Data Privacy considerations in Intensive Care Grids

Jesus Luna [a,1], Marios D. Dikaiakos [a], Theodoros Kyprianou [b], Angelos Bilas [c,2]
Manolis Marazakis [c]

[a] *Department of Computer Science, University of Cyprus, 1678 Nicosia, Cyprus*
[b] *Intensive Care Unit, Nicosia General Hospital, Nicosia, Cyprus*
[c] *Institute of Computer Science, Foundation for Research and Technology - Hellas (FORTH), PO Box 1385. GR-71110. Heraklion, Greece*

Abstract. Novel eHealth systems are being designed to provide a citizen-centered health system, however the even demanding need for computing and data resources has required the adoption of Grid technologies. In most of the cases, this novel *Health Grid* requires not only conveying patient's personal data through public networks, but also storing it into shared resources out of the hospital premises. These features introduce new security concerns, in particular related with *privacy*. In this paper we survey current legal and technological approaches that have been taken to protect a patient's personal data into eHealth systems, with a particular focus in Intensive Care Grids. However, thanks to a security analysis applied over the Intensive Care Grid system (ICGrid) we show that these security mechanisms are not enough to provide a comprehensive solution, mainly because the data-at-rest is still vulnerable to attacks coming from *untrusted* Storage Elements where an attacker may directly access them. To cope with these issues, we propose a new privacy-oriented protocol which uses a combination of encryption and fragmentation to improve data's assurance while keeping compatibility with current legislations and Health Grid security mechanisms.

Keywords. eHealth security, encryption, fragmentation, Intensive Care Grid, privacy

1. Introduction

The term eHealth describes the application of information technology (IT) and communications technologies across the whole range of functions that affect the health sector, from the doctor to the patients. Current eHealth efforts promise substantial productivity gains to "traditional" health systems thanks to economical savings, processes re-engineering, and other related measures with one clear objective: provide a citizen-centered health system. Nowadays eHealth systems demand more computing and storage capabilities, therefore requiring the adoption of new technologies like the Grid, this gave birth to a new term: the *Health Grid*. Unfortunately , these technologies entail great

[1] This work was carried out for the CoreGRID IST project n^{o}004265, funded by the European Commission.
[2] A. Bilas is also with the Dept. of Computer Science, University of Crete, P.O. Box 2208, Heraklion, GR 71409, Greece.

risks as well: When traditionally *isolated* health system share resources through to public networks (i.e. Internet) they become prey of a wide range of attackers.

So, what if a successful attack discloses the patient's personal data stored in the Health Grid? Unfortunately in this case the *patient's privacy is compromised*, but the potential effects extend far beyond the IT world! Privacy is an important component to building trust between health services and users. If a patient does not trust anymore eHealth systems, then he may even avoid care altogether, which might ultimately result in life-treating situations. This latter fact is what makes eHealth security so important and different from other scenarios.

Our belief is that a comprehensive privacy mechanism for the Health Grid must harmonize legal and technological solutions. To provide this kind of solutions it is necessary to consider privacy from a *layered* point of view: legal issues are the common base above which state-of-the-art security technologies are deployed. Unfortunately current technological solutions are not providing such a comprehensive privacy solution and several security gaps at the storage level are still open. The first part of the research in this paper presents the result of applying a security analysis methodology over an Intensive Care Grid scenario (the ICGrid system [10]); this shows that the greatest threat to patient's privacy comes from the Data Grid's Storage Elements, which are untrusted and may easily leak personal data. In an effort to cover these privacy gaps, the second part of our research contributes with a *low-level* protocol for providing privacy to current Intensive Care Grid systems from a data-centric point of view, but taking into account the legal framework and keeping compliance with *high-level* mechanisms. The contributed protocol proposes the use of two basic mechanisms to enhance a patient's data assurance: cryptography and fragmentation.

The rest of this paper is organized as follows: section 2 presents an overview of the legal framework around eHealth privacy, with a special focus on Member States' legislations; afterwards section 3 performs a comprehensive security analysis of a typical Intensive Care Grid system -the ICGrid- by considering current security mechanisms. With the vulnerabilities found thanks to the previous analysis, section 4 gives a high-level description of a protocol being proposed by our research groups to provide privacy to the data at rest. Section 5 reviews the state of the art and finally, section 6 presents our conclusions and future work.

2. eHealth Privacy: a legal point of view

A major concern in eHealth is adequate confidentiality of the individual records being managed electronically. The core component of many eHealth systems is the Electronic Health Record (EHR), which is basically the patient's health record in digital format. Nowadays EHR protection is the focus of privacy legislations around the globe. In the European Union, several Directives of the European Parliament and of the Council protect the processing and free movement of the EHR, however the common factor is the EU Directive on Data Protection [17] which provides the general framework for the protection of privacy with respect to the processing of personal data in its widest sense. In that context it goes further than the protection of the intimacy of the natural persons i.e. generally speaking their private life, because the definition of *personal data* covers all data related to a natural person, whether the context of such information is the private,

public, or professional life of the individual. However, the European Working Party on Data Protection, established under article 29 of the Directive [17] and composed of the national data protection authority of each Member State, has recently acknowledged that some special rules may need to be adopted for key eHealth applications.

A common term referenced in current eHealth legislations is the concept of *consent*. Such consent is defined as any unambiguous, freely given, specific and informed indication of the patients wishes by which he agrees to the processing of his personal data. In other words, *a patient's consent enables the legal processing of his/her EHR*. However, what happens if, for instance after an accident the patient is unable to give his consent for accessing his personal data at the Intensive Care Unit? Most of the legal issues and ambiguities related with eHealth regulations are being carefully studied; in the particular case of the European Union, the European Health Management Association (EHMA) along with the Commission established the "Legally eHealth" [7] project to study these. About the patient's data protection this study gives three basic recommendations which, using the terminology from RFC 2196 (see [9], section 4), may be mapped as *security services* just as shown in table 1. The next section presents the security analysis of an eHealth scenario as a way to identify not only its strengths, but in particular its vulnerabilities, according to the requirements stated in table 1. With this information, and towards implementing a comprehensive and harmonized solution, we will introduce in the rest of this paper a novel low-level privacy protocol for eHealth.

Table 1. Security requirements for implementing Data Protection Legislations in eHealth environments

Legal Issue	**Security Requirement**	**Example**
Patient's Consent	Authentication, Non-repudiation, Integrity	A patient must be confidently identified (authentication) before signing an agreement (non-repudiation) allowing processing his EHR. The signed document should not be modified afterwards (integrity) without notifying the patient.
Specified Purpose	Authorization, Confidentiality, Integrity	If a patient has given his consent to re-use parts of his demographic data (i.e. only age and sex) for statistical purposes, then a pharmaceutical company should have not access to this information (authorization) and even the personnel authorized to process these statistics should not be able to disclose i.e. the patient's name (confidentiality) or modify the record at all (integrity).

3. Use Case: security analysis of ICGrid

From the point of view of a typical eHealth system, its subsystems may be attacked in several ways, however, for the purposes of our research on data privacy the framework proposed by [19] and extended in [14] will be used to find out the main concerns linked with the security of its data and metadata. In a nutshell, the use of this framework consists of determining the basic components related with the system's security (players, attacks, security primitives, granularity of protection, and user inconvenience), so after-

wards they can be summarized to clearly represent its security requirements. As a proof of concept the security analysis will be performed in the *Intensive Care Grid* system (ICGrid) (section 3.1), considering also the underlying Grid Security Infrastructure (section 3.2) and the Electronic Health Card (section 3.3) currently being deployed across Member States. It is worth mentioning that the security mechanisms being considered and the vulnerabilities to be found, can be easily extrapolated to other eHealth scenarios because the framework is general enough for these environments (just as shown in [14] and [13]).

3.1. ICGrid: data and metadata architecture

An Intensive Care Unit (ICU) is the only environment in clinical medicine where all patients are monitored closely and in detail for extended periods of time, using different types of *Medical Monitoring Devices (MMD)*. Taking clinical decisions for the ICU patients based on monitoring can be a very demanding and complex task requiring thorough analysis of the clinical data provided: *even the most skilled physicians are often overwhelmed by huge volumes of data, a case that may lead to errors, or may cause some form of life threatening situation* [8]. Because Grids represented a promising venue for addressing the challenges just described , the ICGrid system [10] was proposed and prototyped over the EGEE infrastructure (Enabling Grids for E-sciencE [1]). Figure 1, illustrates the architecture of the envisioned ICGrid infrastructure, which comprises a number of different sites that are geographically distributed, belong to different organizations, and are connected through the Internet. The *ICGrid framework* is based on a hybrid architecture that combines a heterogeneous set of monitors that sense the inpatients and three Grid-enabled software tools that support the storage, processing and information sharing tasks. The diagram of Figure 1 depicts the acquisition and annotation of parameters of an inpatient at an ICU Site (bottom left) and the transfer of data replicas to two ICGrid Storage Sites. The transfer comprises of the actual sensor data, denoted as *Data*, and the information which is provided by physicians during the annotation phase, denoted as *Metadata*. Note that the *Data* is a selected subset of the acquired signals, those with the highest clinical interest. In particular, the physician that observes the inpatient annotates these signals with metadata in an offline phase. What is considered an interesting incident depends on the subjective opinion of the physician on duty. Consequently, we utilize the notion of a *Clinically Interesting Episode (CIE)* to refer to the captured sensor data along with the metadata that is added by the physician to annotate all the events of interest. Metadata consists of information about the institution, physician, sensors, patient, intervals of the signals, along with some annotation of the signals. The only information that is collected for the inpatient is height, weight, age, and sex. The metadata is encoded as an XML-document defined by an application-tailored schema. On the other hand, the collected data consists of a set of tab-separated text files, one for each sensor. Each line in these files contains a timestamp, the recorded physical parameter and the state of parameter at the given time-stamp (e.g., if the parameter indicates some alert). All the files that belong to an episode are archived together to form the *Data* archive. These two files (Data and Metadata) must be transferred to a storage unit that can be accessed by all the authorized and authenticated parties that will be entities of the ICGrid-VO. Thus, the services must satisfy certain security properties, something that is already inherent to the underlying Grid Security Infrastructure (GSI) just as presented next.

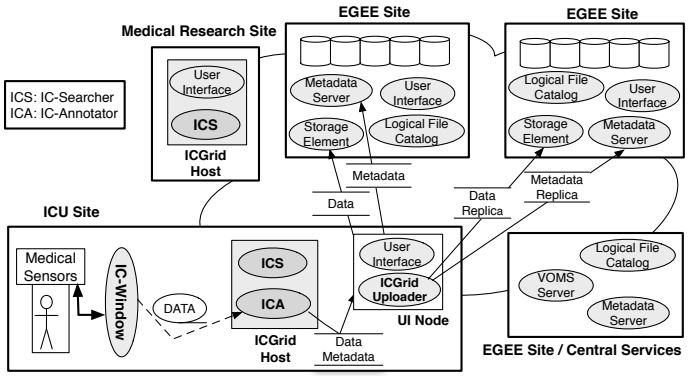

Figure 1. ICGrid System Architecture. White rectangles represent different sites of the infrastructure (each site represents resources of one administrative domain/institution), shaded rectangles represent computer nodes, and shaded ovals depict required Grid services and tools of the ICGrid framework.

3.2. Grid Security Infrastructure

The Grid Security Infrastructure (GSI) [23] is comprised of a set of protocols, libraries, and tools that allow users and applications to securely access Grid resources via well defined Authentication and Authorization mechanisms. In the first case, the Grid client simply uses an X.509 end entity certificate to secure messages and authenticate itself to the Grid service. On the other hand, for Authorization purposes GSI can use an XML-based protocol known as SAML [11], which may retrieve security assertions from third-party services to enable features like role-based authorization. One of these third-party Grid authorization services, widely used in EGEE, is the *Virtual Organization Membership Service* (VOMS) [4]: an Attribute Authority that exposes attributes and encodes the position of the holder inside the VO. Despite its functionalities, nowadays Grid Authentication and Authorization systems are unable to enforce access control close to the Storage Elements and the data itself, in other words, an attacker passing over these security mechanisms (i.e. using a local account with administrative privileges or accessing physically the disks) will have full control over the stored data. These vulnerabilities will be analyzed in section 3.4.

3.3. Electronic Health Card

Member States have begun testing a new health card, known as the Electronic Health Card [16], that contains basic patient data such as name, age and insurance details, as well as electronic prescriptions. It also includes other physical features to identify the owner, i.e. a photograph and human-readable information. With time it will replace EU's existing health insurance cards. Basically this card is a smartcard that stores information in a microchip supporting authentication, authorization and even digital signatures creation. Data protection issues were critical in the design of Electronic Health Cards, so patients must be able to rely on maximum security and confidentiality while operating smoothly in practice. A comprehensive security concept secures the protection of particularly sensitive data, so with few exceptions, the health card can only be used in conjunc-

tion with an *Electronic Health Professional Card*, which carries a "qualified electronic signature (one that meets strict statutory criteria for electronic signatures). In general, Electronic Health Cards represent a big step towards creating a citizen-centered health system, but despite its security advantages, internal storage space is quite limited (just few kilobytes) therefore relying on external storage services over which the card can not offer protection mechanisms. The next section will analyze in detail these security gaps.

3.4. Identifying the Elements for the Security Analysis

As mentioned at the beginning of this section, the first step in our analysis is to identify the elements that play a security-related role into ICGrid:

1. *Players:* four data readers/writers are involved *(i)* the ICU and Medical Research sites that produce and consume the data; *(ii)* the EGEE Central Services that perform VO authentication and authorization as mentioned in section 3.2; *(iii)* the EGEE *storage facilities* for data and metadata; and finally *(iv)* the "wire" or WAN links (public and private) conveying information between the other players.
2. *Attacks:* the generic attacks that may be executed over ICGrid are related with *(i)* Adversaries on the wire; *(ii)* Adversaries on the Central Services; *(iii)* Revoked users on the Central Services; and *(iv)* Adversaries with *full control* of the EGEE storage facilities. Each one of these attacks may result in data being leaked, changed or even destroyed.
3. *User inconvenience:* It is critical for IGGrid operation to have minimum latencies when reading and retrieving the stored data and metadata from the EGEE Site. Since smartcards like the Electronic Health Card are beginning to be introduced into National Health Systems, it is feasible to consider that involved entities (i.e. patients and doctors) will require them for performing operations into our eHealth scenario.
4. *Security Primitives:* two security operations take place into the ICGrid: *(i) Authentication and Authorization* via mechanisms like the ones described in section 3.2) and, *(ii) Consent* of the patient or authorized party if the patient is unable to do it.
5. *Trust Assumptions:* we have considered that in general *(i)* the security tokens used for authentication and consent (i.e. Electronic Health Cards) are personal, intransferable and tamper-resistant; *(ii)* EGEE Sites and/or ICU premises have full control over the data and metadata stored on them; *(iii)* data are encrypted on the public link thanks to secure functionalities (i.e. via SSL); and *(iv)* the EGEE Central Services are managed in a secure manner, therefore providing high assurance to its operations.

3.5. Results of the analysis

Based on the elements identified in the previous section, table 2 summarizes the vulnerabilities identified into the ICGrid system. Results are categorized by possible attacks (main columns) and types of damage – the Leak, Change, Destroy sub-columns –. Cells marked with a "Y" mean that the system (row) is vulnerable to the type of damage caused by this particular attack. Cells marked with a "N" mean that the attacks are not feasible or may not cause a critical damage. If a particular attack does not apply at all, then the cell is marked with a "-".

Table 2. Summary of security issues related with ICGrid

Attack	*Adversary on the wire*			*Adversary w/Central Service*			*Rev. user w/Central Service*			*Adversary w/Storage Site*		
Damage	L	C	D	L	C	D	L	C	D	L	C	D
ICGrid	N	N	Y	N	N	N	Y	Y	Y	Y	Y	Y

From table 2 we can draw interesting conclusion about the overall ICGrid security. First, all the data and metadata being exchanged on the wire is protected (integrity, confidentially) via secure channels (i.e. SSL); however, nothing will stop an attacker from destroying the data by physically damaging the communication channel. It is worth noting that this attack is costly (from the attackers point of view) and nowadays network redundancy provides an excellent solution. On the other hand, according to our experience with the Grid community, the attacks related with Central Services are quite difficult to achieve in practice because most of them are Certification Authorities and authorization servers implementing security policies (both physical and logical), that greatly enhance their assurance.

Also the analysis shows that internal attackers trying to acquire a patient's data using revoked credentials (i.e. former employees) will be able to do so. However, from previous research (i.e. [15]) we can extrapolate well-known real-time security mechanisms to protect the system. Therefore this attacks will not be considered during the rest of this paper. Finally, a critical group of vulnerabilities (last attack column in table 2) are related with compromised EGEE Sites and data at-rest, where an internal attacker (maybe an employee that is collaborating with the attacker) could be able to steal the stored data *directly from the Storage Elements*. This represents a high privacy risk to stored data in an eHealth system. In the next section we examine the associated security tradeoffs in a protocol design for addressing these privacy concerns.

4. Data Privacy Protocol: an overview

From the security analysis presented in section 3 we concluded that despite current security mechanisms, i.e. Grid authorization (section 3.2) and Electronic Health Cards (section 3.3), privacy for data-at-rest has not been achieved for Intensive Care Grids. Therefore the need for "low-level mechanisms" able to protect data and metadata from attacks related with compromised Storage Elements. Towards this goal we have designed a privacy protocol which basic mechanisms are fragmentation and encryption.

In a fragmentation scheme [18], a file f is split into n fragments, all of these are signed and distributed to n remote servers, one fragment per server. The user then can reconstruct f by accessing m fragments ($m \leq n$) arbitrarily chosen. For the proposed protocol, *fragmentation will take place at the Storage Broker* (i.e. EGEE Store Resource Manager [21]).

Use of encryption in conjunction with fragmentation allows for high data assurance, thanks to the protection provided to the data at-rest. For our protocol we decided to use a

symmetric cryptosystem (to benefit performance), with a key build from the combination of the data's cryptographic hash and a fresh-nonce (therefore providing integrity and protection versus replay attacks). As an optional feature a public key cryptosystem may use the patient's X.509 digital certificate and private key from the Electronic Health Card with two purposes, *(i)* digitally sign the data to store (a "low-level" consent mechanism) and, *(ii)* allow the Storage Broker to enforce data access by encrypting the symmetric key with the patient's public key.

An important design decision with the proposed encryption mechanism refers to the entity that should implement it. In general we can say that encryption at the Storage Broker is a promising solution if issues related with symmetric key protection, high availability and performance can be solved. There are however important performance gains that could be achieved if the *untrusted* Storage Elements participate in the whole encryption scheme, but which considerations must be taken to secure such measure? Section 6 will introduce the proposed security protocol considering two variants: *(i)* encryption/fragmentation at Storage Broker and *(ii)* fragmentation at Storage Broker and encryption at Storage Element.

5. State of the Art

As mentioned in section 3, nowadays most of the work related with Health Grids' security and privacy focuses on "high-level" authentication and authorization mechanisms that rely on Grid-IDs and VOMS-like infrastructures [4], therefore leaving data vulnerable into the untrusted Storage Elements just as shown with our previous analysis 3.5. An example of these kind of mechanisms can be seen into the BRIDGES [20]and SHARE [5] Health Grids. However, as far as we know the *Hydra* system [3] implemented for the EGEE's Biomed/Medical Data Management user group, is the only proposal to build an eHealth Data Grid with a security mechanism able to protect patient's data at rest. Hydra encrypts the files and stores them on normal storage elements, however for availability the encryption key is fragmented and stored in the service called the "Hydra Keystore". Contrary to our proposal, in Hydra the data itself is not fragmented, therefore it can be compromised if the encryption key is leaked at the clients. On the other hand, Hydra looks like a promising base for implementing the additional privacy features proposed in this paper.

Despite other state of the art distributed storage systems have not been specifically designed for the Health Grid, they are worth to mention due to its security features and potential use in these environments. The rest of this section will review four of these systems closely related to our proposal. In first place let us mention POTSHARDS [22], which implements an storage system for long-time archiving that does not use encryption, but a mechanism called "probably secure secret splitting" that fragments the file to store prior to distributing it across separately-managed archives. A similar approach is given by Cleversafe [2], which implements also an Information Dispersal Algorithm (based on the Reed-Solomon algorithm) for its open-source *Dispersed Storage Project*. Despite this system does not use encryption at all, the authors provide a flexible API that we may extend in a near future -for the purposes of this research- with the proposed cryptography mechanism. In general both, POTSHARDS and Cleversafe, are interesting to cope with the management problems posed by cryptosystems and long-living data,

however the security achieved only by fragmenting the files could not be enough for some highly-sensitive environments. On the other hand it is worth to mention the Farsite system [6], which provides security and high availability by storing encrypted replicas of each file on multiple machines. However the use of replication instead of fragmentation reduces data assurance (the attacker just needs to compromise one node to retrieve a full file) and may not be bandwidth-wise for big files. Similar to our proposal is also OceanStore [12], where stored data are protected with redundancy (also using erasure codes) and cryptographic mechanisms. An interesting feature in OceanStore is the ability to perform server-side operations directly on the encrypted data, this increases system's performance without sacrificing security.

6. Conclusions and Future Work

The computing and storage potential of the Grid have been foreseen as a suitable solution for implementing eHealth systems able to store and manage data particularly related with Intensive Care Units. One of the most important aspects in eHealth security is privacy, because patient's trust rest on the assumption that his data are being confidently protected by the system. If privacy is compromised, then the patient may avoid eHealth systems at all, thus resulting in life-threatening scenarios. Unfortunately the use of public networks in eHealth Grids had introduced a series of vulnerabilities that may negatively affect patient's trust in these technologies.

Our belief is that eHealth privacy must be enforced in a *layered* approach, where technological solutions complement current legislations. This paper has surveyed important efforts in both aspects, from Data Protection legislations in the European Union to novel mechanisms like the Electronic Health Card. In all of these the central piece is the concept of consent. Unfortunately current legal and technological approaches are unable to provide privacy to the lower levels of Intensive Care Grids, that is, the Storage Elements. This became evident after performing a security analysis over a eHealth Grid scenario, the ICGrid system. As a first step on proposing a security mechanism for Intensive Care Grids' data and metadata, in this paper we contributed with a privacy protocol able to use a mix of encryption and fragmentation to protect the patient's personal data from untrusted storage sites, while keeping compliance with upper-level implementations (i.e. the Electronic Health Card and the Grid Security Infrastructure) and current legislations.

Future work will focus on performance tests that provide more information about the optimal design of the privacy protocol presented in this paper: encryption/fragmentation at Storage Broker and, fragmentation at Storage Broker with encryption at Storage Elements. If no performance improvements are noticeable, then undoubtedly the first option is the best one from the security point of view, because encryption keys are never released to the untrusted Storage Elements. However, if big performance gains are achieved by moving the encryption mechanism to the Storage Elements, then the second option should be further investigated, maybe considering new requirements (i.e. searching information on stored datasets) or security enhancements (i.e. lazy re-encryption).

References

[1] Enabling Grids for E-SciencE project. http://www.eu-egee.org/.

[2] Cleversafe. http://www.cleversafe.com, 2007.
[3] Encrypted Storage and Hydra. https://twiki.cern.ch/twiki/bin/view/EGEE/DMEDS, September 2007.
[4] EU DataGrid, VOMS Architecture v1.1. http://grid-auth.infn.it/docs/VOMS-v1_1.pdf, March 2007.
[5] SHARE: Technology and Security Roadmap. http://wiki.healthgrid.org/index.php/Share_Roadmap_I, February 2007.
[6] Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, and Roger Wattenhofer. Farsite: Federated, available, and reliable storage for an incompletely trusted environment. In *OSDI*, 2002.
[7] European Health Management Association. Legally eHealth - Deliverable 2. http://www.ehma.org/_fileupload/Downloads/Legally_eHealth-Del_02-Data_Protection-v08(revised_after_submission).pdf, January 2006. Processing Medical data: data protection, confidentiallity and security.
[8] B. Hayes-Roth et al. Guardian: A prototype intelligent agent for intensive care monitoring. *Artificial Intelligence in Medicine*, 4:165–185, 1992.
[9] B. Fraser. Site Security Handbook. RFC 2196 (Informational), 1997.
[10] K. Gjermundrod, M. Dikaiakos, D. Zeinalipour-Yazti, G. Panayi, and Th. Kyprianou. Icgrid: Enabling intensive care medical research on the egee grid. In *From Genes to Personalized HealthCare: Grid Solutons for the Life Sciences. Proceedings of HealthGrid 2007*, pages 248–257. IOS Press, 2007.
[11] The OASIS Group. Security Association Markup Language (SAML) Specification v.1.0. http://www.oasis-open.org/committees/security/, April 2007.
[12] John Kubiatowicz and et. al. Oceanstore: An architecture for global-scale persistent storage. In *ASPLOS*, pages 190–201, 2000.
[13] Jesus Luna et al. Providing security to the desktop data grid. Accepted for the 2nd. Workshop on Desktop Grids and Volunteer Computing Systems (PCGrid 2008).
[14] Jesus Luna et al. An analysis of security services in grid storage systems. In *CoreGRID Workshop on Grid Middleware 2007*, June 2007.
[15] Jesus Luna, Manel Medina, and Oscar Manso. Using ogro and certiver to improve ocsp validation for grids. In Yeh-Ching Chung and José E. Moreira, editors, *GPC*, volume 3947 of *Lecture Notes in Computer Science*, pages 12–21. Springer, 2006.
[16] Federal Ministry of Health. The Electronic Health Card. http://www.die-gesundheitskarte.de/download/dokumente/broschuere_elektronische_gesundheitskarte_engl.pdf, Octuber 2006. Public Relations Section. Berlin, Germany.
[17] European Parliament. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31., Octuber 1995.
[18] Michael O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *J. ACM*, 36(2):335–348, 1989.
[19] Erik Riedel, Mahesh Kallahalla, and Ram Swaminathan. A framework for evaluating storage system security. In Darrell D. E. Long, editor, *FAST*, pages 15–30. USENIX, 2002.
[20] Richard O. Sinnott, Micha Bayer, A. J. Stell, and Jos Koetsier. Grid infrastructures for secure access to and use of bioinformatics data: Experiences from the bridges project. In *ARES*, pages 950–957. IEEE Computer Society, 2006.
[21] Graeme A. Stewart, David Cameron, Greig A Cowan, and Gavin McCance. Storage and Data Management in EGEE. In *5th Australasian Symposium on Grid Computing and e-Research (AusGrid 2007)*, January 2007.
[22] Mark W. Storer, Kevin M. Greenan, Ethan L. Miller, and Kaladhar Voruganti. Secure, archival storage with potshards. In *FAST'07: Proceedings of the 5th conference on USENIX Conference on File and Storage Technologies*, pages 11–11, Berkeley, CA, USA, 2007. USENIX Association.
[23] Von Welch. Globus toolkit version 4 grid security infrastructure: A standards perspective. http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf, 2005. The Globus Security Team.