GEMSS: Privacy and security for a Medical Grid

Jean A.M. Herveg[1], Federico Crazzolara[2], Stuart E. Middleton[3], Darren Marvin[3], Y. Poullet[1]

[1]Centre de Recherches Informatique & Droit, FUNDP, Belgium
[2]C&C Research Laboratories, NEC Europe Ltd., St. Augustin, Germany
[3]IT Innovation Centre, University of Southampton, UK

Contact
Jean A.M. Herveg
Centre de Recherches Informatique & Droit
Faculté de Droit de Namur – FUNDP
5 rempart de la Vierge
B – 5000 NAMUR (BELGIUM)
tel: 00 32 81 72 47 68, fax: 00 32 81 72 52 02, email:jean.herveg@fundp.ac.be

1. Summary

This paper gives a legal qualification to the operations performed upon the patient's data, in view of Directive 95/46, when using the GEMSS medical Grid applications. It identifies measures ensuring the security of the data processing, and describes the legal rationale behind the choice of security technology.
Our legal analysis demonstrates that each GEMSS service provider acts as a processor of the controller of the patient's data processing for healthcare purposes. With respect to this, the controller has to choose a processor providing sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out, and ensure the compliance with those measures. These measures have to ensure a level of security appropriate to the risks represented by the processing and nature of the data, with regard to the state of the art and the cost of their implementation.
Having identified the legal requirements we then describe the security technology employed within the GEMSS Grid middleware. The security technology employed is based on a public key infrastructure (PKI), and implements end-to-end security mechanisms in line with the web services security (WS Security, WS Trust and SecureConversation) specifications. The GEMSS middleware ensures a degree of protection of patient data that is appropriate for the health care sector and is in line with the European Directives. We hope that GEMSS will become synonymous for high security data processing and give further guarantees to controllers that GEMSS providers are sufficiently secure.

2. Keywords

Grid, Legal, Medical, Personal Data, Security

3. Introduction

The use of GRID technology in the healthcare sector raises significant legal and security issues. The goal of the GEMSS project (Grid-enabled Medical Simulation Services) [12] is to develop six testbeds for medical imaging applications. In this context, the project examines explicitly both the legal and technical framework in which such Grid tools could be exploited. The legal study aims to analyse the pertinent European regulations considering the specific characteristics of the GEMSS applications. This analysis allows us to draw the common legal framework in which these applications might be developed. Moreover, this approach allows us to show which aspects are not covered by European Law, and where disharmony between the national legislations might exist.

Considering the normative plurality characterizing the European legal system, the results of the legal analysis of a defined situation depend logically on the viewpoint adopted. Three approaches have been selected in the GEMSS project, which are considered to be the most relevant:

- Protection of the patient's privacy; more specifically the processing of the patient's personal data (the two concepts do not share exactly the same meaning).
- Contractual aspects.
- Responsibilities and liabilities concerning the use of the GEMSS applications.

The technical analysis studies and tests the required measures to ensure the security of the applications as required by the European Directives. We use the legal analysis to generate security requirements, and hence guide our choice of security technology. The security technology employed in GEMSS is based on a public key infrastructure (PKI), and implements end-to-end security mechanisms in line with the web services security (WS Security, WS Trust and SecureConversation) specifications. The GEMSS Grid is based on middleware that is specifically being developed to provide the necessary security for a lawful personal data processing.

This paper will first describe the legal qualification of the operations performed upon the patient's personal data when using the GEMSS applications, in view of Directive 95/46 [1], and then identify the technical measures used to ensure the confidentiality of the patient's processed data. We conclude with a short discussion of the progress so far, and shed some light on our ambitions for this work both within the GEMSS project and during the exploitation phase after the project completes.

4. *RATIONE MATERIAE* APPLICATION OF DIRECTIVE 95/46 TO GRID-ENABLED MEDICAL SIMULATION SERVICES

According to its article 3.1, Directive 95/46 applies to wholly or partly automated processing of personal data and to other processing of personal data which form part of a filing system or are intended to form part of a filing [2].

The use of the GEMSS applications starts with the collection of the patient's data in view of generating the needed medical images (e.g. by way of a scanner). The medical practitioner is in charge of this collection. He sends the data through the Internet to the GEMSS provider. This last one might be chosen via a special electronic register. The GEMSS provider participates in the generation of the medical image by using software and computational resources both in his possession. In some circumstances, another provider might allow the use of software needed to generate the medical image.

Directive 95/46 represents consecutively a pertinent European regulation to study. Indeed, the collected patient's data, sent through the Internet and processed by the GEMSS provider, are personal data as they are related to a well-identified natural person. If the data sent through the Internet is not directly nominative, it is nevertheless related to an identifiable natural person, by mean of any code in order to permit their imputation to an identified patient.

Besides the collection of the patient's personal data, its transmission through the Internet and its processing by the GEMSS provider constitute sets of operations performed upon personal data by automated means.

However, these sets of operations are only one part of all the sets of operations performed upon the patient's data to support the healthcare provided to him by his medical practitioner. All the sets of operations performed upon the patient's personal data are integral parts of the same and unique data processing defined by its therapeutic purpose, and to which they are linked.

This implies that the use of the GEMSS applications does not create a new processing of personal data. Their use is only a new part of a pre-existing processing of personal data for therapeutic purpose or for scientific research. If necessary, the controller of the personal data processing will have to adapt his procedures to the use of such new tools, according to the applicable national rules transposing Directive 95/46.

5. PARTLY SUB-PROCESSING OF THE PATIENT'S DATA BY THE GEMSS PROVIDER

When processing personal data on behalf of the controller, the GEMSS provider acts as a processor defined in article 2, e, of Directive 95/46. Providing software to help the imaging processing does not constitute in itself an operation performed upon personal data.
Using the GEMSS applications, the controller has to choose a processor providing sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out, and must ensure compliance with those measures, according to article 17, § 2, of Directive 95/46.
Carrying out the processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instruction from the controller and that the appropriate technical and organizational measures, as defined by the law of the Member State in which the processor is established, shall also incumbent on the processor, according to article 17, § 3, of Directive 95/46.
For the purpose of keeping proof, the parts of the contract or the legal act relating to the data protection and the requirements relating to these measures, shall be in written form or in another equivalent form, according to article 17, § 4, of Directive 95/46.

6. TECHNICAL REQUIREMENTS DERIVING FROM DIRECTIVE 95/46

The measures used by the GEMSS provider have to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular when the processing involves the transmission of data over a network, and against all other unlawful forms of processing. With regard to the state of the art and the cost of their implementation, such measures have to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected [3]. Consequently, the more sensitive the data is the more risky the processing will be. As personal data related to health are very sensitive, the security level of the data processing has to be at maximum.
For examples of security measures, it is useful to refer to the measures recommended e.g. by Rec. 1997(5) of 13 Feb. 1997 of the Council of Europe on the protection of medical data, article 9 [4].

7. SECURITY IN THE GEMSS HEALTHGRID

The GEMSS Grid operates with middleware capable of providing a high degree of security for the processing of personal data. The security mechanisms of the GEMSS Grid ensure confidentiality and integrity of personal data as well as identification, authentication, and authorization of data processors. Table 1 shows how the technical requirements of the previous section relate to the security technology.
The Security Infrastructure of the GEMSS Grid (Figure 1) is based on a Public Key Infrastructure (PKI), which follows the guidelines defined in the X.509 Internet Drafts and standards [5], [6], [7]. The GEMSS PKI, as defined by the GEMSS Certificate Policy [8], foresees the three typical roles of Certification Authority, Registration Authority and Relying Party and clearly defines procedures for requesting, issuing, revoking and distributing GEMSS certificates. All GEMSS Certificates are in the X.509 Certificate format [9] and are used by people or machines for authentication, identification and authorization purposes on the GEMSS Grid. The Certificate Policy and the Certification Practice Statement of the GEMSS CA ensure that the GEMSS Certificates issued to people are in line with Directive 1999/93EC of the European Parliament and the Council, on a Community framework for electronic signatures [10].
There are two layers of security for the communication over the GEMSS Grid. Using GEMSS Certificates, communication points are authenticated via the HTTPS protocol. Confidentiality and integrity of the transmitted personal data are also ensured between physical communication points using the HTTPS protocol. The topology of the GEMSS Grid includes distributed services and clients protected by firewalls. They belong to different trust domains and their communication may go through intermediaries lying in demilitarized zones (DMZs)

which forward relevant messages to more protected network domains. The transport-level security mechanisms do not protect against misbehaving intermediaries, which could capture transmitted personal data or even masquerade as false data processors. The threat is real – DMZs are usually and necessarily more open to hacker or unauthorized staff intrusion as one would like.
The GEMSS middleware is Web-Service oriented with end-to-end security mechanisms implemented which are primarily those defined by the Web-Service Security Specifications [11]. Messages that contain personal data are first processed according to a security policy before they are handed over to the transport layer taking care of the communication, using the HTTPS protocol. In turn, when a message arrives, the transport layer hands the message over to a security module, which performs the necessary signature verifications and decryptions. These security modules sit at the communication end-points of GEMSS Services and Clients. The GEMSS Security Infrastructure provides not only for end-to-end message security (message authentication and integrity) but also for secure end-to-end channels. Security Token Providers are activated to provide GEMSS Services and Clients, through Security Token Services, with those security tokens required by the security policy in force.
The GEMSS certificates are used not only for the security of the communication from one end to the other but also for the authorized access to selected GEMSS Services and Resources. The Access rights associated with a certificate are assigned or negotiated before hand by a business process and enforced through the GEMSS Authorisation component. Although the risk of intrusions and attacks to the GEMSS Grid is minimised by GEMSS middleware state of the art security mechanisms, it can never be completely excluded. The GEMSS Security Infrastructure includes an Intrusion Detection System capable of detecting intrusions and attacks. The logs produced by the system might be used as a forensic evidence for legal actions against intruders.

8. Conclusions

The GEMSS provider acts as a processor of the controller of the patient's data processing for healthcare purpose. With respect to this, the controller has to choose a processor providing sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out, and must ensure the compliance with those measures. These measures have to ensure a level of security appropriate to the risks represented by the processing and the nature of the data, with regard to the state of the art and the cost of their implementation. Considering the very sensitive nature of the personal data related to health, the level of security has to be at maximum.
Several levels of protection are implemented which rely on a robust and standardized public-key infrastructure. They ensure confidentiality and integrity of personal data as well as authentication of personal data processors. If such protection was broken, an additional logging and intrusion detection system provides security in depth. We hope that GEMSS will become synonymous with high-security personal data processing for the healthcare sector.
The immediate next steps for us in GEMSS is to finish reviewing EU contractual law and perform a review of commercially available off the shelf security tools. Towards the end of the project we will be looking at HealthGrid liabilities issues and the security and legal needs during any exploitation phase after the project.

9. Acknowledgement

This work was supported by the EC under Research Contract IST-2001-37153 GEMSS (GRID-enabled Medical Simulation Services)

10. References

1. D. 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. O.J. 23/11/1995:L 281,0031-0050.

2. Herveg J, Poullet Y. Directive 95/46 and the use of GRID technologies in the healthcare sector : selected legal issues. Proceedings of the 1st European HealthGRID Conference, Lyon, 16th & 17th Jan. 2003 : 229-236.
3. Article 17, § 1, of Directive 95/46.
4. Cf. also: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm.
5. Information technology – Open Systems Interconnection – The Directory: Authentication Framework. ITU-T Recommendation X.509, ISO/IEC 9594-8. March 2000.
6. Arsenault A, Turner S. Internet X.509 Public Key Infrastructure: Roadmap. Internet Draft, PKIX Working Group, July 2002.
7. Chokhani S, Ford W, Sabett R, Merrill C, Wu S. Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. Internet Draft, PKIX Working Group, April 2003.
8. Crazzolara F. GEMSS Certificate Policy, v 1.0. September 2003.
9. Information technology – Open Systems Interconnection – The Directory: Authentication Framework. ITU-T Recommendation X.509, ISO/IEC 9594-8. March 2000.
10. D. 1999/93 on a Community Framework for Electronic Signatures. O.J. 19/01/2000 : L013, 0012-0020.
11. Security in a Web Services World: A Proposed Architecture and Roadmap. IBM Corporation and Microsoft Corporation – joint security whitepaper, Version 1.0, April 2002.
12. GEMSS public home page: http://www.ccrl-nece.de/gemss/

11. Figures

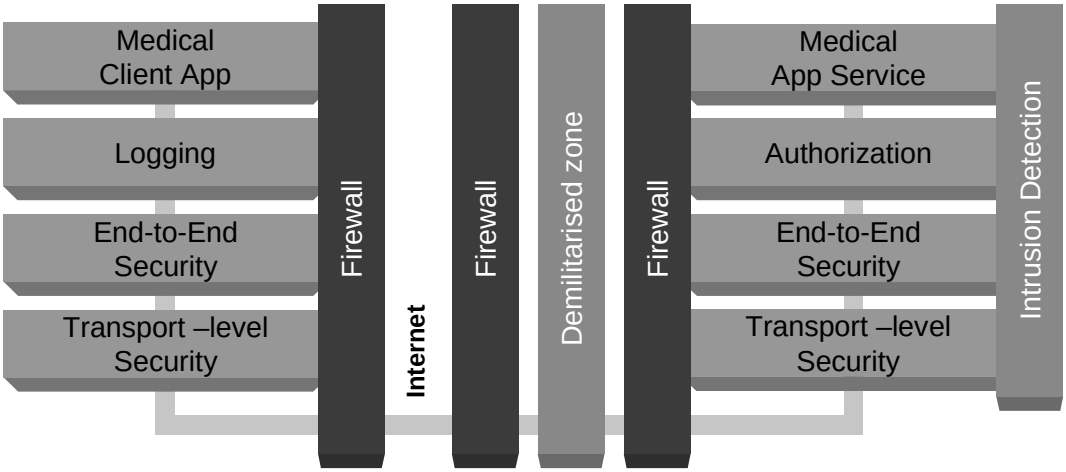

Figure 1 : Overview of the GEMSS Security Infrastructure

12. Tables

Technical requirement	*Security solution*
Protection of data in transit	PKI, X.509 compliance, WS Security, HTTPS
Accidental and unlawful loss of data	PKI, certificate access rights
Unauthorized access to data	Firewalls, access control
Unlawful processing of data	PKI, WS Security, Intrusion detection, logging

Table 1 : Technical requirements and security solutions used in GEMSS

13. Summary

This paper gives a legal qualification to the operations performed upon the patient's data, in view of Directive 95/46, when using the GEMSS medical Grid applications. It identifies measures ensuring the security of the data processing, and describes the legal rationale behind the choice of security technology.

Our legal analysis demonstrates that each GEMSS service provider acts as a processor of the controller of the patient's data processing for healthcare purposes. With respect to this, the controller has to choose a processor providing sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out, and ensure the compliance with those measures. These measures have to ensure a level of security appropriate to the risks represented by the processing and nature of the data, with regard to the state of the art and the cost of their implementation.

Having identified the legal requirements we then describe the security technology employed within the GEMSS Grid middleware. The security technology employed is based on a public key infrastructure (PKI), and implements end-to-end security mechanisms in line with the web services security (WS Security, WS Trust and SecureConversation) specifications. The GEMSS middleware ensures a degree of protection of patient data that is appropriate for the health care sector and is in line with the European Directives. We hope that GEMSS will become synonymous for high security data processing and give further guarantees to controllers that GEMSS providers are sufficiently secure.

14. Keywords

Grid, Legal, Medical, Personal Data, Security