

CoreGRID: European Research Network on Foundations, Software Infrastructures and Applications for large scale distributed, GRID and Peer-to-Peer Technologies

Data Privacy Considerations in Intensive Care Grids

University of Cyprus, FORTH ICS and
General Hospital of Nicosia

J. Luna, M. Flouris, M. Marazakis, A. Bilas,
M. Dikaiakos, H. Gjermundrod and T. Kyprianou

June-2008

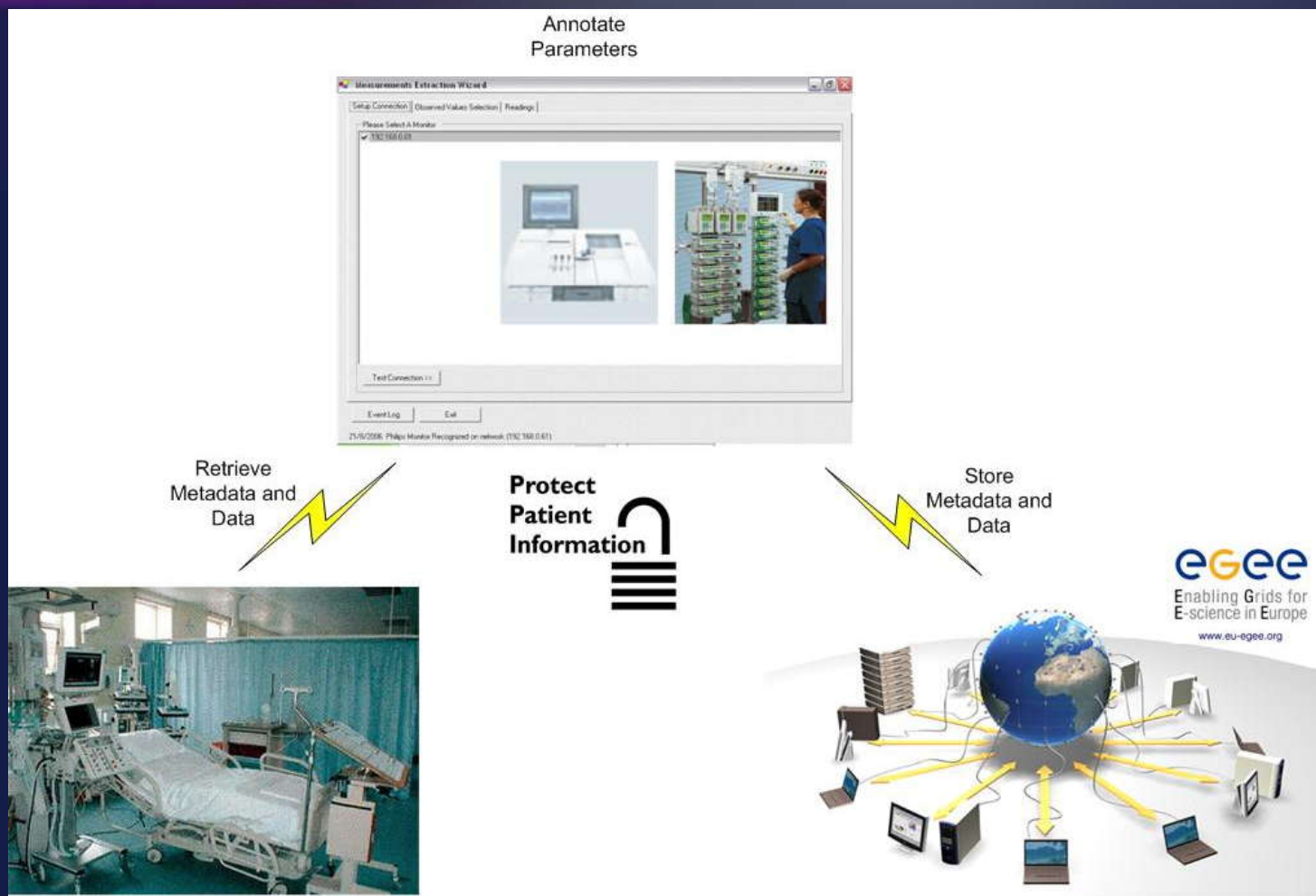
Outline

- **The Intensive Care Grid:**
 - **Motivation.**
 - **High-level Architecture.**
- **Security Requirements.**
- **Privacy Protocol.**
- **Conclusions and Future Work.**
- **Published Material.**

The Intensive Care Grid

- Intensive Care Units (ICUs) require mechanisms for data acquisition, validation, storage, analysis, correlation, etc.
- *ICGrid* has been prototyped over EGEE (Enabling Grids for E-Science in Europe) to cope with these needs.
- ICGrid's hybrid architecture combines sensors and Grid-enabled software tools.
- Everyday an ICU generates approx. 350 Mbytes:
 - Actual sensor's Data (not considering images).
 - Metadata, including patient's information and physician's annotations.

High-level architecture



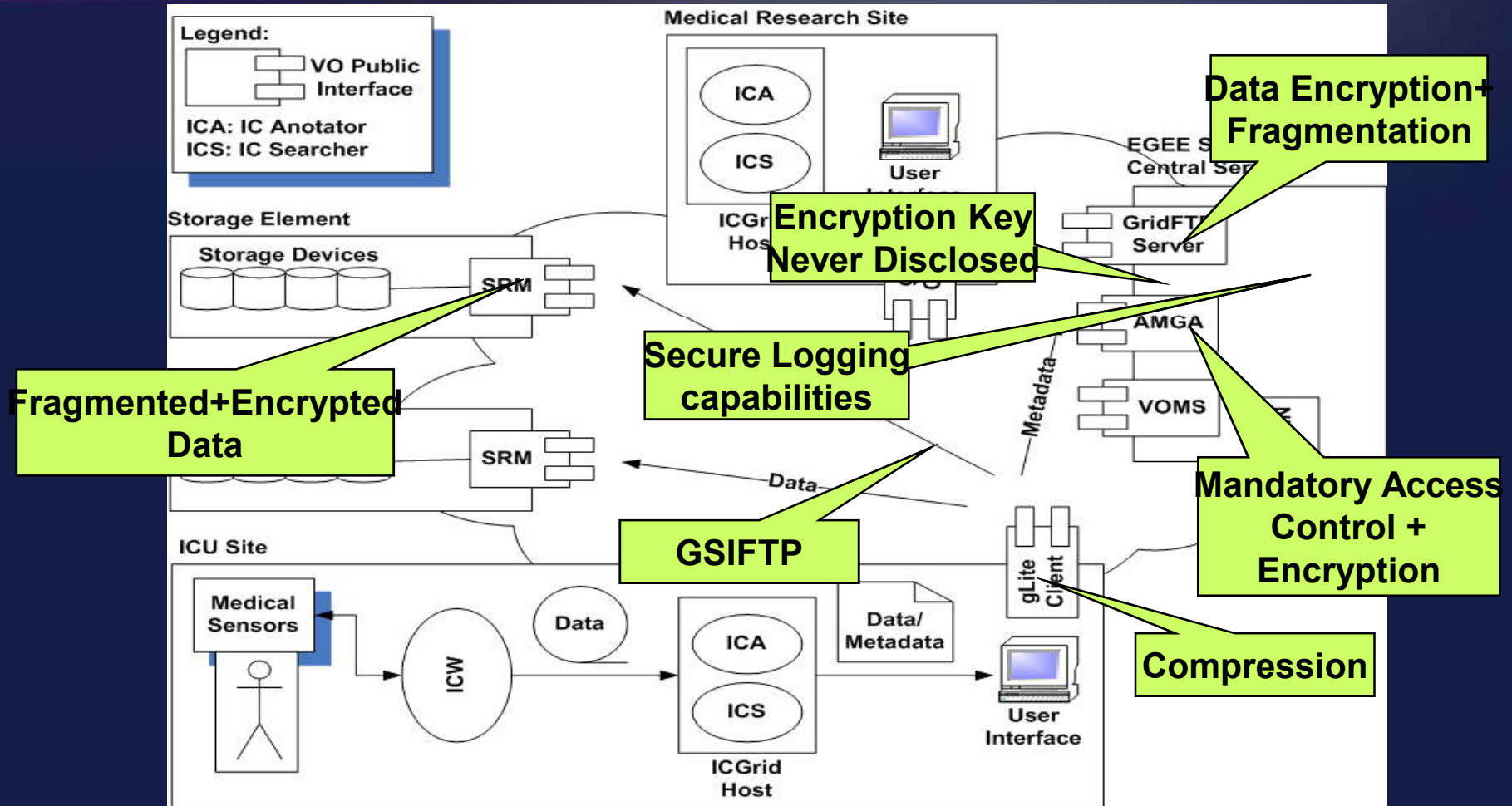
Security Requirements for Data and Metadata

- How to implement a data security solution for ICGrid, compliant with Legal and Technological approaches?
- We applied a data-security analysis framework defined in previous research to investigate Players, Trust Assumptions, Security Primitives, Attacks and Damages.
- Current security mechanisms:
 - Secure inter-site channels (i.e. GSIFTP).
 - EGEE Central Services (i.e. CA, VOMS) and implemented AuthN/AuthZ mechanisms are trusted.
- Identified Vulnerabilities:
 - Attackers with revoked credentials (latency in propagating revocation information). -> OGF
 - *Compromised Storage Elements provide full control over stored data.*

Privacy Protocol

- **Two basic mechanisms:**
 - **Cryptography (VO-level confidentiality, integrity) for Data and Metadata. *Design criteria:* performance, encryption keys do not traverse the network.**
 - **Data Fragmentation (high availability, confidentiality, scalability).**
- **Secondary mechanisms:**
 - **Mandatory Access Control for Metadata.**
 - **A Secure Log to back-trace operations.**

Proposed Security Architecture over gLite



Conclusions and Future Work

- **Due to new vulnerabilities being introduced, keeping patient's privacy has become a priority for Intensive Care Grids.**
- **Comprehensive Privacy Solutions should encompass Legal and Technological aspects. Interoperability Now!**
- **Based on a security analysis framework, a Privacy Protocol (cryptography, fragmentation) has been proposed for ICGrid.**
- **The protocol is being implement with the EGEE middleware (gLite).**
- **Prototype and follow-up being presented at OGF in Barcelona.**

Published Material

- **“An analysis of security services in Grid storage systems”**. In CoreGRID Workshop on Grid Middleware 2007. (Also published as TR-0090).
- **“D.IA.16 Update of the Survey Material on Trust and Security”**. Collaboration WP7. 2007.
- **“Providing security to the Desktop Data Grid”**. In CoreGRID PCGrid Workshop 2008.
- **“Using the gLite middleware to implement a secure Intensive Care Grid System”**. Accepted for the CoreGRID Workshop on Grid Middleware 2008.
- **“Knowledge and Data Management in Grids: notes on the state of the art”**. Collaboration WP2. To be published as CoreGrid White Paper WHP-002. 2008.

Thank you for your attention!

Questions?

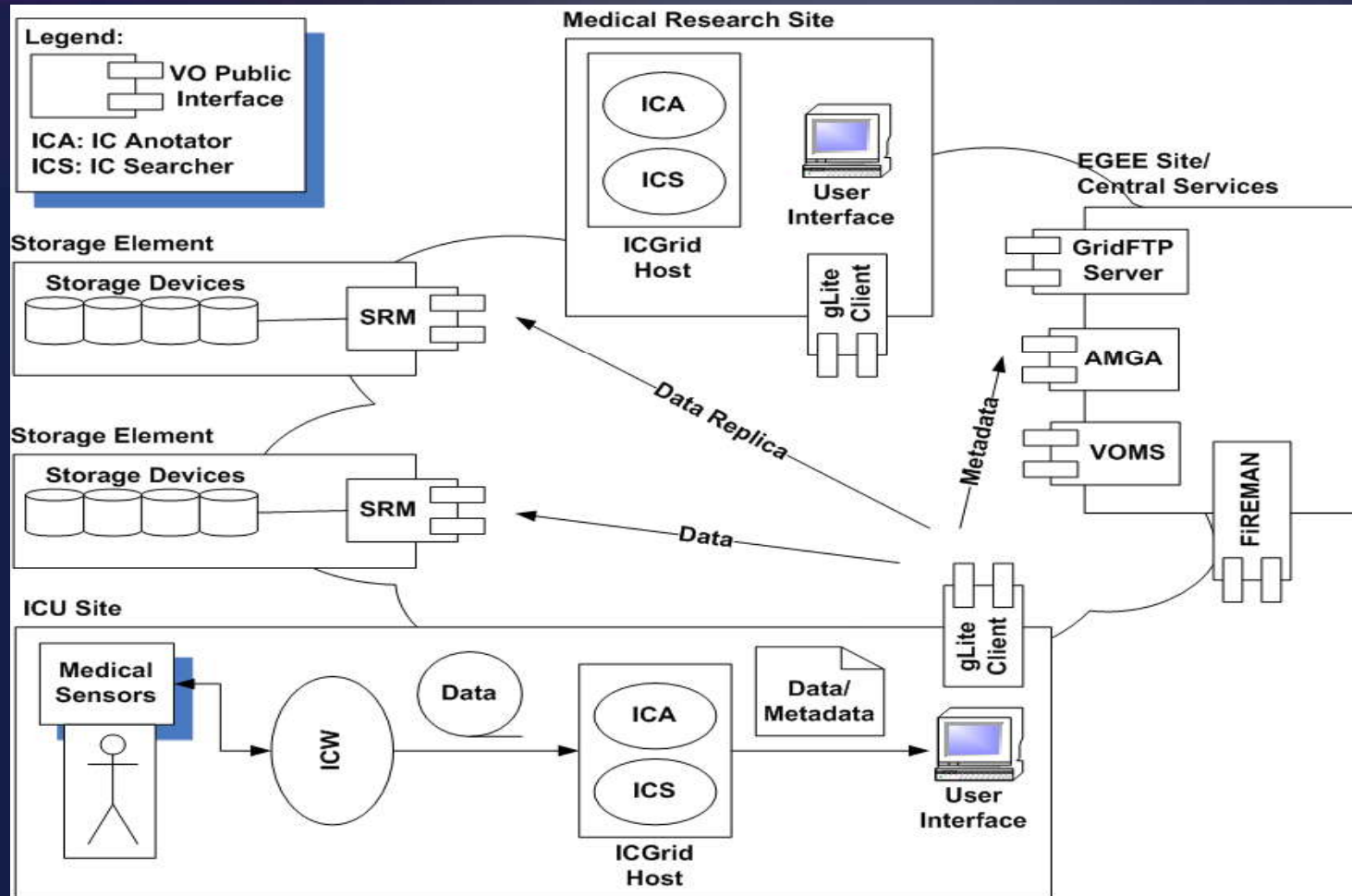


Jesus Luna

jluna@cs.ucy.ac.cy

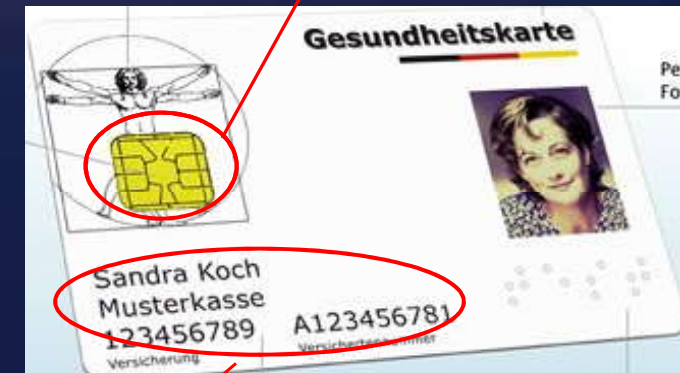
jluna@ics.forth.gr

Architecture



Example: Electronic Health Card (Germany)

- To replace European Health Insurance Card.
- Patient decides IF and WHICH information can be recorded or deleted and WHO has access to it.
- Two-keys principle:
 - The card itself.
 - PIN as sign of consent.
- In emergencies, data can be accessed with a Health Professional Card (i.e. ICU, paramedics).
- 50 most recent accesses are logged.



Cryptoprocessor

Administrative
Data