Using Trusted Third Parties for Secure Telemedical Applications over the WWW: The EUROMED-ETS approach[*+]

Sokratis K. Katsikas [1] , Diomidis D. Spinellis [1] , John Iliadis [1] and Bernd Blobel [2]

[1] Dept. of Mathematics, University of the Aegean, Karlovassi GR-83200, Greece

[2] Otto-von-Guericke University Magdeburg, Institute of Biometrics and Medical Informatics, Dept. of Medical Informatics, Leipziger str. 44, D-39120 Magdeburg, Germany

Abstract

This paper reports on the results obtained by the pilot operation of Trusted Third Parties (TTP) for secure telemedical applications over the WWW. The work reported on herein was carried out within the context of EUROMED-ETS, a R&D project funded by the INFOSEC office of Directorate General XIII of the European Union. The paper discusses the platform used, the security needs of the specific application, the TTP solution provided, the steps taken in order to implement the solution at a pilot scale and the results of the pilot operation; it is compiled using material included in the project deliverables.

[*] *International Journal of Medical Informatics*, 49(1):59-68, March 1998.

[+] 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.

1. Introduction

EUROMED is a hierarchical telemedicine network that links isolated medical sites with specialised clinics and High-Performance Computing Networking (HPCN) centres across Europe. EUROMED has developed a hierarchical suite of packages for telemedical visualisation, called "Visualisation Suite". EUROMED utilises the Internet and World-Wide Web (WWW) tools, such as Web browsers, 3-Dimensional Visualisation tools and languages (VRML), and interactive navigation tools written in Java, to combine the telemedicine network and the Visualisation Suite in a complementary manner to existing medical facilities.

EUROMED bases communication among participating sites on Internet technologies. A number of sites that participate in EUROMED store medical data about patients, as well as image processing and archive applications. A physician seeking information to reach diagnosis for a given patient, searches the EUROMED Network with a WWW browser and collects the available data for the specific patient.

EUROMED supports three levels of hierarchy: the Hierarchical Computer Network (HCN), which relates to the networking infrastructure, the Hierarchical Computing Facilities Infrastructure (HCFI), which concentrates on powerful computing facilities, and the Hierarchical Medical Facilities Infrastructure (HMFI) which deals with medical applications.

EUROMED-ETS is a project funded by the Commission of the European Communities that started in January 1997 and concentrates on:

- security problems stemming from the electronic transactions between the HMFI and the HCFI over the HCN, using the web as the link technology between these two levels of infrastructure,
- security problems stemming from the electronic transactions between entities of the HMFI level over the HCN, using e-mail to establish communication between the aforementioned entities.

EUROMED is based on a set of Web servers. Each of these servers hosts a number of HTML pages that allow users to access medical data. Access is provided both to static data and to medical applications and visualisation tools; in the latter case, WWW is used as a common framework for the interworking of applications.

It is self-evident that a system, such as EUROMED, with open specifications and a diverse user base (hospital, institutions, etc.), that utilises Internet as its underlying communications facility, is exposed to all security threats present in today's open networks [2]. In particular, by monitoring communication lines, wiretappers may gain unauthorised access to local or remote medical data, thereby violating the patients' 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 the operation of a whole site, that is masquerade a false site as a legitimate one.

EUROMED-ETS deals with the above major threats EUROMED faces, by providing integrity, authentication and confidentiality services using measures such as:

- *digital signatures* to ensure data integrity
- *encryption* to provide confidentiality.

In the context of realisation of the above mentioned services and mechanisms, organisational, medical, social, ethical, and technical aspects are considered by EUROMED-ETS.

This paper reports on the establishment, initialisation, operation and validation of a pilot network of TTPs for the needs of EUROMED. Following the TTP specifications [3], pilot TTP sites were established in four different locations in Europe: Institute of Computer and Communication Systems - ICCS (Athens-Greece), University Hospital Magdeburg - UHM (Magdeburg-

Germany), University of the Aegean - UoA (Samos-Greece), and University of Calabria - UniCAL (Calabria-Italy).

2. Organisational Set-up of TTP sites

2.1 Introduction

This section reports on the organisational measures taken by the UoA pilot site. In particular, the overall roles assumed by the EUROMED pilot team are described and their undertaken responsibilities and rights are specified. Details for the organisational set-up of all other pilot sites are hereby ommitted for the sake of brevity but can be found in [1].

Among the functions performed by the certification authority are: initialisation, electronic registration, authentication, key generation and distribution, key personalisation, certificate generation, certificate directory management, certificate revocation, CRL generation, maintenance, distribution storage and retrieval.

2.2 UoA organisational setup

2.2.1 Organisational Roles

The roles assumed by the UoA pilot team were the following:

- Professionals (practitioners)
- Certificate Authority operators and administrators
- Directory Server administrators
- Secure Information Dissemination
- EUROMED site operators
- Pilot Testers
- Pilot Documentors
- Pilot Help Desk
- Integrated TTP Services

Other EUROMED-ETS partners assumed initially a subset of these roles (e.g. EUROMED site, Professionals), thus helping in the overall testing and control of the pilot outcome.

2.2.2 Certification scheme

In the certification scheme selected at the EUROMED-ETS pilot phase, ICCS was the root Certificate Authority. UoA was the first level subordinate Certificate Authority; almost all the other partners were requesting and receiving certificates (either CA or Server/personal certificates) from the UoA CA.

2.2.3 Directory Setup

Referrals have been used for the interconnection of the Directories setup by the EUROMED-ETS pilot partners. During the pilot phase, the UoA and ICCS had setup and operating Directory Services. Any request to the UoA Directory which could not be served was referred (redirected) to the ICCS Directory and vice-versa. The Directories have served in that way as a repository for identification and authentication information; this information was utilised automatically by the EUROMED-ETS pilot Secure Web Servers to identify potential users and grant or deny to them rights; this identification information was also accessible anonymously through the Internet by the use of LDAP search tools. [4]

The types of rights that have been granted to the UoA EUROMED-ETS pilot team members were the following:

- Certificate server administration
- Certificate issuance
- DIT management right
- Secure Web Server administration

- Secure Web Server content management
- Systems' administration and maintenance
- Auditing

Besides that, non-UoA users could access the UoA TTP site after having requested and received their own personal certificate. This gave them access to the following:

- UoA Secure Web Server
- UoA Directory Server
- UoA Certificate Server

3. Technical Infrastructure

3.1 Introduction

Again, for the sake of brevity, only the UoA infrastructure is described. Details for the infrastructure at other pilot sites can be found in [1].

The hardware used in the EUROMED-ETS pilot phase consisted of a number of Sun and Intel based workstations and servers, operating with the Solaris and Windows NT systems. The pilot was equipped with all the peripherals needed to achieve the maximum compatibility and platform capabilities for supporting the EUROMED-ETS needs. The EUROMED-ETS servers were operating on LANs, directly connected to the Internet through large bandwidth leased lines. However, it should be mentioned that large bandwidth lines is not a necessity for the operability of the EUROMED project.

The software used in the EUROMED-ETS pilot has been carefully selected after an exhaustive research of all Web Security related software. At the time we chose Netscape as a software provider for the Web security products, it was the only integrated available solution. It has to be stated that the Web security domain was (and is) still being developed with new products, implementations and upgrades appearing in the market continuously.

The network structure of all EUROMED-ETS pilot sites was approximately the same; with small variances in bandwidth considered not worthy to be mentioned. Specific references to the proxies used and the required configuration (and therefore to the ones that may be used in EUROMED-ETS) are included in the "Network" section. Besides that, the need for auditing is mentioned as well.

3.2 UoA Infrastructure

The Pilot phase was supported by the Research Lab of the University of the Aegean. The Research Lab is equipped with a multitude of network servers, graphics workstations and PC workstations from a variety of vendors (Sun, SG). The LAN is connected to the Internet through a 2Mbps leased line. A subset of this equipment, as well as the network facilities, were involved in the Pilot setup and operation.

3.2.1 Hardware

The main EUROMED component that is being secured by EUROMED-ETS is the EUROMED-PC software, a low cost implementation of EUROMED for personal computers. The technical characteristics of the EUROMED-PC we used at the UoA were: Intel Pentium 200, 64 MB of RAM, IDE Hard disk 2.1 GB, S3 Trio 64 video card, 3COM Etherlink XL network adapter, 10x CD-ROM

3.2.2 Software

The EUROMED application operating on EUROMED-PC is WebTSN v1.0. This application is tightly incorporated in the Web environment, using Borland Intrabuilder's advanced capabilities.

The database used by the application itself to keep the medical records at a local level is “Local Interbase”.

We have chosen Netscape Enterprise v3.0 as our Web Server. The selection was made between numerous Web Servers. Enterprise v3.0 was the only Web Server, at the time, that offered both advanced Web capabilities, and the SSL3 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 EUROMED-ETS Pilot. It provides LDAP integration; this means that the users and access rights can be stored directly to a LDAP Directory.

Netscape’s Certificate Server v1.01 has been chosen as a CA for the EUROMED-ETS Pilot. It is a solid product; many tests have been run against it already by the Internet community and it seems that he has passed all of them with a remarkable ease. For the record, it can issue certificates for SSL-based authentication, [5] S/MIME, and object signing. It supports many standards that EUROMED-ETS was demanding from a CA, such as X.509v3 [6], SSLv3, PKCS and LDAP. It provides LDAP integration; this means that the certificates and users may be published/stored directly to an LDAP Directory. Moreover, the Web-based certificate management permits to a certificate issuer or a CA administrator to execute jobs remotely.

The *Directory Server* we used is Netscape’s Directory Server v1.02. It supports LDAPv2, as this is described in RFC1777, RFC1778 and RFC1759. Besides these, it supports referrals, as they have been introduced to the LDAP protocol by the University of Michigan. Furthermore, it allows administrators to extend the directory schema (data model) to keep track of new information; also, it allows cross-platform administration from various computers on the network using the point-and-click interface of Netscape; enables bulk administration through import and export of LDAP Interchange Format (LDIF) files. Finally, it creates error, access, and change logs with varying administrator-controllable levels of detail.

The clients we have chosen are Netscape Navigator and Netscape Communicator. It should be mentioned that only the latter is equipped with an extra, independent LDAP search tool which can be used separately from the browser part of the application. Navigator has no such tool at all, but one may use the Web Directory Gateway that Netscape Directory Services 1.02 offer.

3.2.3 Network

A proxy or a firewall, or -what we meet most often- a combination of these two increases by a great degree the security of systems that lie under its “umbrella”. However, in our case, it may prove to be catastrophic. Limiting the use of ports, or certain kinds of incoming/outgoing packets may render one of the Servers/Applications unusable for anyone outside the firewall; that is the whole world. Thus, one should be extremely cautious with the usage of firewalls, if any are used. Ports that may or will be needed for the EUROMED sites to operate smoothly are 80 (default HTTP), 443 (default HTTPS), 389 (LDAP default), 636 (LDAPS default), plus one custom port used for secure communication with the Certificate Server.

One might say that we could as well use ports greater than 1024 for all operations and therefore avoid the most common troubles/conflicts appearing by the usage of Firewalls. This is true and all that is needed to be done is to concatenate the port number to the address of a Server. However this could/would implicate things for users. One of our aims should be simplicity and to provide a user-friendly solution. After all, the end-users of EUROMED will not be experienced computer users. However, we should not sacrifice in any way, the security in order to provide an easy to use and simple product. On top of the public encryption provided, a very strict control can be performed by means of high and low level auditing.

3.2.4 Application Entities

By this term we refer to all server processes that support specific services. The ones installed for the Pilot phase of EUROMED ETS are:

Certificate server

- Key pair generation
- Certificate Request (CSR) submission
- Certificate Request Management
- Key personalisation
- Operator identification
- Certificate Signing/Issuance
- Directory Update
- Certificate Revocation
- CMS Management

Directory Server

- LDAP support
- Directory Lookup
- Directory Updates
- HTTP management interface

Secure HTTP server

- HTTP/SSLv3
- Client authentication
- Access categorisation
- Access rights
- Directory Lookup
- Timestamping
- Application

4. Operation and evaluation report on UoA pilot

4.1 Summary of Test Results

Tests were executed during the course of the Pilot phase and were performed either locally, or between ICCS and UoA.

Detailed results and "log" sections (containing all necessary supporting log, output and sniffer data) were kept.(see [1] for details of the testing procedure and test results).

The log section, although lengthy, is provided both for documentation and for possible communication with tool manufacturers for helping the latter to trace and correct any problems that were definitely identified in their products.

4.2 Personnel, Training and Internal Organisation of the UoA TTP

The UoA EUROMED-ETS pilot team consisted of a small group of persons, each charged with different responsibilities. The task categories were : System Administration, Server Installation and Administration, Audit Control, Pilot Management, Pilot Documentation and Pilot Testing. Each member of the pilot team possessed only the passwords and proper certificates needed to accomplish his own task. Information flow between these tasks (and therefore between the persons in charge of them) was accomplished either through Secure e-mail (S/MIME) or standard Telephony. Information dissemination was accomplished by means of a mailing list.

The team members were keeping a full log (documentation) of their work and remarks on the Pilot; in some cases a daily log was been kept. This documentation was available to any of the UoA Pilot team members, in order to gain knowledge and familiarity with all the aspects of the Pilot. This training procedure has proven to be quite fruitful, since every team member had a general view of the pilot and was able to co-operate in an efficient manner with all the other team members.

The Pilot tests, as defined in the ICCS test cases [3], were conducted mainly by those who were in charge of the UoA Pilot testing. However, most of the team members co-operated in the testing, whenever that was needed, following the directions of the UoA Pilot Tester.

4.3 UoA TTP: Internal Structure and Procedures

The TTP security scheme used by the EUROMED-ETS Security Architecture consists of the following components :

- Directory Services
- Certificate Servers
- Secure Web

State-of-the-art technology has been used in order to secure the medical transactions of EUROMED. Trusted Third Parties were constructed and dispersed geographically to assure that security provisions would be available at any request, anytime. To construct a solid, distributed operation environment Directory Services were implemented, acting as a repository of security information, such as identification and authentication data. These data were utilised for enabling and supporting of secure, encrypted transactions between Secure (SSL) Web Servers, inter-operating with the medical applications and data at a local level, and Web clients.

Certificate Servers were installed at UoA, ICCS. The latter was the Root CA[1]. The UoA CA was installed as a subordinate CA. Web Servers were installed afterwards and certificates were issued for all the installed Servers and for the users that participated in the project; certificates were also issued for some "dummy" users, to be used for test purposes. A series of informal tests have been performed to make sure that certificates could be issued, and that EUROMED-ETS participants (users, servers) could install them and make use of them.

UHM and UniCAL installed (for local test reasons only) Certificate Servers, as subordinate to the UoA CA, and Secure Web Servers. Client certificate were issued by the UoA for both the UHM, UniCAL.

After that, the UoA successfully installed and configured the EUROMED web application (WebTSN) to interoperate with the UoA Web Server. Partners were asked to request client (personal) certificates in order to be able to visit the UoA Web site; this site was created both for the dissemination of information

4.4 Service Initialisation and Adjustments

We have performed an extensive research to find all available ways to store a user's sensitive data (user's key pairs, certificates) in a safe medium; we have gone through several documents and FAQ's, asked directly the Web browsers' companies, posted questions in relative newsgroups. The results we came up with show beyond any doubt that the only browser able to operate fully in a TTP environment and at the same time store the user's sensitive data in a safe medium is Netscape Communicator 4.0 and above.

In Communicator 4.x, every time a new user wants to use the browser, he has to create a personal profile (personal data including name, e-mail address, news server, mail server, future key pairs and certificates etc.). This personal profile is , by default, stored in the local hard disk. However there is the option, during the creation of the profile (a straightforward procedure that any user should be able to perform) to store the latter on any other medium, such as a diskette. We do not recommend that, if the user is going to use newsgroups as well; the diskette does not have enough space to fit all these in. In that case, or in the case the user wants to perform faster access to his/her certificates and key pairs, he may just as well store his personal profile in a Zip or Jazz drive. The sizes of these disks (Zip, Jazz) render them quite portable and, at the same time, they offer high capacities (Zip=100MB, Jazz=1.0GB), along with high speed access!

[1] Certificate Authority

One could divide the *Directory structures* into two kinds : referrals and replication. In referrals, 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. In replication, all Directories 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.

We believe that due to the vast amount of information that will be contained in a real-world EUROMED-ETS Directory, replication would not be the optimal solution. Referrals should be preferred. The optimal solution would be to have a part of the Directory replicated and another part being accessed by referrals. The question that arises is where to draw the line between replication and referrals. One possible solution would be to replicate the country-wide Directory and leave all queries outside each country to be served by the use of referrals. In any case, the Directory structure should be seriously considered only when all the Directory branches that are going to be setup and the equivalent bandwidths become known.

Remote auditing should be considered necessary in our case; we should not exclude the case of a "security hole" in the TTP security system, provoked either by an OS malfunction or by a browsers' or Servers' malfunction. We should use auditing in order to discover as soon as possible this security leak and fix it immediately. However, it may not be possible to have administrators on a 24h basis watching every EUROMED CA, Directory or Web Server, that is why we should take advantage of remote auditing capabilities, either these offered directly from the Servers we used, or the ones we can build. It would be wise to have an administrator checking up on a group of Servers; maybe an administrator controlling all Servers that exist within one country.

Some remote auditing capabilities are directly offered to us through Enterprise 3.x (they have not been tested). We can though construct a "remote auditing system" without difficulty.

Frequent *backups* should be scheduled, covering the certificates databases, the configuration files of the Servers and the medical databases. They should be kept either on a second hard disk (controlled by a separate SCSI controller) or on tape. Especially in the case of Windows NT we would recommend a second hard disk of capacity greater or equal of the first hard disk's, in order to perform Disk Mirroring.

A feature for *retrieving a certificate directly from the Directory* is still not available in Netscape's Directory Server. However, the Application Programming Interfaces (API) that accompanies the Directory provides all the programming capabilities needed to construct any additional components to support that feature too. Until then, a user has to enter the Certificate Server's site in order to install his issued certificate; this is not a difficult task though, even for the end user.

The standard procedure, as defined by Netscape, to issue a certificate is the following :

- The user performs a certificate request (through Certificate Server's interface)
- The Directory/Certificate Server operator verifies the user's identity and his legal right to possess a certificate and performs the following actions :
    - The operator adds this user to the Directory
    - The operator issues a certificate for this user, which is automatically added to the Directory

Tools can be built, using the Application Programming Interfaces that Netscape has given out for the Servers, which automate part of this process. We take for granted naturally that this process should not be fully automated, because a small leak in this automation could cause a major

security leak in our whole system. The identification of the person requesting a certificate and the verification of his legal right to possess one should be conducted by a human being.

The well known export policy of the USA will not change, at least not soon; the result is that some “really strong” encryption tools are out of reach for Europe, at the moment; tools related to this project’s nature, such as Browsers and Servers, supporting 128-bit encryption algorithms. However, there are at least two ways to surpass these problems.

The first includes the combined use of SSLeay, Netscape APIs, HTML and Java in order to incorporate 128-bit encryption to the “low-level encryption” Netscape products use.

The second way of overcoming this problem is to use “security proxies”, such as Stronghold (http://stronghold.ukweb.com). Using such tools one could possibly equip the European versions of the Netscape Servers with 128-bit encryption, without a lot of programming effort.

From all the web browsers we have tested, only Netscape Communicator 4.0 seems to be able to store a person’s certificates directly into a storage medium other than local hard disk. However, you are forced to store all personal data and personal browser configuration into the same medium. Therefore, choosing a floppy disk as the certificate storage medium means that your web bookmarks, your e-mail and a lot of other things, will be store there. That should not constitute a problem but if we take under consideration the slow speed of operation of floppy disks, this choice of storage medium could possibly slow down the whole operation of the user. Concluding, a safe medium should be selected, other than the local hard disk, at all costs, for security reasons; however the floppy disk seems inadequate for the time being. Alternatives to the floppy disk which will do the job are the ZIP drive (portable, 100MB of capacity, high access speed) and the Jazz drive (portable, 1GB of capacity, high access speed). There are of course the Bernoulli drives, but these cannot be considered portable.

5. Conclusions

The EUROMED-ETS pilot phase has been completed and its results are described in summary in this paper. TTP services are established in four different sites. The EUROMED platform, on which the pilot operation took place, and its specifications have been described. The organisational set up, the technical infrastructure, the pilot operation and evaluation have been described in this papere. The TTP functions applied are: certification authority, key generation, naming authority, public key, registration authority.

Each EUROMED site contains a local database with medical data and a set of tools to make these data available via the Internet using secure WWW technologies. Data is protected from unauthorised access. EUROMED TTP sites offer the required functionality for the issuance and maintenance of certificates. A Directory (global, as far as EUROMED-ETS is concerned) is deployed, where information is stored about the TTPs themselves, server certificates and user certificates. The EUROMED-ETS TTP sites maintain distinct parts of this Directory, which replicates across Directory servers for efficiency and redundancy purposes.

SSL is the protocol used in order to establish a secure and authentication session. SSL is embedded in the web tools used. SSL is defined in a draft IETF standard and available publicly over the Internet. SSL is a protocol that sets up a secure session among two endpoints connected via an insecure network. It operates upon the TCP layer of the TCP/IP protocol suite. Most of SSL's operation (capability negotiation, certificate exchange, session key negotiation, session management) is transparent to the application endpoints above SSL.

The proposed solution was characterised by its open architecture and its capability to interoperate with a large number of Web tools. The implementation procedures followed in this pilot phase were not restricted by any products. Although available technology was used, components can be

substituted by others, offering larger key lengths, and any browser supporting SSL with an RC2/128 capability is able to replace the existing ones in the EUROMED sites.

EUROMED user needs were not examined, as EUROMED has not reached a stage mature enough for doing so; thus the user needs determined by other projects [7] were considered.

EUROMED has so far standardised the use of the WWW for telemedical applications. EUROMED -ETS shows that the security problems considered arising from the first and third hierarchical stage can be solved by the use of TTP technology. However, if EUROMED is to operate in a real world scale, a stronger cryptographic engine should be used in order to assure in the best possible way the confidentiality of exchanged information. The latter may be accomplished either by developing modules which will interact with the ones used at the present time, or by replacing the modules which currently perform the cryptographic functions. Only then EUROMED will reach its true potential and all its participants (amongst them 80 Hospitals through out Europe) will start utilising its true benefits.

6. References

[1] *EUROMED-ETS, Deliverable No.3,* Pilot and Validation of Security Measures in EUROMED, Polemi D. (Ed.), INFOSEC Project 20820, CEC, DGXIII B-6, September 1997.

[2] Addressing Threats and Security issues in World Wide Web Technology, Gritzalis S., Spinellis D., in *Proceedings of the CMS '97 3rd IFIP joint working Conference on Communications and Multimedia Security, (S.Katsikas Ed.),* pp.33-46, Chapman & Hall, September 1997.

[3] *EUROMED-ETS, Deliverable No.2,* Trusted Third Parties in EUROMED: The proposed Solution, Polemi D. (Ed.), INFOSEC Project 20820, CEC, DGXIII B-6, May 1997.

[4] Lightweight Directory Access Protocol, Yeong W., Howes T., Kille S., Performance Systems International, University of Michigan, ISODE Consortium, *Request For Comments RFC 1777*.

[5] The SSL protocol ver 3.0, Freier A., Karlton P., Kocher P., Netscape Communications Corporation, at *http://home.netscape.com/eng/ssl3.*

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

[7] *EUROMED-ETS, Deliverable No.1,* Review of Existing Results of TTPs for Health Care Systems, Polemi D. (Ed.), INFOSEC Project 20820, CEC, DGXIII B-6, March 1997.