Netscape products and other pertinent implementations), c) Network sniffing tools (sniffit, tcpdump operating under the Unix OS), d) CGI scripts, e) Web authoring tools (Netscape Communicator v4.0), f) Network Operation Centre (NOC) tools as well as various public domain tools available for the Unix OS.

4.2 Organisational set-up of TTP sites

TTP sites and organisational roles

During the pilot implementation, services were established, as described above, in ICCS (Athens-Greece), UHM (Magdeburg-Germany), UoA (Samos-Greece) and UniCAL (Calabria-Italy). The specific organisational setup of the pilot was designed and applied in order to balance the workload between the pilot team members and therefore take advantage of the knowledge and experience in similar projects of that team to the maximum degree.

The roles assumed by the pilot team were [6]: a) Professionals, b) Certificate Authority operators and administrators, c) Directory Server administrators, d) Secure Web server administrator, e) EUROMED site operators, f) Testers, g) Documentors and h) the Help Desk support team.

Certification scheme

In the hierarchical certification scheme selected at the pilot phase, ICCS was the root Certificate Authority. UoA was the first level subordinate Certificate Authority. All other partners were requesting and receiving certificates (either CA or server/personal certificates) from the UoA CA.

Directory Services were setup by UoA and ICCS, hosting identification and authentication information for the entities belonging to the UoA and ICCS domains. These Directory Servers received SSL key certificates from the reciprocal Certificate Authorities. Secure Web Servers were setup by all pilot partners. The SSL key certificates that were installed in those Web Servers were issued by the reciprocal Certificate Authorities. Finally, client certificates were issued for every pilot team member by their local Certificate Authorities.

The RSA keys used in the aforementioned certificates had a length of 512 bits (US export version). These should be changed often enough to protect the confidentiality of the SSL sessions. The RSA keys used from the CA for signing keys and issuing the respective certificates had a length of 1024 bits.

Directory setup

The role of a Directory in a TTP security scheme is to serve as a repository for identification and authentication information. This information is used automatically by the Secure Web Servers to identify potential users and grant or deny to them certain rights. One can divide the Directory structures into referral and replication-based. In referral-based structures, the Directory branches contain only the local entries. If a query for an external entity is made, then the local Directory refers that query to the corresponding directory branch. Another Directory structure is based on replication, that is all Directory branches contain the same entries; they achieve that by replicating the entries of the "main" Directory. The latter is the only directory which can be modified at any time; all the others just replicate the modified entries of it. However, all directory branches can be used to serve queries of any kind, for any entity, since each one of them contains the whole Directory. Due to the vast amount of information that will be contained in a real-world Directory, replication would not be feasible, so referrals were preferred.

Personnel and training of TTP members

Every member's pilot team consisted of a small group of persons, each charged with different responsibilities. The task categories were: a) System Administration, b) Server Installation and Administration, c) Audit Control, d) Pilot Management, e) Pilot Documentation, and f) Pilot Testing. Each candidate member, before joining the unit, was given a weekly, full time, training course by the co-ordinator. This course contained information on cryptographic algorithms, protocols, software and management issues.

4.3 Legal issues concerning TTPs

The TTPs implemented were to be used for communicating personal health data via the Web. This data is protected by the requirements of the European Convention on Human Rights [17], and the recommendations on the Protection of Medical and Genetic Data [18]. With respect to them, the TTPs must meet the requirements of the European Union Data Protection Directive.

The safest professional and customer-friendly approach to a medical TTP would appear to be one that provides no access to keys which are used for encryption for confidentiality, while the safest political and technical approach would be to build in such facilities and rely on legal and organisational safeguards to control their use.

The legal recognition of digital signature is still under evolution. According to COM(97)503 [19] *"... In order to achieve as wide as possible acceptance of digital signatures Member States should co-ordinate activities to ensure legal recognition of digital signatures at the latest by the year 2000. The Commission will evaluate the necessity to provide for the legal recognition of digital signatures at Community level by harmonising different national regulation"*. Until the harmonisation stage is reached, separate agreements may be needed in order to secure the legal framework for using digital signatures.

4.4 Session example

In order to illustrate the operation of EUROMED-ETS, the following paragraphs contain a session example. Assume that a Physician *P*, using a Client machine *C*, wants to connect to Server *S* of Hospital *H*, to obtain the patient record of the hospital Guest *G*. A TTP provides the Certification Authority *CA* and Directory *D* services. If *P* is not a registered user in the TTP scheme he must register and obtain a certificate from a *CA*. These steps will allow him to be authenticated by the Server *S*, grant him the rights he may have as a Physician and communicate securely with *S*. *S* must be certified by one of the *CA*s too.

It should be noted that once the users obtain the necessary authentication credentials (X.509 v3 certificates), the security layer becomes totally transparent to them. They do not need to implicate into any of the security procedures that take place any time they access locally or remotely the medical data. Figure 2 depicts the communication channels mentioned in the session example.

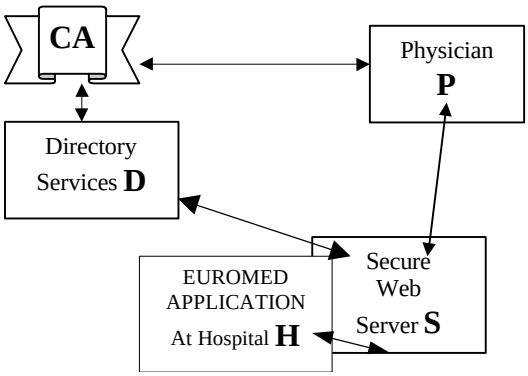

Figure 2: Session example

The technical details of the registration and certification process for *P* at the pilot are as follows:

[1] *P* will point his browser to the *CA* and apply for a certificate (if it the first time *C* is contacting a *CA* to request a certificate, *P* will be prompted by his browser to create his

RSA keypair). *P* will be instructed by the *CA* to provide certain identification information.

[2] The *CA* administrators will forward his request to the *D* administrators; they will verify the identification information *P* has provided the *CA* with.

[3] *P* will be asked by the *D* administrator to provide any needed additional information to prove his identity according to the *CA* policy.

[4] If his identity is confirmed, an entry for him will be created in the Directory and the *CA* administrators will be notified.

[5] The *CA* administrators will issue his certificate and notify *P* to download his certificate from a specific URL.

[6] *P* must download and install automatically the certificate in his browser

P is now ready to commence secure, authenticated communication sessions with Server *S* of Hospital *H* and any other server that performs lookups in the Directory *D* in order to authenticate the users that request access. It should be mentioned that if *S* does not possess a certificate, the system administrators of Hospital *H* must follow the same procedure to register and obtain a certificate for *S*. Assume that *P* attempts access to *S*, in order to obtain the patient record of *G*. The procedure is the following:

[1] *P* points his browser in client machine *C*, to *S*.

[2] *SSL handshake* occurs and secure communication commences between the two parties as soon as *P* enters his secret key password in order to unlock it. The communication is encrypted, using two RC4 keys (the length of the keys has to be decided upon in order to provide strong authentication and to comply with the existing legal and regulatory requirements). One key is used for the encryption of data sent by the Web server and the decryption of data received by the client and the other is used for the encryption of data sent by the client and received by the Web server. The seed for the generation of both keys is randomly generated by the client during the SSL handshake and is securely communicated to the server, using his public RSA key (512 bits).

[3] *S* performs a secure lookup in the *CA Directory*. If *P* is a registered physician and his certificate has not been revoked he will be in the Physicians group, with a valid certificate. The *CA Directory* performs a search and if the requested data do not exist locally, refers the request to the appropriate Directory branch. When that is reached group membership, certificate and other identification data of *P* are returned to *S*.

[4] *S* compares the certificate presented to him by *C* and the certificate contained for *P* in the *CA Directory*. If they match, authentication was successful.

[5] *S* uses the identification data received from the *CA Directory* to perform a lookup in the local Access Control List. According to the local *ACL*, all physicians have the right to obtain patient records, so *S* grants the right to *C* to access the patient record of *G*.

[6] The patient record of *G* is presented to *P*.

The above procedure is completely transparent to *P*. He only knows that he has directed his browser to *S* and requested for the patient record of *G*, which he has finally taken.

5. CONCLUDING REMARKS AND FUTURE WORK

The successful completion of the pilot operation made us aware of a number of problems that should have to be addressed before globally deploying Web-based telemedical applications. The resilience of the Internet leaves currently a lot to be desired. The sensitive nature of medical data and the circumstances under which it will be demanded require a network that can provide guarantees of service level and quality.

Although we implemented an ad-hoc security policy for handling medical data, any real-world wide-scale telemedical application deployment will need an international framework specifying the access rights of all health-care participants to patient data. Given the sensitive nature of the patient data and the widely differing national policies and participant interests and culture, we believe that this problem will need decisive action by governments [19] and the healthcare community in order to be satisfactorily resolved.

During the implementation phase it was discovered that many “Web-development” tools were in fact delivering Java-based applications that used out-of-band socket-based communication mechanisms, thus effectively side-stepping the HTTP-HTML protocols we were attempting to secure. Developers need to take extra care when securing Web-based applications until Internet security is addressed at the transport layer.

The controversial export restrictions, currently affecting the key length supported by many US products, are another well-publicised problem area. In our opinion it will not be too long before mature full encryption strength products are successfully marketed by companies not affected by the US export restrictions. Until that time however, the security of Web-based applications outside the US may be considered questionable and, in any case, context dependent.

A final point, that needs further attention, concerns the scalability of our approach. Due to the novelty of the proposed infrastructure, a wider-scale pilot is needed in order to examine and verify the architecture’s behaviour under a larger number of servers and clients.

Nevertheless, the problems outlined above are mainly implementation dependent that are expected to be addressed as the technologies, the market, and the medical security frameworks mature. They are not meant to underrate the main finding of our research work, which is that secure telemedical applications can be deployed over the Web, based on a trusted third party architecture and using open interoperating technologies.

References

[1] Gritzalis S., Spinellis D., "Addressing Threats and Security Issues in WWW Technology", in *Proc. of the 3rd IFIP International Conference on Communications and Multimedia Security,* pp. 33-46, Chapman & Hall, September 1997.

[2] Meyer K., Schaeffer S., Baker D., "Addressing Threats in WWW Technology", in *Proc. of the 11th IEEE Computer Security Applications Conference*, pp. 123-132, December 1996.

[3] Cameron D., *Security Issues for the Internet and the World Wide Web*, CTR Corp., USA 1997.

[4] Berners-Lee T., Connolly D., Hypertext Markup Language 2.0, *RFC 1866*, Internet Engineering Task Force, 1995.

[5] Garfinkel S., Spafford G., *Web Security and Commerce*, O'Reilly & Associates, June 1997.

[6] Katsikas S., Spinellis D., Iliadis J., Blobel B., "Using TTP's for secure telemedical applications over the Web: The EUROMED-ETS approach", *International Journal of Medical Informatics*, Vol. 49, no. 1, pp. 59-68, March 1998.

[7] Council of Europe, Recommendation R(97)5, *On the Protection of Medical Data*, Council of Europe, February 12, 1997.

[8] *http://home.netscape.com/newsref/std/SSL.html*, April 1997.

[9] Gollmann D., "What do we mean by entity authentication?", in *Proc. of the 1996 IEEE Symposium on Security and Privacy*, pp. 46-54, June 1996.

[10] *"CCITT Recommendations X.500-X.521, Data Communication Networks Directory"*, CCITT, November 1988.

[11] Yeong W., Howes T., Kille S., "Lightweight Directory Access Protocol", Univ. of Michigan, ISODE Consortium, *RFC 1777*, 1995.

[12] Garfinkel S., Spafford G., *Practical Unix and Internet Security*, O'Reilly & Associates, April 1996.

[13] "*CCITT Blue Book, Recommendation X.509 and ISO 9594-8, Information Processing Systems - Open Systems Interconnection - The Directory Authentication Framework*", CCITT, Geneva, March 1988.

[14] T. Howes, S. Kille, W. Yeong, C. Robbins, "The String Representation of Standard Attribute Syntaxes", *RFC 1778*, 1995.

[15] *http://Web.umich.edu/~rsug/ldap/ldap.html*, November 1997.

[16] *http://www.psy.uq.edu.au:8080/~ftp/Crypto*, September 1997.

[17] Council of Europe, *Convention for the Protection of individuals with regard to automatic processing of personal data*, Convention No. 108, January 1981.

[18] Council of Europe, *On the Protection of Medical and Genetic Data*, R(96) Draft Recommendation, June 1996.

[19] European Commission, *"Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption"*, Com from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions, COM (97) 503, October 1997.