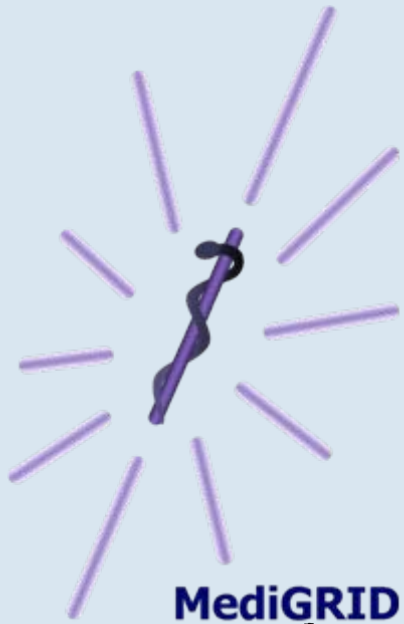
V19
Shortcomings of current Grid middlewares regarding data security and data protection

Göttingen, 27.03.2007

Yassene Mohammed



MediGRID
Bundesministerium
für Bildung
und Forschung

- **Requirements**
- **What does Globus offer?**
- **What is still missing?**
- **Solution outline**
- **Open questions**

legal framework for the protection, security and transport of personal data

- 95/46/EC processing of personal data
- 97/66/EC protection of privacy in the telecommunications sector
- 99/93/EC a framework for electronic signatures
- 2002/58/EC privacy and electronic communications

…

- [StGB, 1998] Neufassung des Strafgesetzbuches (Revised version of the penal code)
- [BDSG, 2001] das Bundesdatenschutzgesetz (Federal data protection act)
- [SigG, 2001] das Signaturgesetz (Signature act)
- [BOÄ-BW, 2001] die Ärztliche Berufsordnung (Medical profession code)

…

- Landesdatenschutzgesetze (Data protection act of the federal states)
- Landeskrankenhausgesetze (Hospital act of the federal states)

…

The legal framework implies special requirements regarding data security and data protection:

(1) Confidentiality

(2) Integrity and authenticity

(3) Accessibility

(4) Accountability

Additional data protection requirements arise dealing with person related data especially in the health care sector:

(1) Data necessarity principle: disclose all person related data of a patient, but not more than the needed data for the treatment

(2) Context of treatment: person related data of a patient should be disclosed only to the personnel participating in his treatment

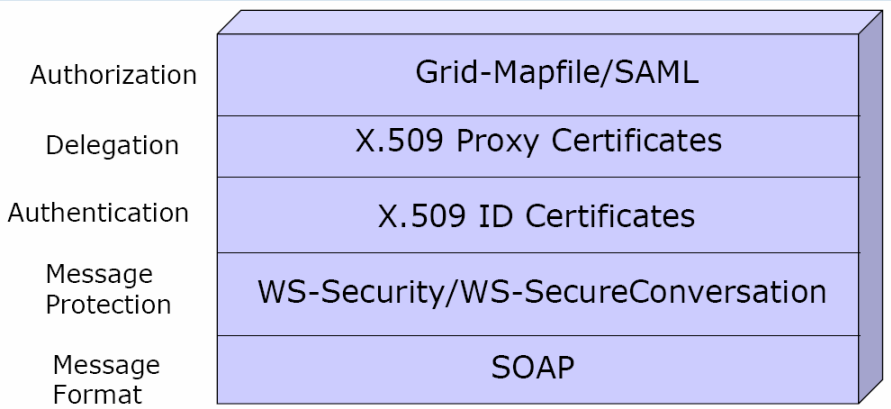
(3) Patient consent: the patient should formally agree on the handling of his person related data

(4) The guarantee of patient rights: the possibility of rectification, blocking, deletion of his personal data should be offered

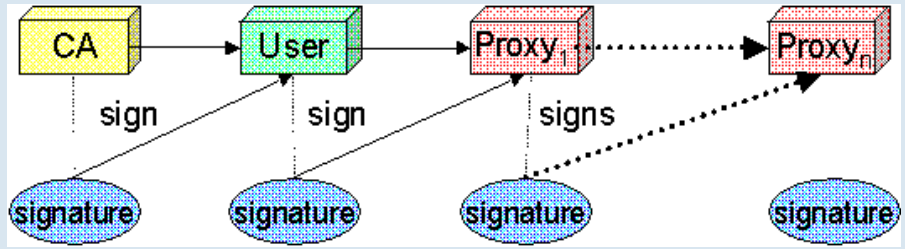
GT4 security deal with

- **Authentication,**
- **communication security,**
- **Authorization, and**
- **supporting functions for managing user credentials and maintaining group membership information.**

Security Layers in GT4*



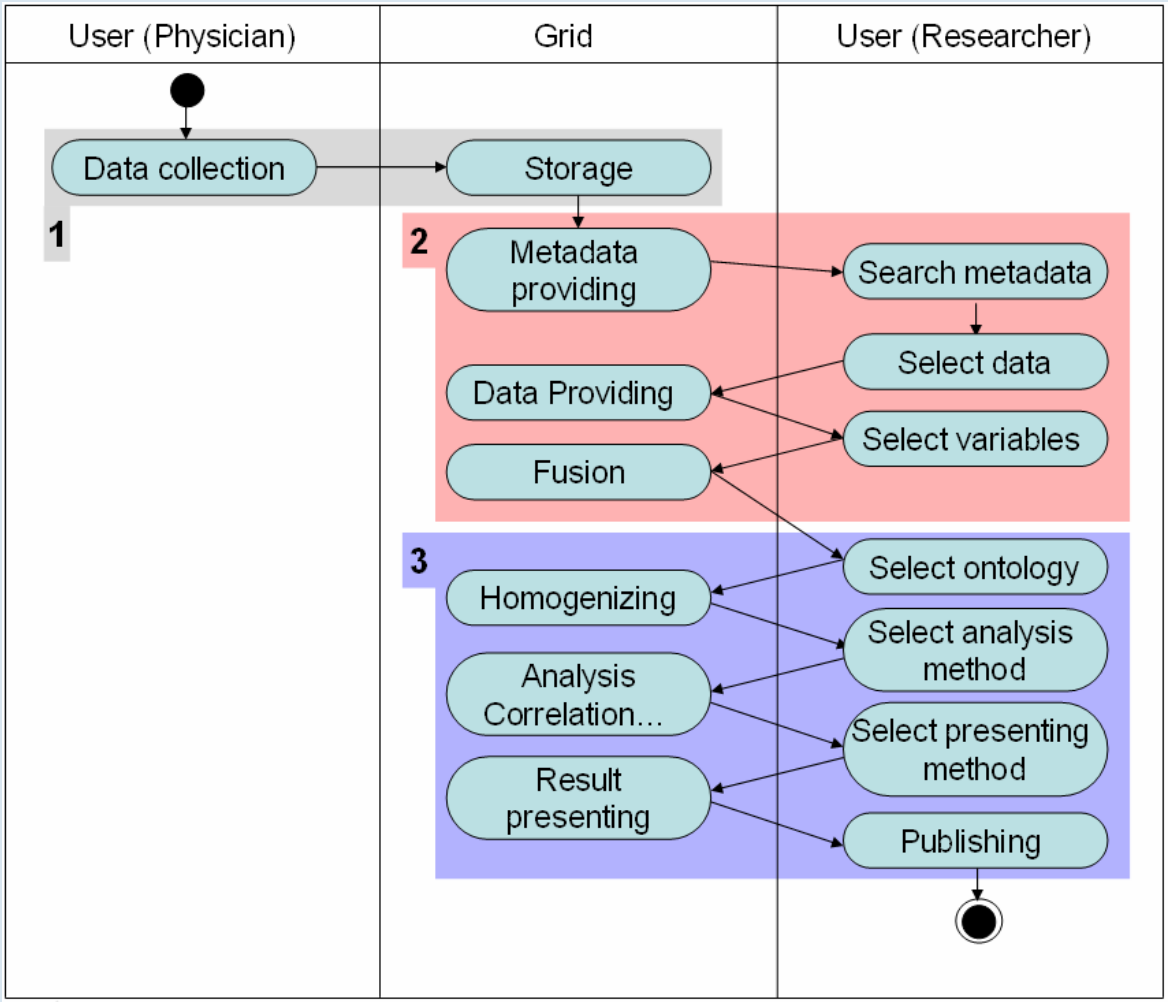
Proxy Certificates (MyProxy) **



* **F. Siebenlist, Von Welch.** ***Grid Security: The Globus Perspective.*** **In** ***GlobusWORLD 2005, Feb 7-11, Boston, MA.***

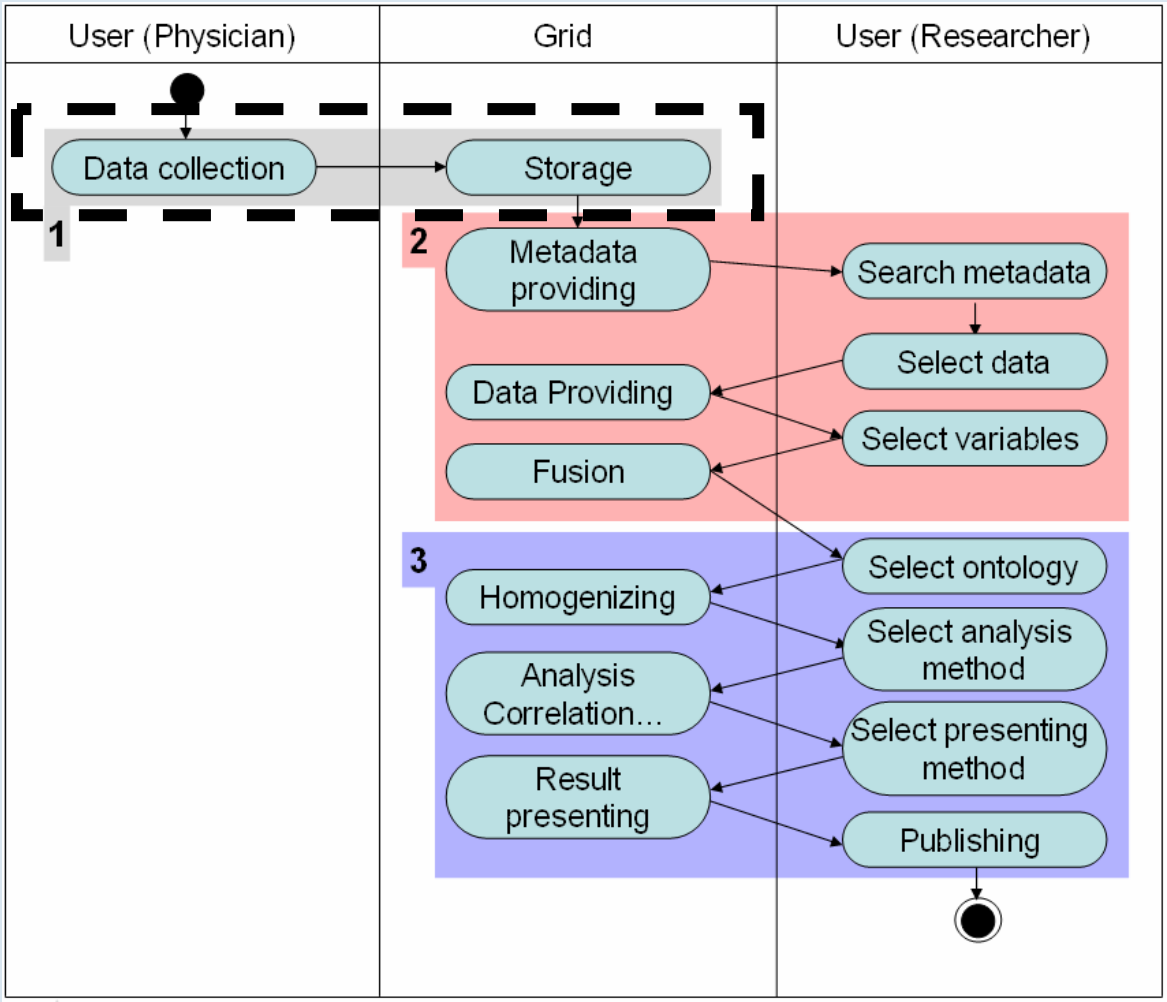
** **The GT4 Securtiy Team, GT 4.0 Security: Key Concept.** http://www.globus.org/toolkit/docs/4.0/security/key-index.html **[10.12.2006]**

Activity diagram of the service flow in (Medi)GRID
1- Upload 2- Retrieval 3 – Processing



***Mohammed Y, Sax U., Viezens F, Rienhoff O. Shortcomings of Current Grid Middlewares Regarding Privacy in HealthGrid. Proceedings of Healthgrid 2007. April 24-27, Geneva**

What does Globus offer?

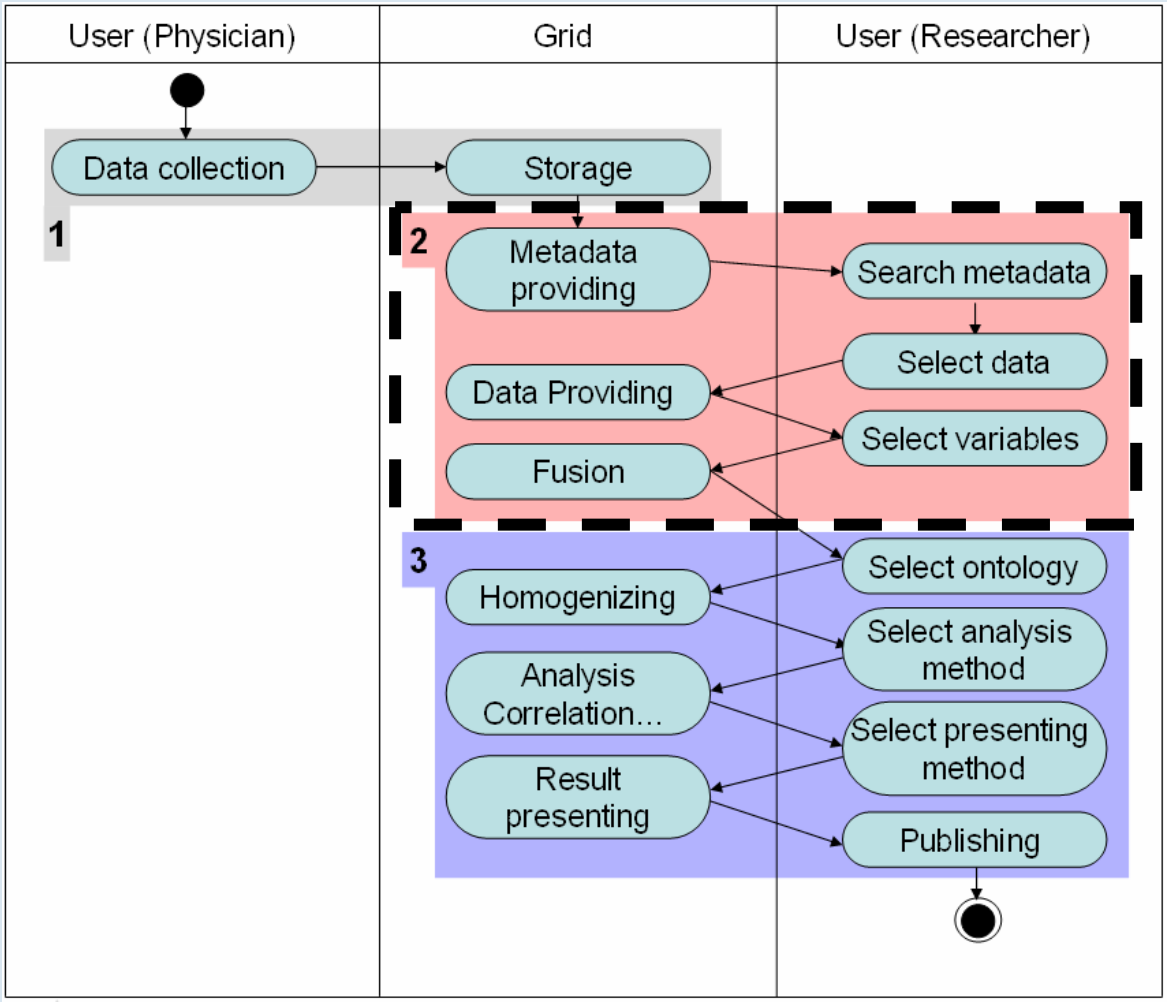


GSI +
GT4 Data Management

- **Data movement: GridFTP, Reliable File Transfer (RDT)**
- **Data replication: Replica Location Service (RLS)**
- **Higher level data services: Data Replication Service (DRS)**

→ confidentiality of communication
→ data integrity

What does Globus offer?

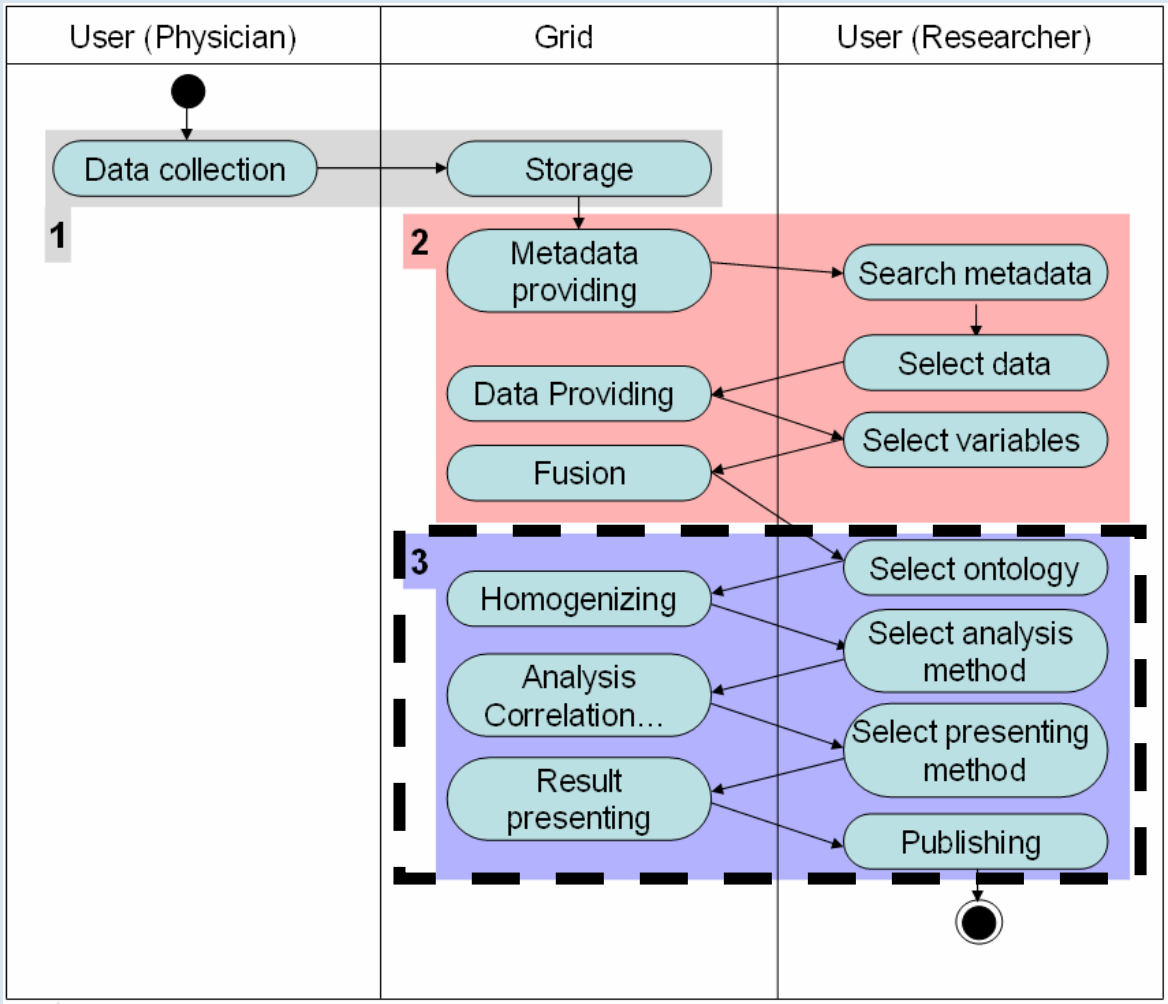


… +

- **Storage Resource Broker (SRB) – a data grid management system**
- **Open Grid Services Architecture - Data Access and Integration Services (OGSA-DAI)**
- **…**

→ confidentiality of communication
→ data integrity
→ accessibility

What does Globus offer?



… +

- **WS-Resource Framework (WSRF)**
- **Grid Resource Allocation and Management (GRAM) - Execution Management**
- **Monitoring and Discovery System (MDS) - Information Services**

→ confidentiality of communication
→ data integrity
→ accessibility
→ confidentiality within applications

Supplemental “Enhanced Security” elements for a (Health)Grid:

- ***Auditing***
- ***Trackability (a priori)***

→ **Auditing and tracking-possibilities cover the <u>accountability</u> requirement**

Supplemental “Enhanced Security” elements for a (Health)Grid:

- ***Fine grained role based access control*** **with respect to access rights within medical documents and within medical databases.**

→ **Cover the requirements of releasing only necessary data.**

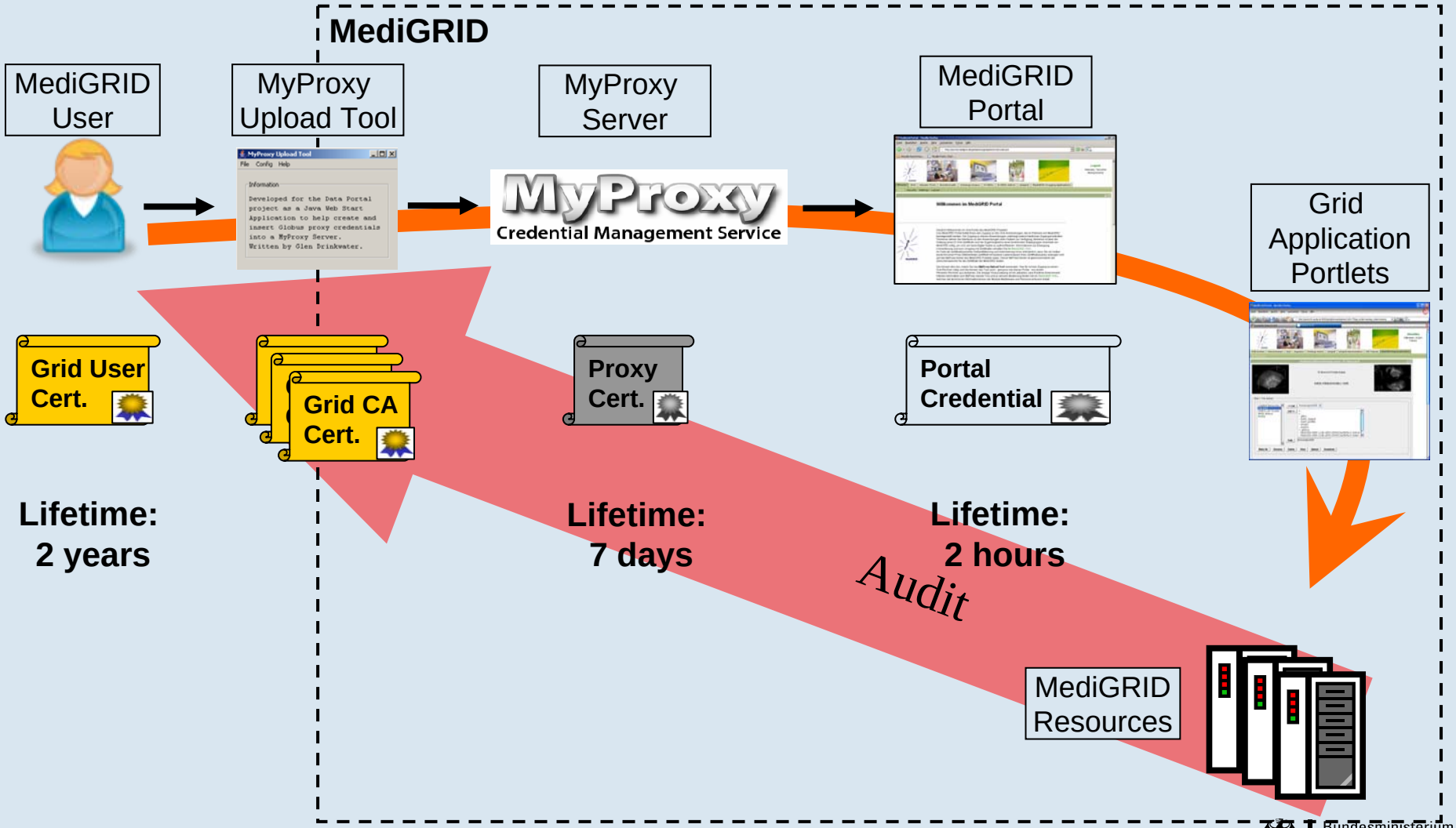
- ***Trust and trust-delegation*****: Using the data of a minor or a person with dementia requires that an authorized person signs electronically on behalf of those persons (eConsent).**

Supplemental “Enhanced Security” elements for a (Health)Grid:

- **Safety: requires policies for data storage and policies for data management.**

→ **Safety reflects the need to develop and adopt suitable policies for the use and storage of data; a complementary safeguard principle when intending to use sensitive data considering the accessibility in time (long term archiving) and place (replicas).**

Solution outline in MediGRID: Audit



Solution outline in MediGRID

Security policy framework

- **Phase one - developing phase**
- **Phase two - production and developing phase**
- **Phase three – enabling Trackability**

***Sax U, Mohammed Y, Viezens F, Rienhoff O. MediGRID moving towards a Horizontal HealthGrid – First Results. Submitted to Amia 2007**

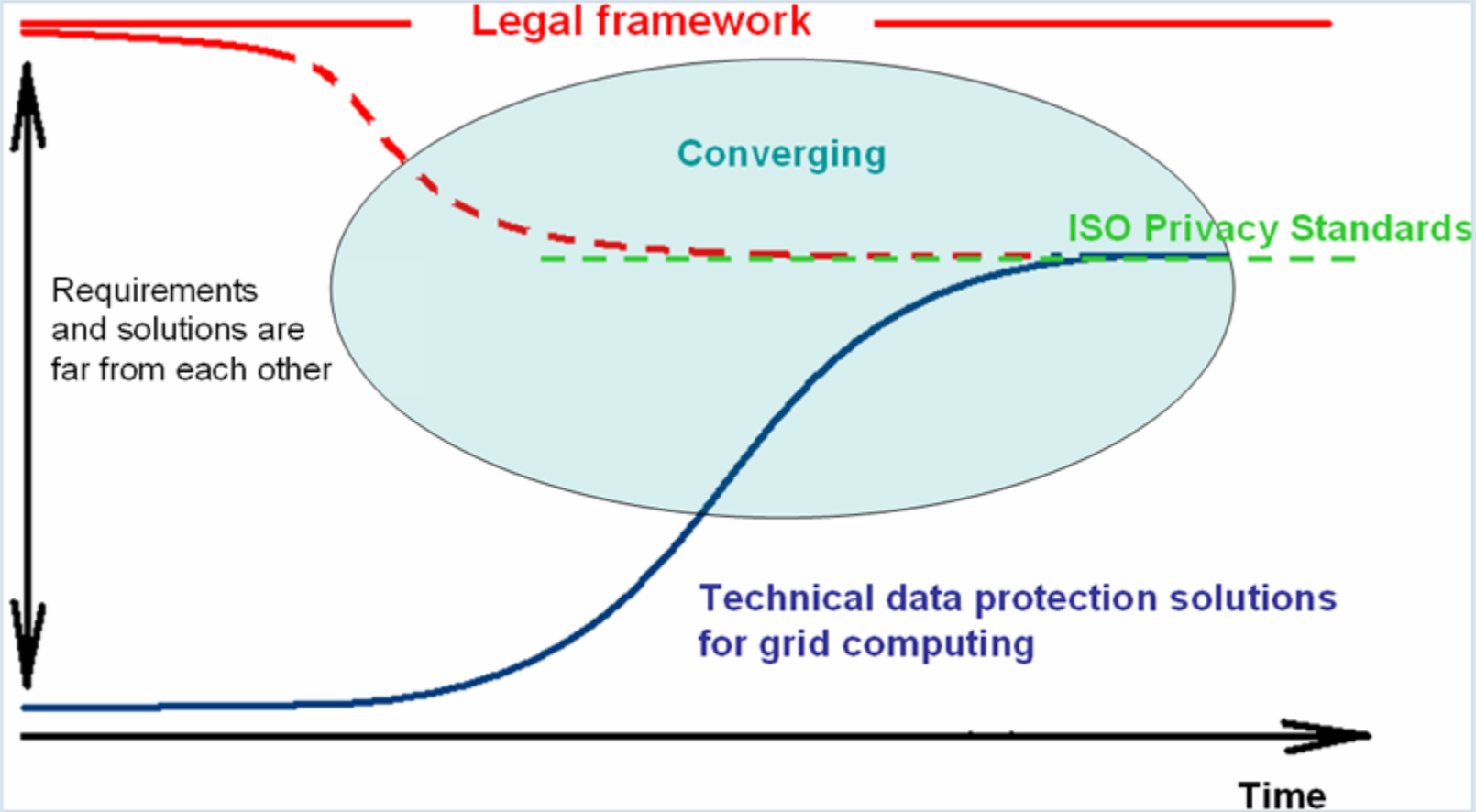
Solution outline in MediGRID

The “Enhanced Security” package is rather a one step towards enabling grid technology to be used by the biomedicine community than a complete solution.

In biomedicine applications sustainability should be guaranteed. That means we need to deal with two further dimensions for a more suitable solution:

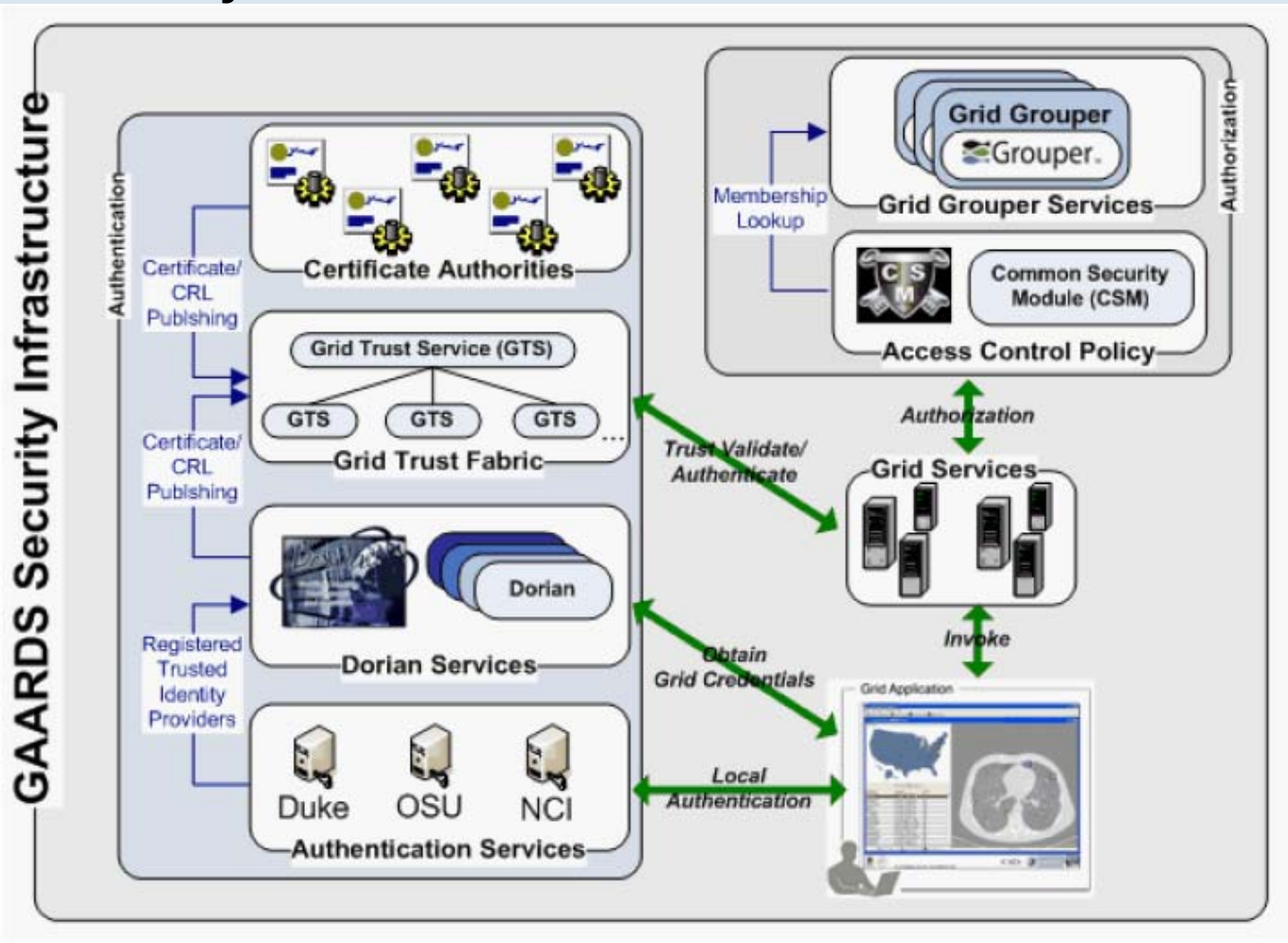
future development of the grid technologies and legal framework and
internationality.

Future development of the grid technologies and legal framework



*** Mohammed Y, Viezens F, Sax U, Rienhoff O. Rechtliche Aspekte bei Grid-Computing in der Medizin. In: Niederlag W, Dierks C, Rienhoff O, Lemke HU, eds. Rechtliche Aspekte der Telemedizin. Vol 2/2006; 2006:235-245.]**

Internationality
caBIG security



*Oster S, Foster I, Shanbhag A, Langella S, McConnell P, Hastings S, Wellborn D, Ervin D, Bragg V, Kurc T, Kumar V, Saltz J, Phillips J, Madduri R, Chilukuri R, Gawor J, Akkala S, Siebenlist F, Kher M, Wilde M, Erickson-Hirons W, Kettimuthu R, Manisundaram A, Allcock B, Komatsoulis G. *caGrid 1.0 USER'S GUIDE*

Does this solve the Grid-Security problem?

gridftp

- Extension of FTP to support striped and remote-controlled transfer
- Part of Globus
- Implementation in Globus based on wuftpd

gridftpd

- CVE-2004-0185 – wuftpd

ftpd.c from wuftpd

```
char *skey_challenge(char *name, struct passwd *pwd, int
pwok)
{
      static char buf[128];
      ...
      if (pwd == NULL || skeychallenge(&skey, pwd->pw_name,
                                       sbuf))
          sprintf(buf, "Password required for %s.", name);
      else
          sprintf(buf, "%s %s for %s.", sbuf,
                  pwok ? "allowed" : "required", name);
      return (buf);
}
```


gridftpd

ftpd.c from gsi-wuftpd (gridftp), GT 4.0.2

```
char *skey_challenge(char *name, struct passwd *pwd, int
  pwok)
{
    static char buf[128];
    char sbuf[40];
    struct skey skey;

    /* Display s/key challenge where appropriate. */

    if (pwd == NULL || skeychallenge(&skey, pwd->pw_name,
                                     sbuf))
        sprintf(buf, "Password required for %s.", name);
    else
        sprintf(buf, "%s %s for %s.", sbuf,
                pwok ? "allowed" : "required", name);
    return (buf);
}
```


Things to do in long winter nights

- Proper code audit of Grid middleware
- Architecture review of Grid middleware
- Architecture & implementation review of Grid applications
- Puzzling over unsolved fundamental problems
- Investigate implications of “service-oriented architecture” fancy

How to deal with it?

- **Code verifying**
- **Software validation (Common Criteria…)**
- **Enforce security within implemented application**
- **Risk analysis**

This question is open for the specialists in the DGI !

Many thanks for your attention!