Pseudonymity Service

Henri Mikkonen

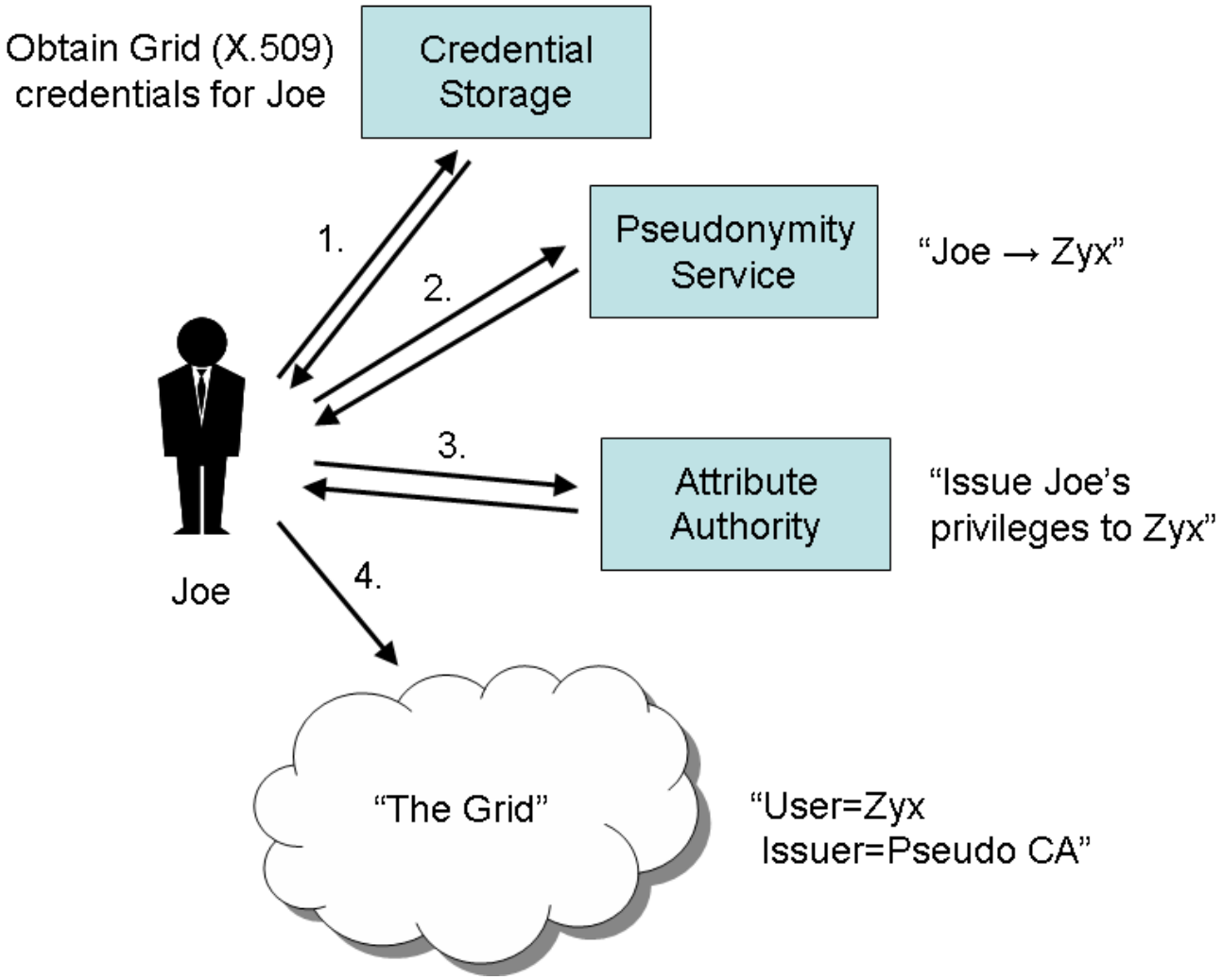
EGEE-II JRA1 All-Hands Meeting

18-20 June 2007, Helsinki, Finland

Introduction

- **As described in the EGEE Global Security Architecture document (DJRA3.1):**
  - 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.
  - The pseudonymity service swaps the user's real identity for a pseudonym, thus hiding it from immediate exposure in logs and on the network.
    - The pseudonymity service acts in all regards as another TTP, with the addition that it is also trusted to keep the relationship between the pseudonym and real identity secret.
    - This trust has to be kept unless law enforcement or a similar legitimate body requires it as part of e.g. an investigation on malicious use.

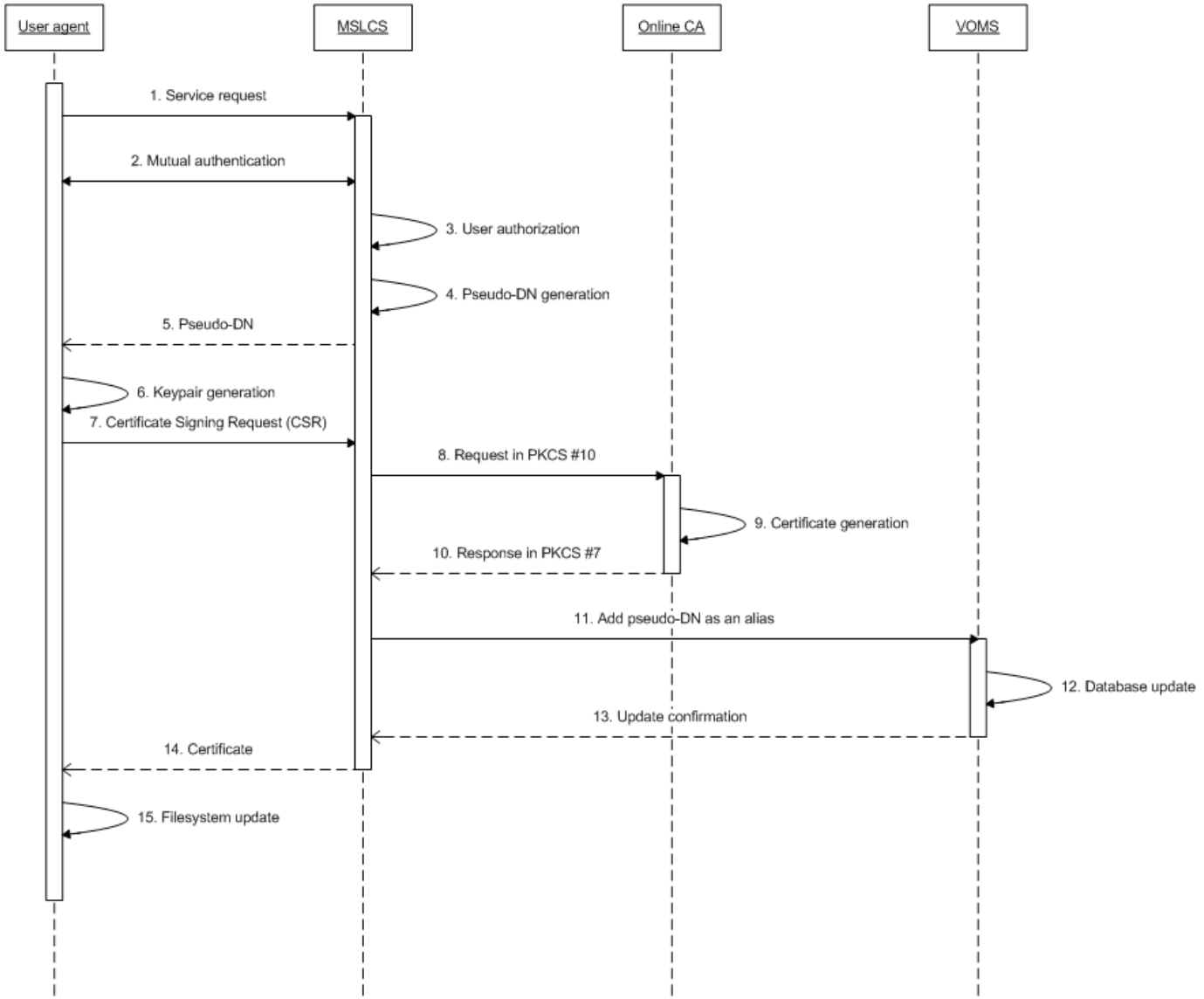
Overview


Obtain Grid (X.509) credentials for Joe
Credential Storage
1.
2.
Pseudonymity Service
"Joe → Zyx"
3.
Attribute Authority
"Issue Joe's privileges to Zyx"
Joe
4.
"The Grid"
"User=Zyx
Issuer=Pseudo CA"

Current design

- **Pseudonymity Service seems to have some similarities with the SWITCH's SLCS server**
  - It is used for obtaining short-live certificates from an online CA.
  - Thanks to the SLCS's modular implementation, it can be used as a basis for the pseudonymity service implementation too.
- **Required modifications/plugins to the SLCS software**
  - Server-side
    - Authenticate/authorize users by VOMS proxy certificates instead of Shibboleth (TrustManager functionality)
    - Implement a new DN builder (For creating pseudo-DNs)
    - Inform VOMS server of the pseudo DNs
    - Interface for obtaining the pseudo users' information
    - (Support for CMP-protocol (RFC 4210) in the OnlineCA connection)
  - Client/UI-side
    - Utilize VOMS proxy in the HTTPS mutual authentication
    - Store the pseudo certificate & key in the file system

Current sequence



Current issues

- **Certificate lifetime**
  - Long enough to avoid renewal
  - Short enough to avoid revocation
    - <1 million seconds?
- **Auditing**
  - Who is authorized to obtain the user information and how?
  - Can pseudo-DNs be “recycled” in a specific time scale?
    - DJRA3.1 mentions one-time identity
- **VOMS**
  - The DN-alias functionality does not exist yet
- **Module/package naming**
  - org.glite.pseudo.*?