Pseudonymity-related work in EGEE-II

Henri Mikkonen / HIP

MWSG, EGEE'07 Conference

Budapest, Hungary

Information Society and Media

Background

- **As described in the EGEE Global Security Architecture document (DJRA3.1)**
  - "...*an outsider should not be able to deduce a particular user's activities, such as how much of the resources the user consumes or what applications are run...*"
  - Information creep is of serious concern to applications in areas of highly competitive research, such as biomedicine.
    - At least the resource administrators are able to figure out the used resources and applications.
  - Users should be able to hide their real identity behind pseudonym identity
    - pseudonymity = almost-anonymity

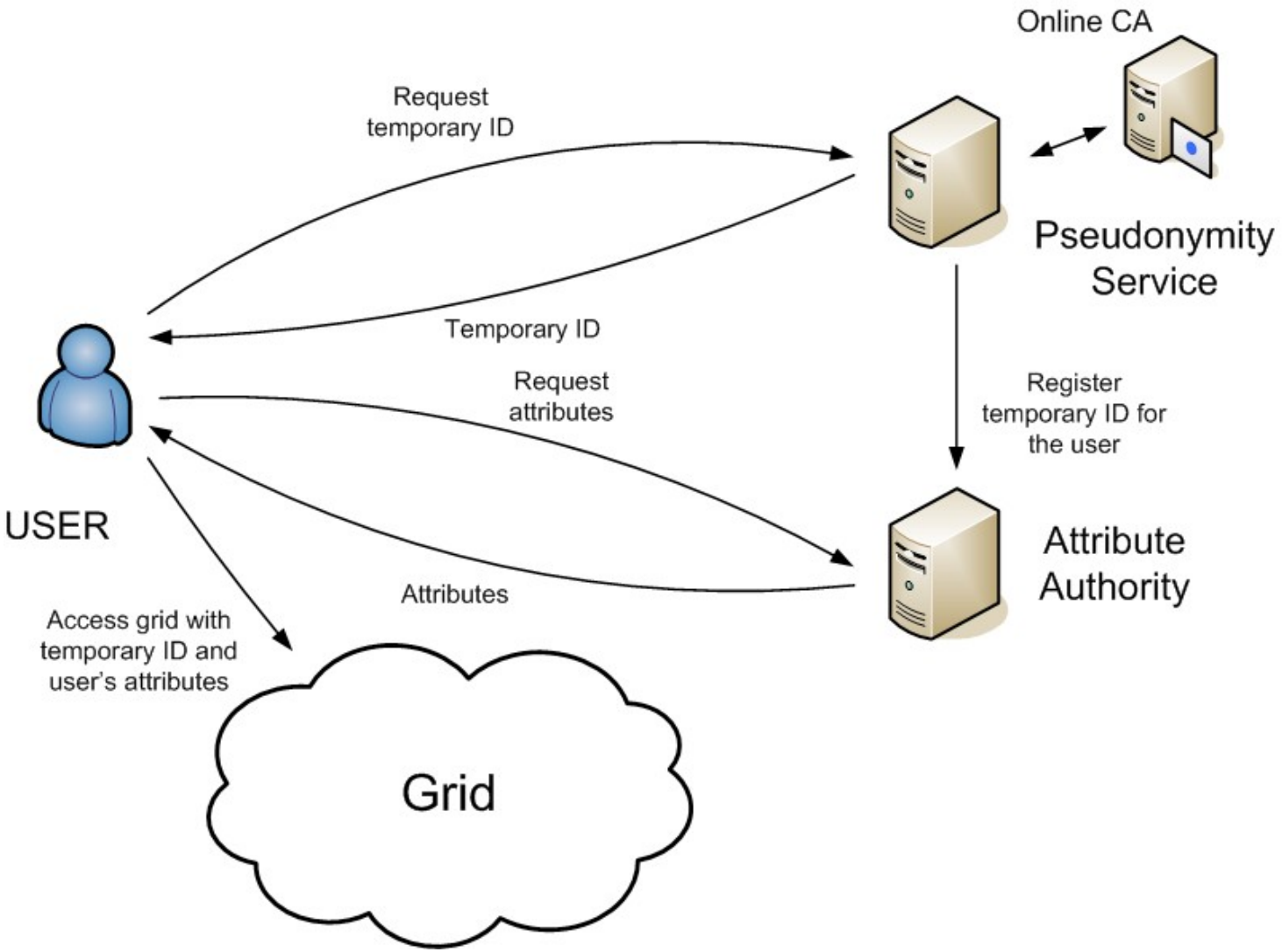
Pseudo-System Requirements

- **Must interoperate with the existing gLite middleware with minimal modifications**
  - The pseudonym identities must be based on X.509 certificates
- **The relationships between the pseudonym and real identities must be kept secret**
  - The pseudonym identities must be unique and short-live
- **The relationships must be possible to reveal in the case of misuse**
  - Law enforcement or a similar legitimate body may require it as a part of their investigations

Pseudo-System Components

- **Pseudonymity Service**
  - The pseudonym identity provider and accountant
- **Online CA**
  - Issues certificates with a pseudonymous subject DN
  - Standards like CMC (RFC 2797) and CMP (RFC 4210) exist for the communication
- **Attribute Authority**
  - Provides the attributes for the pseudonym identities

Interaction of the Components



Current Design

- **Pseudonymity Service seems to have some similarities with the already implemented SLCS server**
  - It is used for obtaining short-live certificates from an online CA
- **Required modifications/plugins to the SLCS software**
  - Server-side
    - Non-Shibboleth user authentication (proxy certificate)
    - Non-Shibboleth user authorization (VOMS attributes)
    - New DN builder for creating pseudonymous DNs
    - Registration of the pseudonymous DNs to VOMS
    - (Better support for different online CA connections)
  - Client/UI-side
    - Utilize VOMS proxy in the TLS mutual authentication
    - (Management of multiple pseudonymous certificates and keys)

Current Status

- **Currently in the implementation phase**
  - First implementations ready for
    - User authentication using proxy certificate
    - Pseudonymous DN builder for the SLCS server
    - CMP protocol support for the SLCS server
    - Client tool utilizing VOMS proxies
  - Currently under construction:
    - User authorization using VOMS attributes from the proxy
    - Registration of the pseudonymous DSs to VOMS
- **The first working prototype ready for testing by the end of 2007**