Security (JRA3)

Åke Edlund, JRA3 Manager, KTH
David Groep, Security Expert, NIKHEF
EGEE 1st EU Review
9-11/02/2005

Introduction - JRA3 Objectives

- **Enable secure operation of a European Grid infrastructure.**
  - Develop security architectures, frameworks and policies.
  - Definition of incident response methods and authentication policies.
- **Consistent design of security mechanisms for all core Grid services**
  - Meet production needs of resource providers with regard to identity, integrity and protection.
- **Provide robust, supportable security components (as part of JRA1)**
  - Select, re-engineer, integrate identified Grid Services
- **Selection of security components is based on requirements of:**
  - The Middleware developers
  - The Applications
  - The Grid operations

Introduction - Achievements, Issues and Mitigation

Major achievements

- **Producing key security deliverables (well received in the community)**
  - Global Security Architecture
  - Site Access Control Architecture
- **Delivered a number of security modules, of which four will be part of gLite v1**
- **Driving community level agreements for middleware and policy**
  - EUGridPMA

Major issues and mitigation

- **Geographically distributed teams**
  - Need to improve the handing over of security modules to the middleware developers. More F2F meetings.
  - Improve further contact with NA4, applications.
- **Conflicting/challenging security requirements from applications**
  - Proposed solutions meeting the sets of requirements as much as possible.

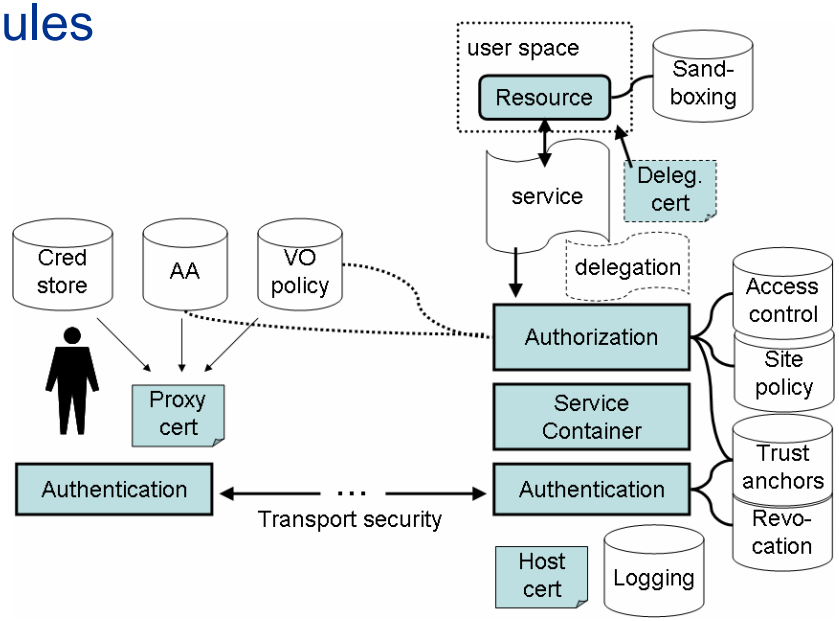
Architecture - Baseline assumptions

- **Security Architecture - Modular, Agnostic, Standard, Interoperable**
  - Modular – possible to add new modules later
  - Agnostic – implementation independent
  - Standard – e.g. start with transport-level security but intend to move to message-level security when it matures
  - Interoperable - at least for AuthN & AuthZ
  - Applied to Web-services hosted in containers (Apache Axis & Tomcat) and applications as additional modules

Requirement: Support for legacy and non-WS based software components

Solution: Modular authentication and authorization software suitable for integration

Fulfilled/Time frame: Yes/Now



Architecture - Baseline assumptions

Security Requirements - a horizontal activity, managed through central groups

- Lesson learned: reused and updated requirements from earlier projects
- Collecting (continuous process) the requirements from the activities - Middleware, Sites, Applications.
- Share the requirements with other grid activities and get feedback, e.g. OSG.
- Prioritization set in the security groups, with representatives from all involved activities.
- Defining what security modules to deliver when.

Major security issues with current production service

Major issues

- Many of the services don't have authentication.
- Information system has host-based access control only
- Data storage is effectively based on VO membership only
- Procedural issues, e.g. in incident handling
- No resource control on the local clusters
- Proliferation of network connectivity (especially outbound)
- Users store private credentials on NFS file systems.
- VOs are managed in LDAPs that are not secured.

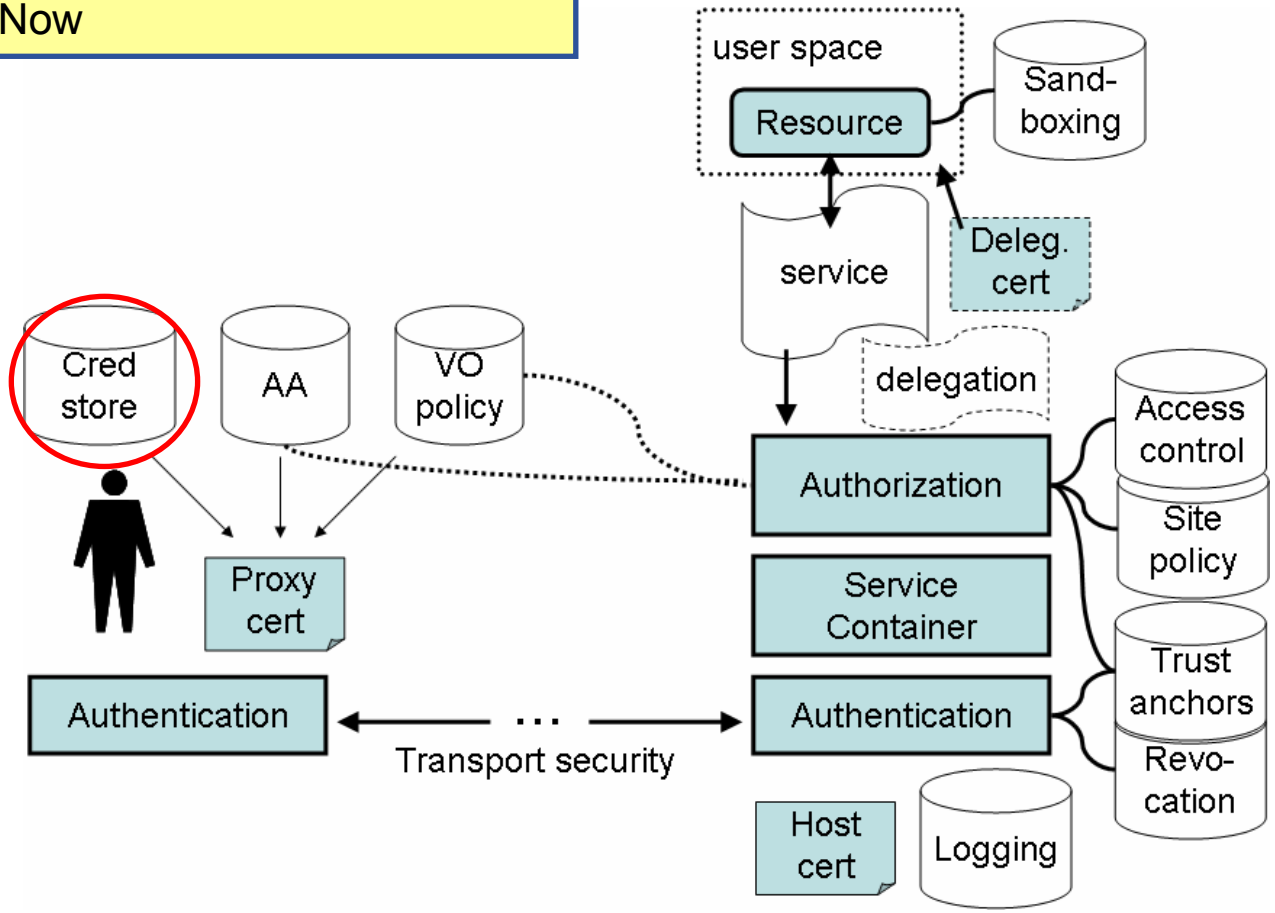
Will gLite be any better?

gLite will have less of these limitations, but we will still need to use and deploy the software correctly and within its limitations.

- Better and more flexible tools for authorization and credential management.
- Improved operational procedures and processes.
- New services and solutions such as DCS, data key management, pseudonymity,sandboxing.

Services - Authentication

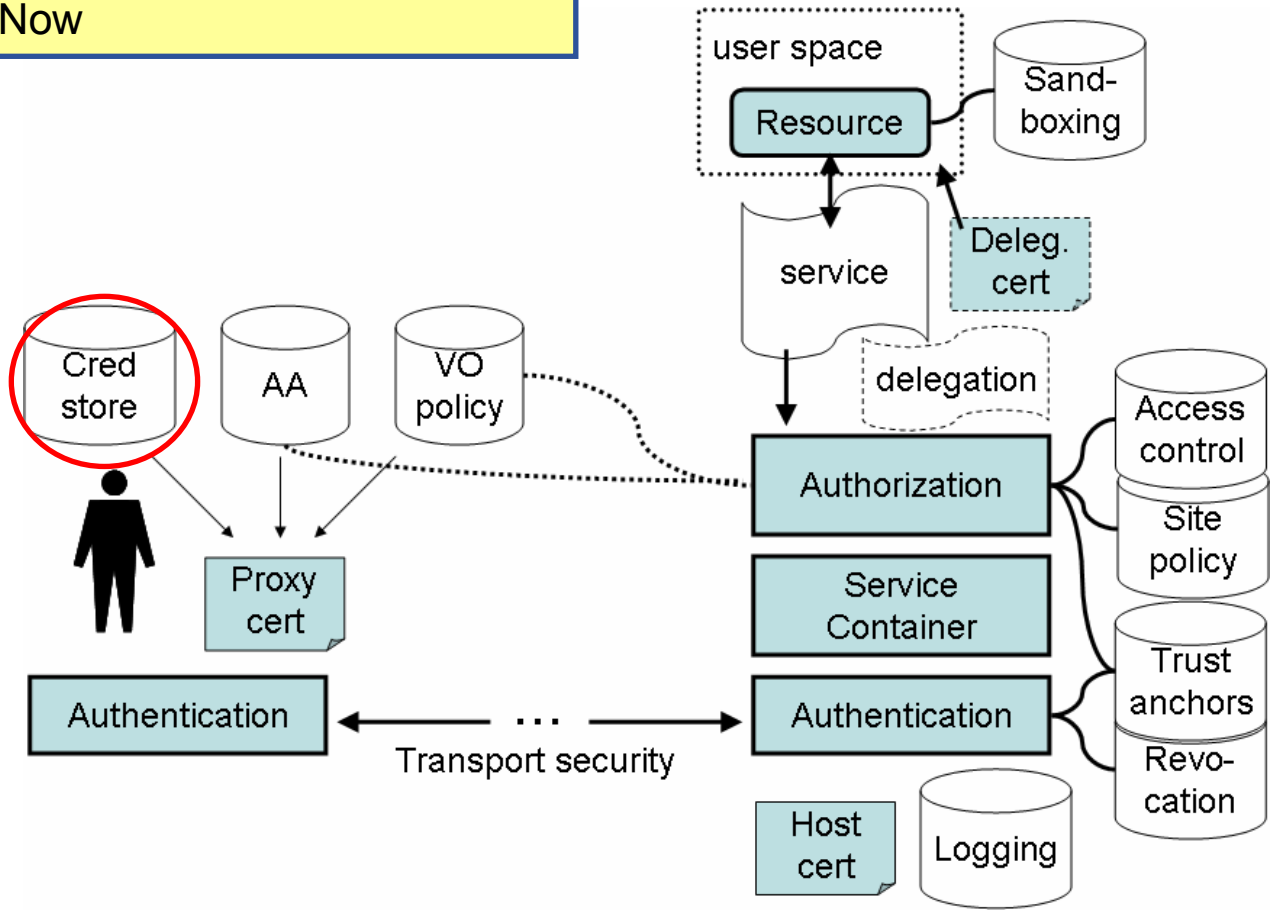
Managed credential storage ensures proper security of credentials. Password-scrambled files should go away
Fulfilled/Time frame: Yes/Now



Services - Authentication

Managed credential storage ensures proper security of credentials. Password-scrambled files should go away
Fulfilled/Time frame: Yes/Now

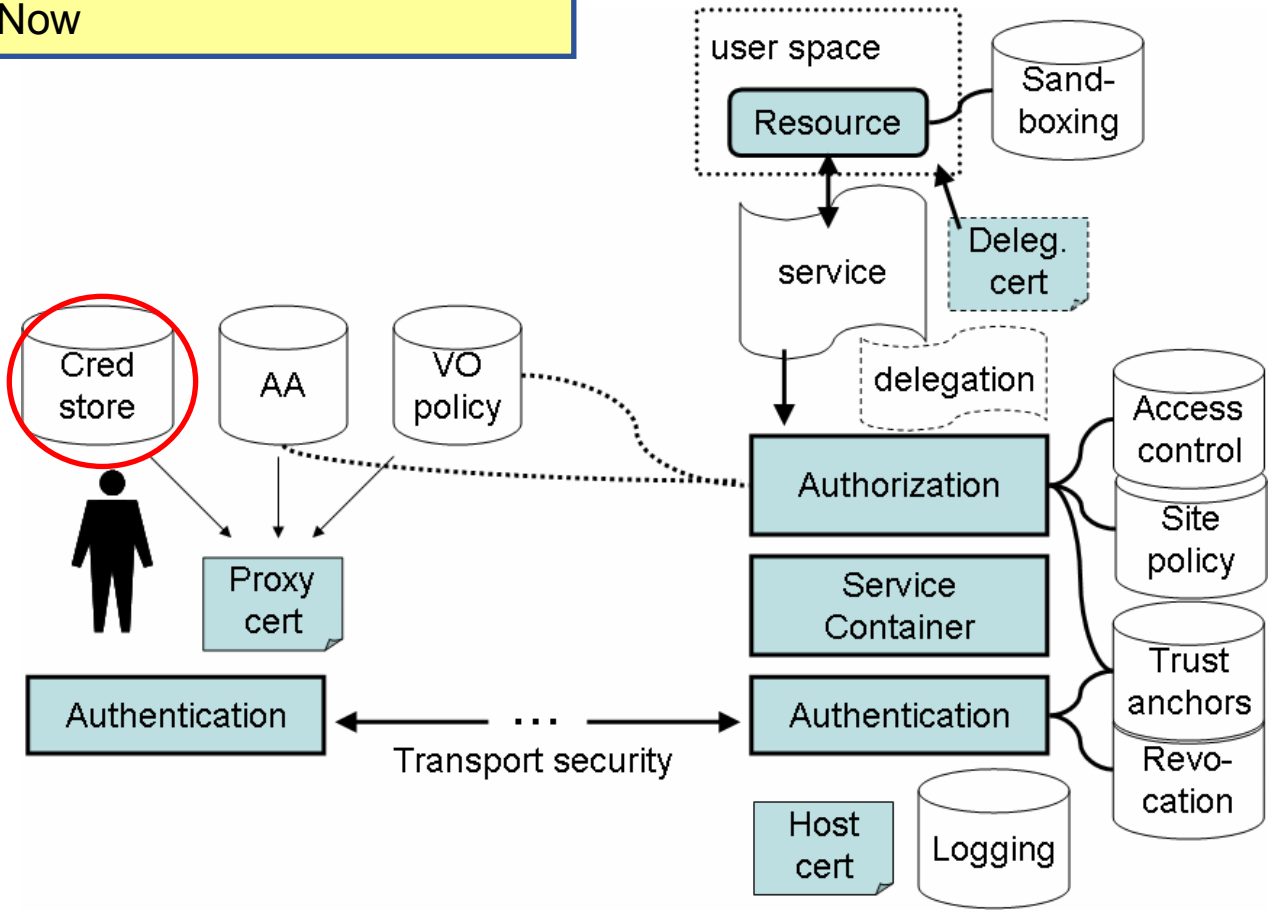
Fulfilled by the architecture



Services - Authentication

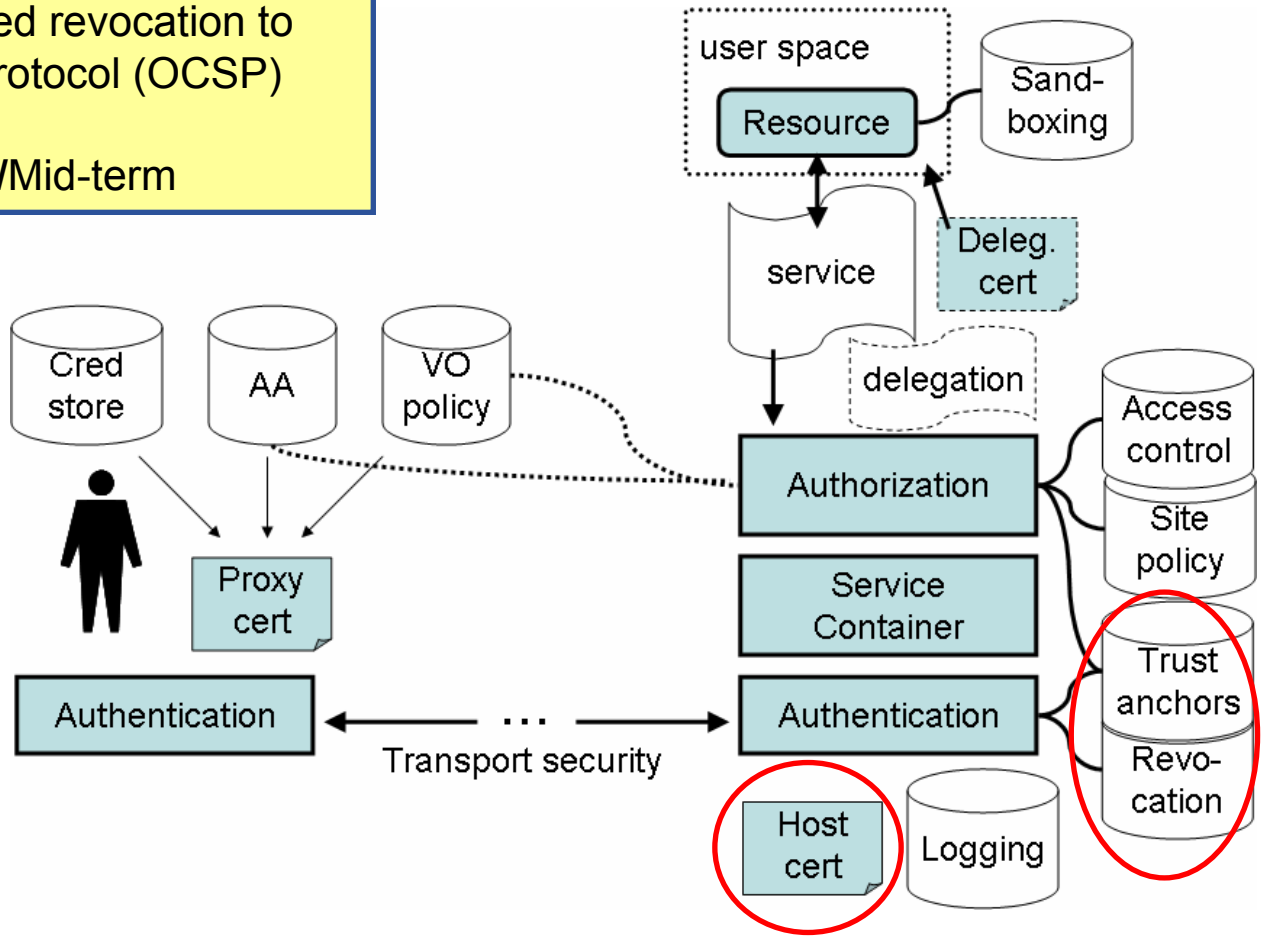
Managed credential storage ensures proper security of credentials. Password-scrambled files should go away
Fulfilled/Time frame: Yes/Now

When is the solution available to be used? E.g. mid-term = PM24



Services - Authentication

Requirement: Timely credential revocation
Solution: Gradual transition from Certificate Revocation List (CRL) based revocation to Online Certificate Status Protocol (OCSP) based revocation
Fulfilled/Time frame: Yes/Mid-term

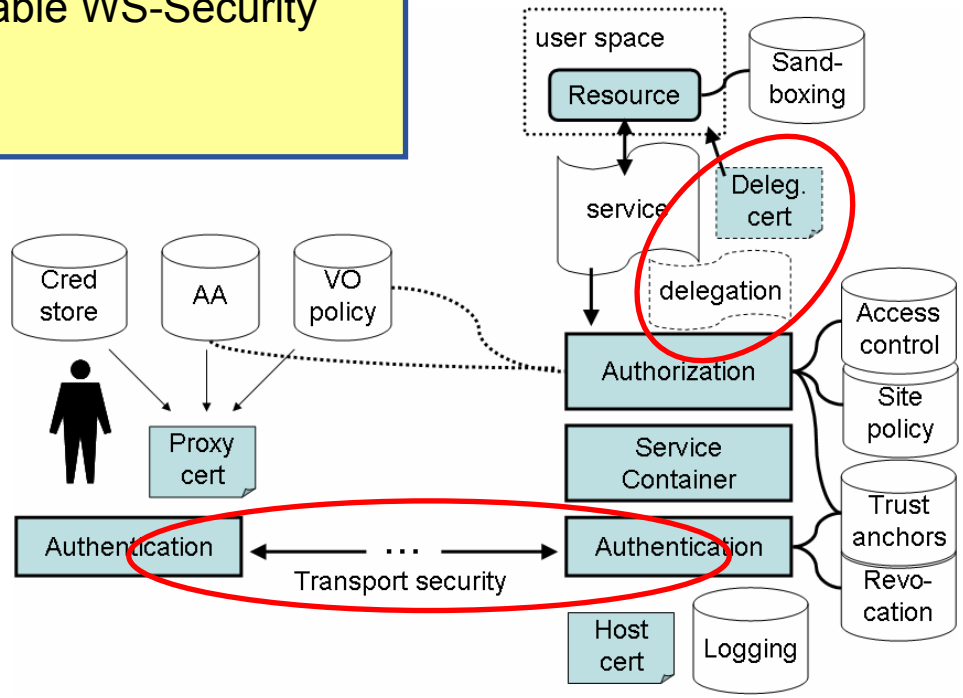


Services - TLS vs MLS

Transport Level Security
- Uses widely deployed TLS/SSL protocol
- Doesn't provides security through intermediate hosts (can be done using delegation, not yet delivered).

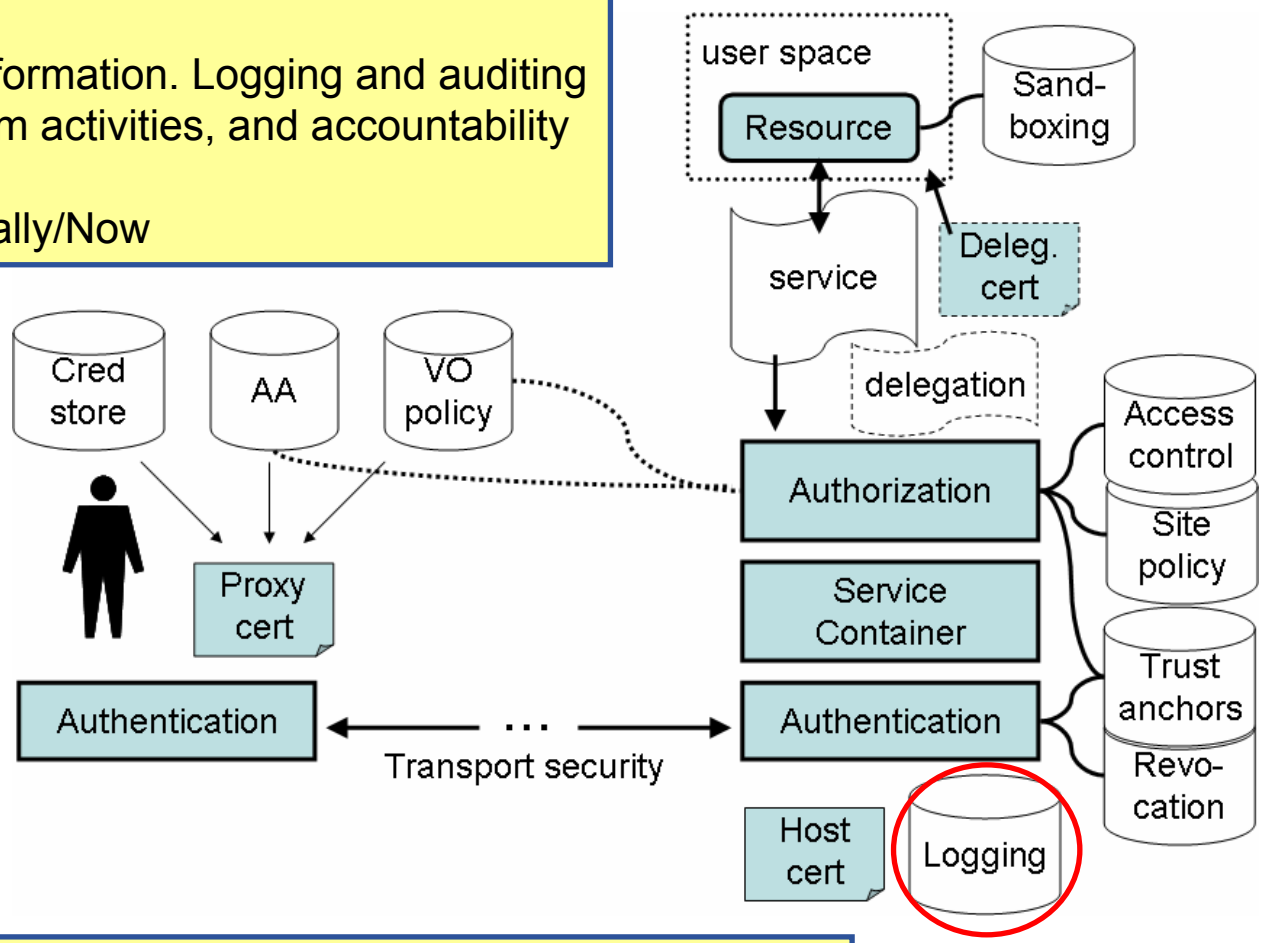
Message Level Security
- Uses Web Services or SOAP messages security technology
- Recommended by WS-I Consortium as preferable WS-Security solution
- Performance and support issues

So, TLS for now
- SOAP over HTTPS with proxy cert supported path validation
- WS interface for delegation
- **Move to MLS as we go along**
- Use cases for MLS exist already (DM)



Services - Logging and Auditing

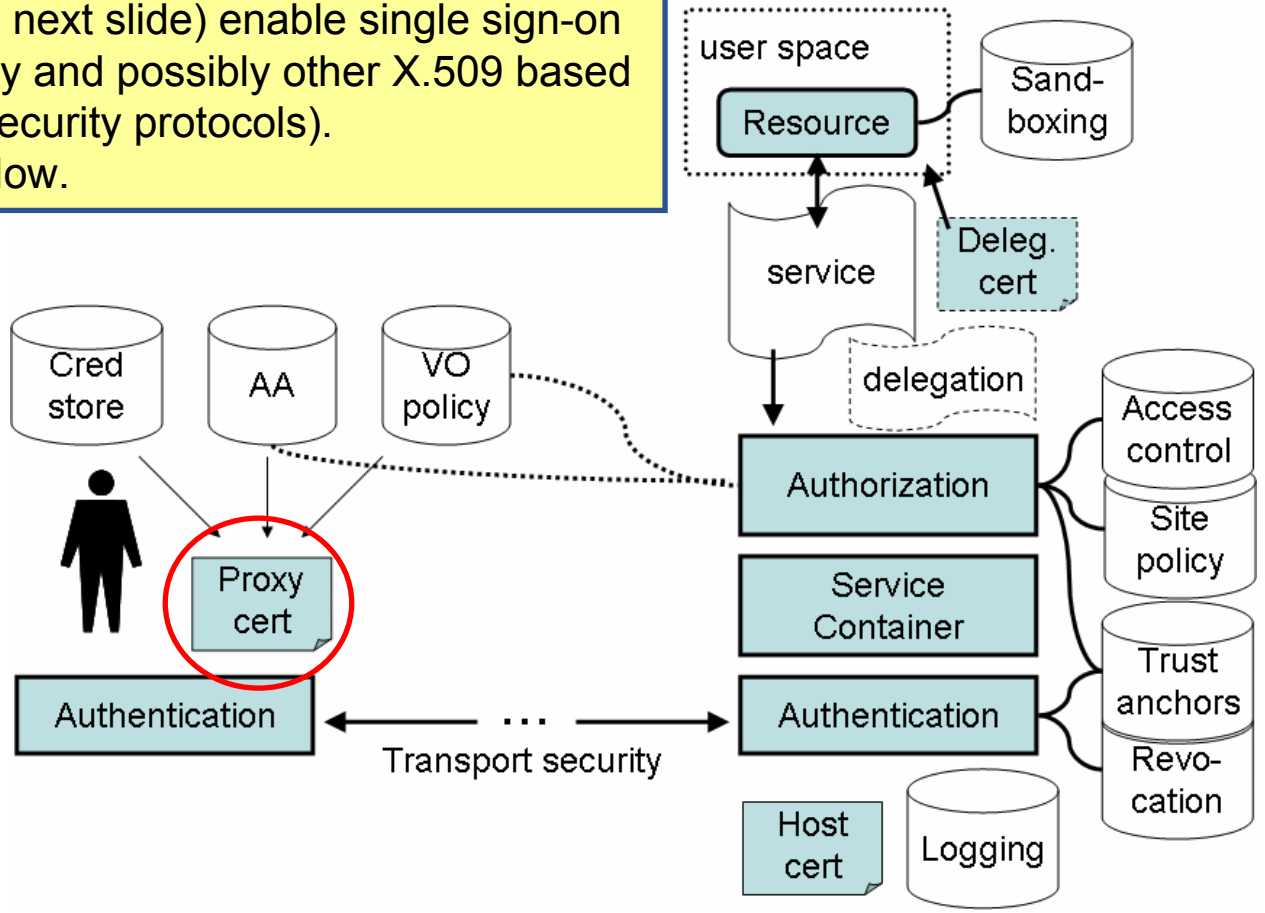
Requirement: Audit ability
Solution: Meaningful log information. Logging and auditing ensures monitoring of system activities, and accountability in case of a security event
Fulfilled/Time frame: Partially/Now



Requirement:. Accountability
Solution: All relevant system interactions can be traced back to a user
Fulfilled/Time frame: Yes/Now

Services - Authentication

Requirement: Single sign-on.
Solution: Proxy certificates and a global authentication infrastructure (**EUGridPMA** - next slide) enable single sign-on (using TLS, GSI, WS-Security and possibly other X.509 based transport or message-level security protocols).
Fulfilled/Time frame: Yes/Now.

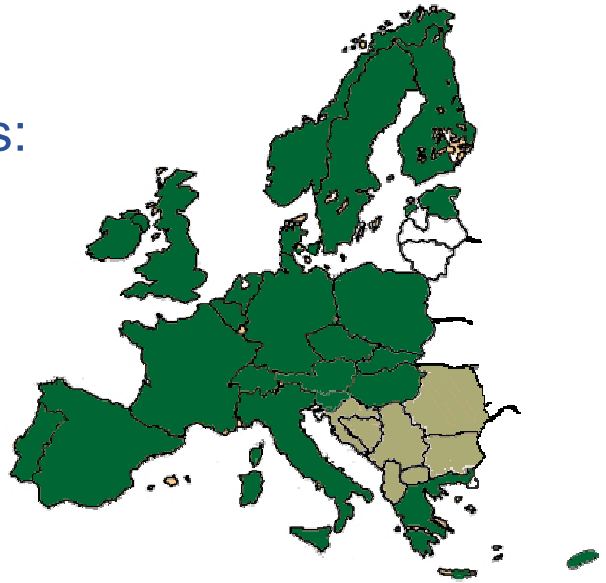


Global authentication infrastructure

EUGridPMA (Chair: David Groep, JRA3)

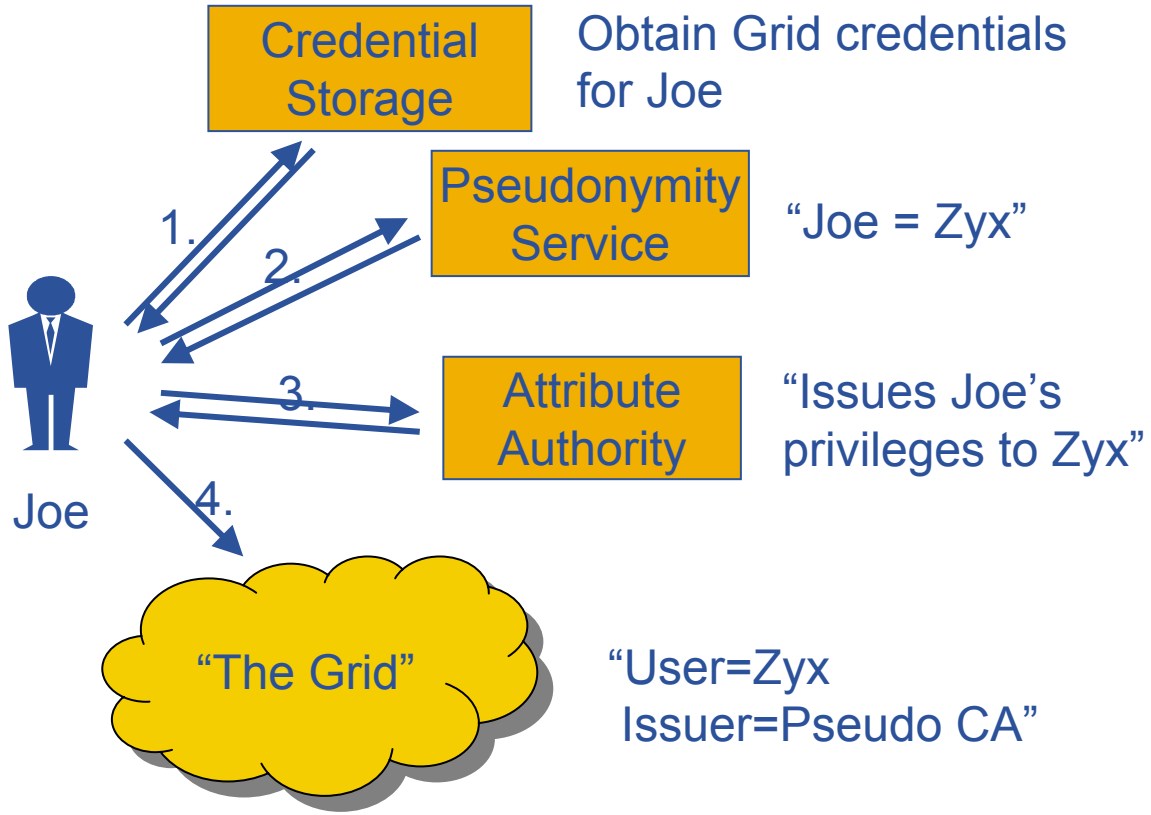
European **Grid** Authentication **P**olicy
Management **A**uthority for e-Science

- Setting **guidelines and minimum requirements** for Grid authentication for e-Science
- Now a Global federation of grid identity providers, based on EUGridPMA requirements: **the International Grid Federation (IGF)**
- **EUGridPMA was the driving example** for similar groups in Asian-Pacific and the Americas
- Coverage of Europe almost complete
  - **30 accredited members**
  - 7 non-EU countries + 1 treaty organization
- **Initiative strongly encouraged by the eInfrastructures Reflection Group (eIRG)**



Services - Authentication

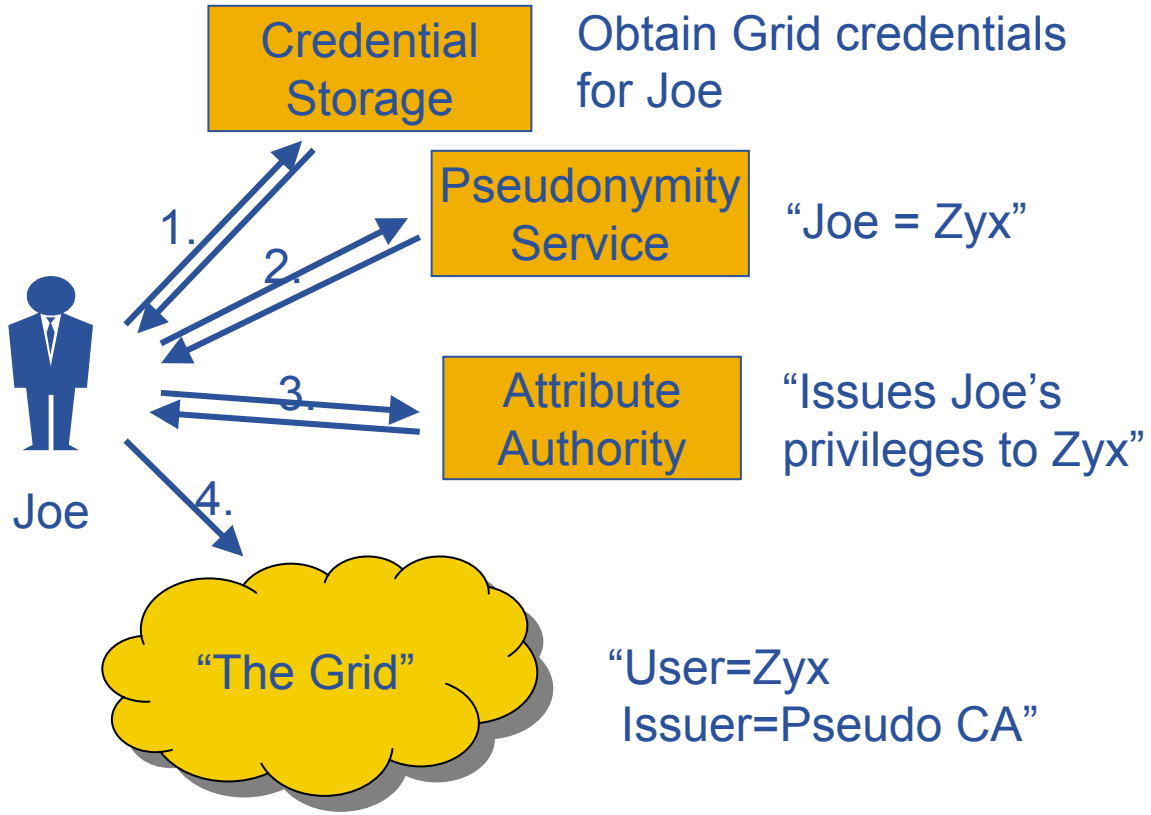
Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
Fulfilled/Time frame: Partially/Mid-term



Services - Authentication

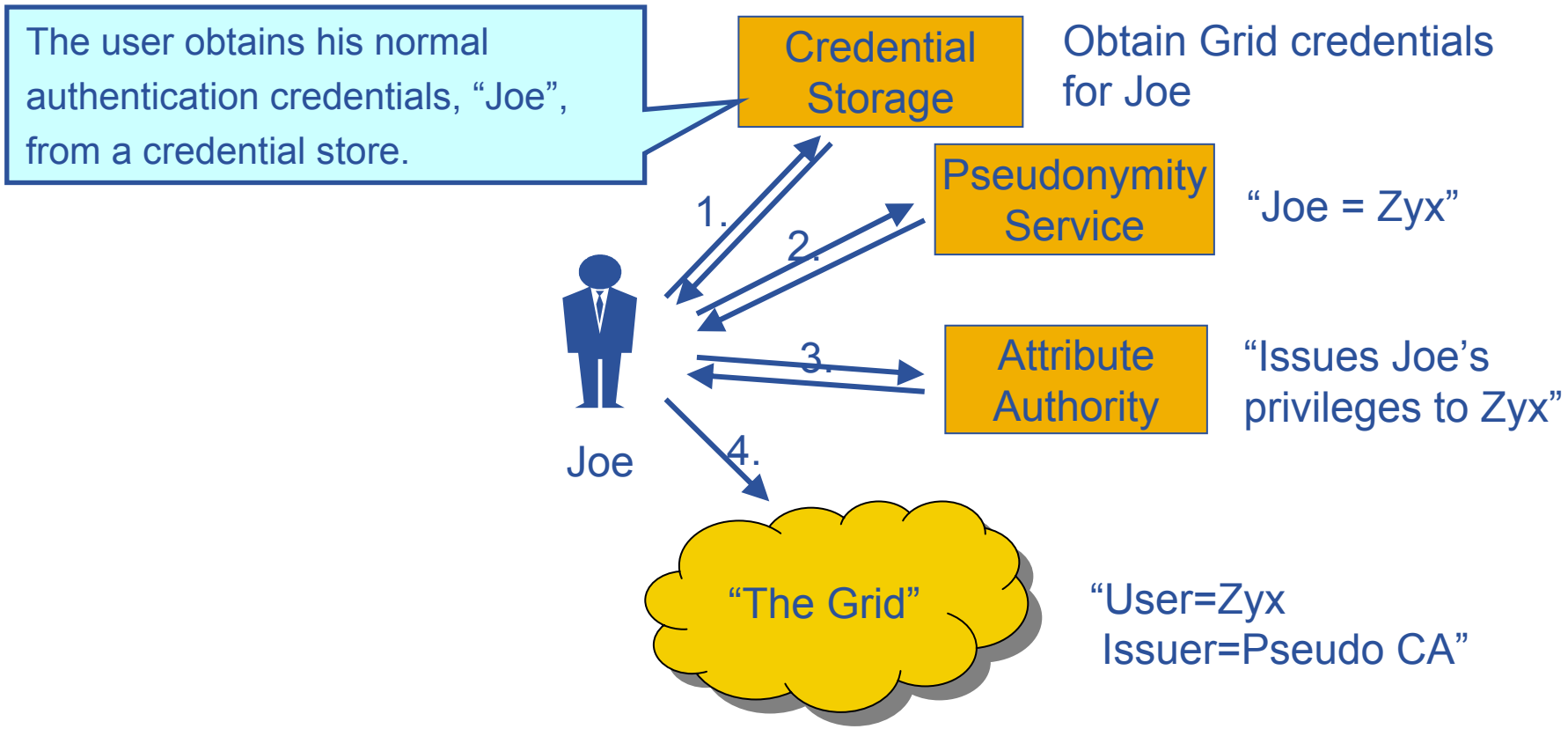
Requirement: Us identity traceability
Solution: Pseud d privacy concerns.
Fulfilled/Time fra

Challenging security requirement from applications



Services - Authentication

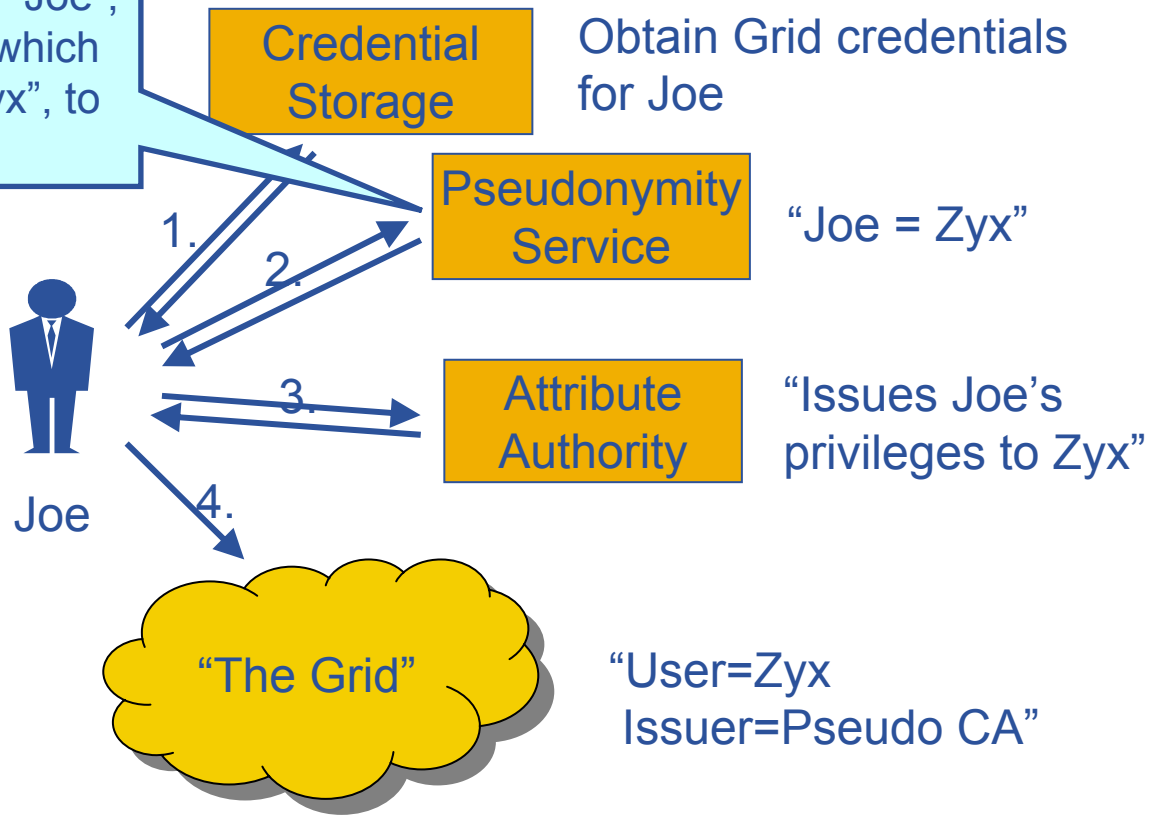
Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
Fulfilled/Time frame: Partially/Mid-term



Services - Authentication

Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
Fulfilled/Time frame: Partially/Mid-term

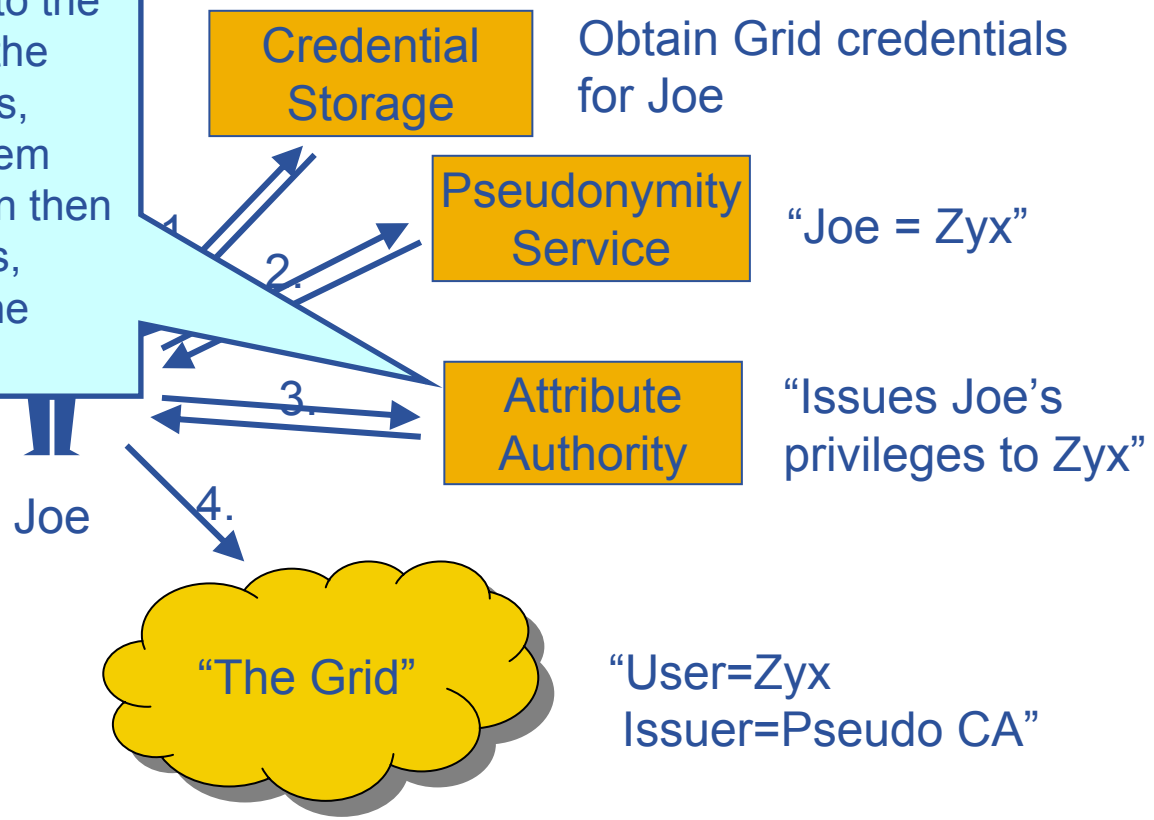
The user authenticates, using "Joe", to the pseudonymity service, which issues a one-time identity, "Zyx", to the user.



Services - Authentication

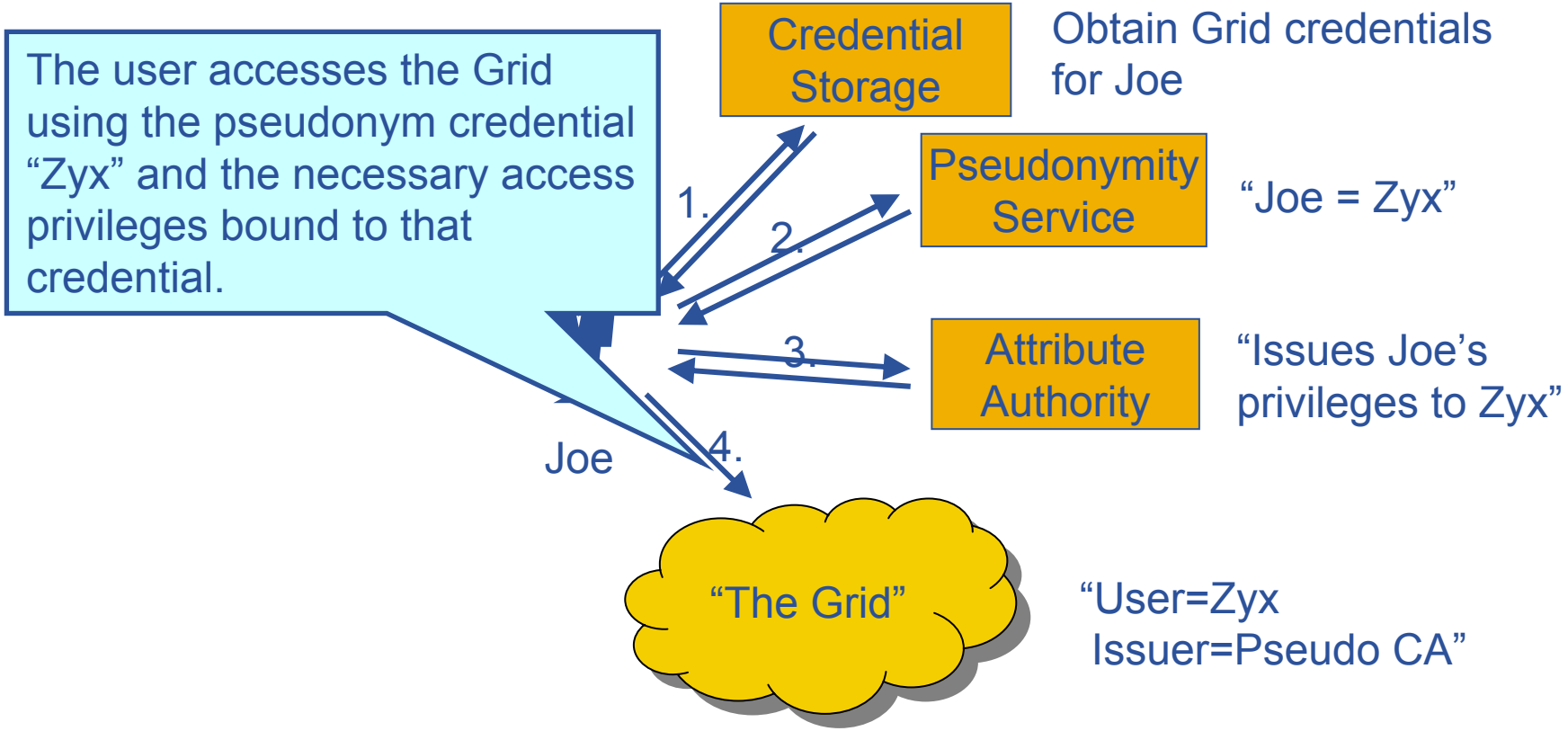
Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
Fulfilled/Time frame: Partially/Mid-term

The user authenticates twice to the attribute authority using both the "Joe" and the "Zyx" credentials, thus proving possession of them both. The attribute autority can then bind the autorization attributes, originally issued to "Joe", to the one-time identity, "Zyx".



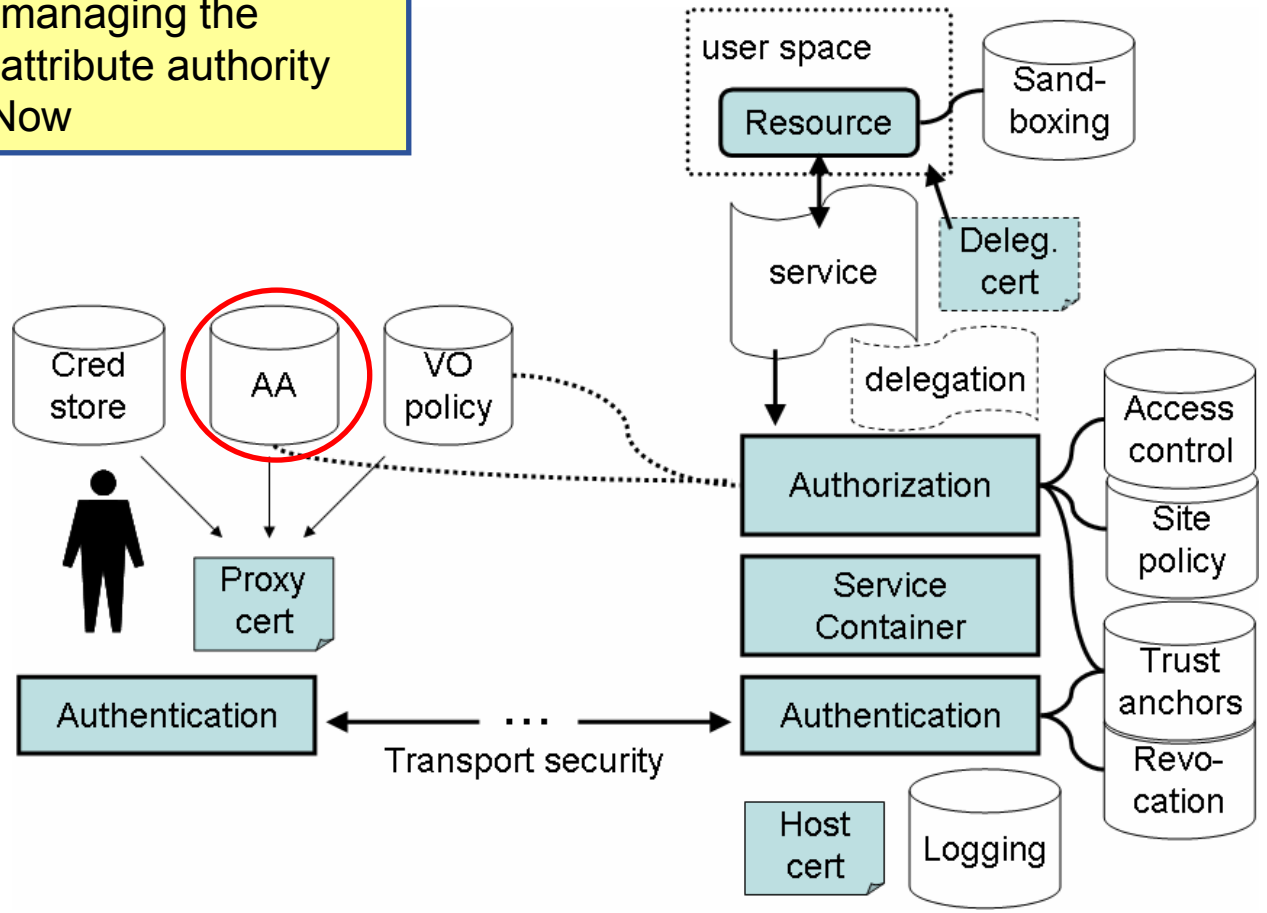
Services - Authentication

Requirement: User Privacy. **Issue:** Identity anonymity vs. identity traceability
Solution: Pseudonymity services addresses anonymity and privacy concerns.
Fulfilled/Time frame: Partially/Mid-term



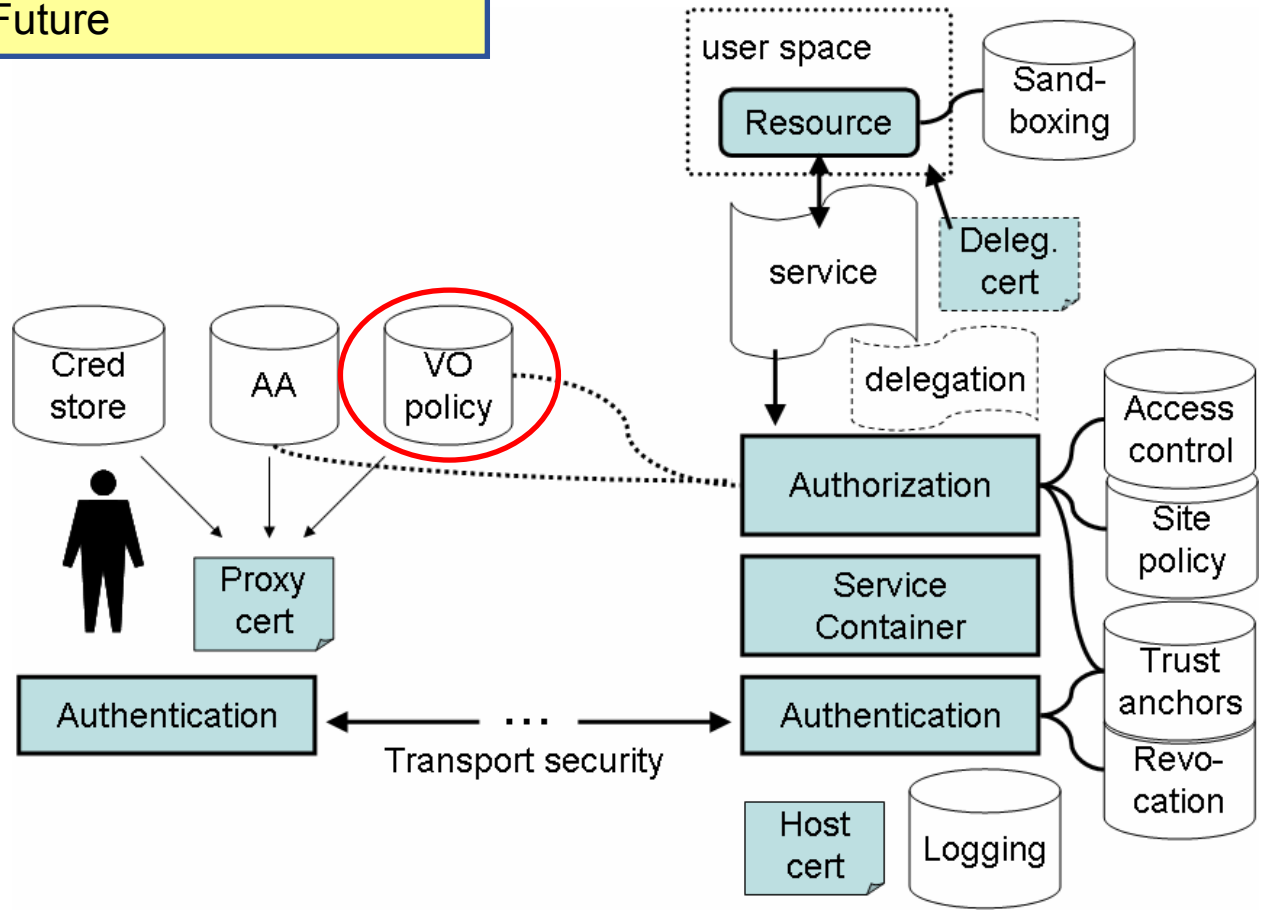
Services - Authorization

Requirement: VO managed access control
Solution: The Virtual Organization Membership Service (VOMS) is used for managing the membership to VOs and as attribute authority
Fulfilled/Time frame: Yes/Now



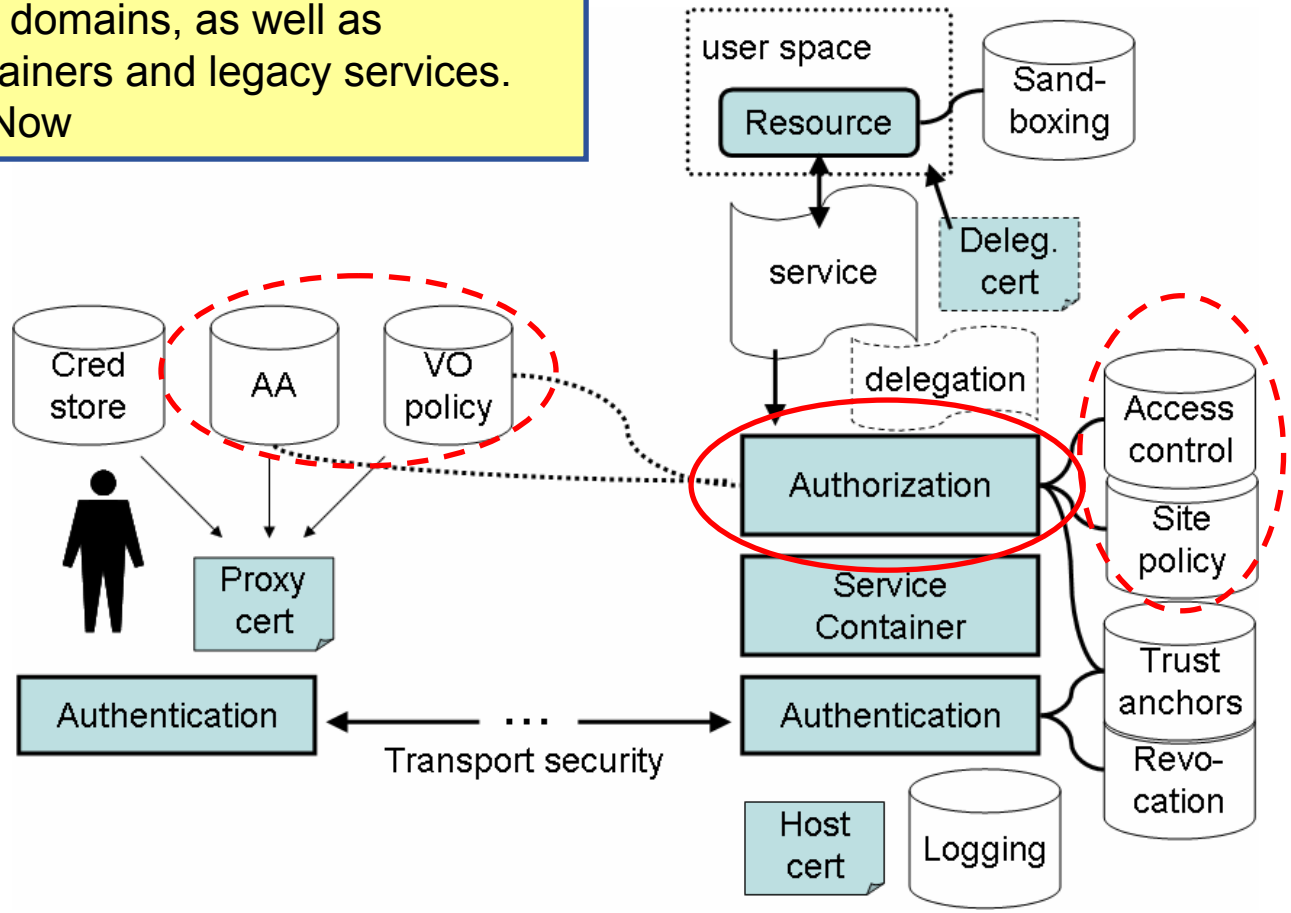
Services - Authorization

Policy assertion services enable the consolidation and central administration of common policy
Fulfilled/Time frame: Yes/Future



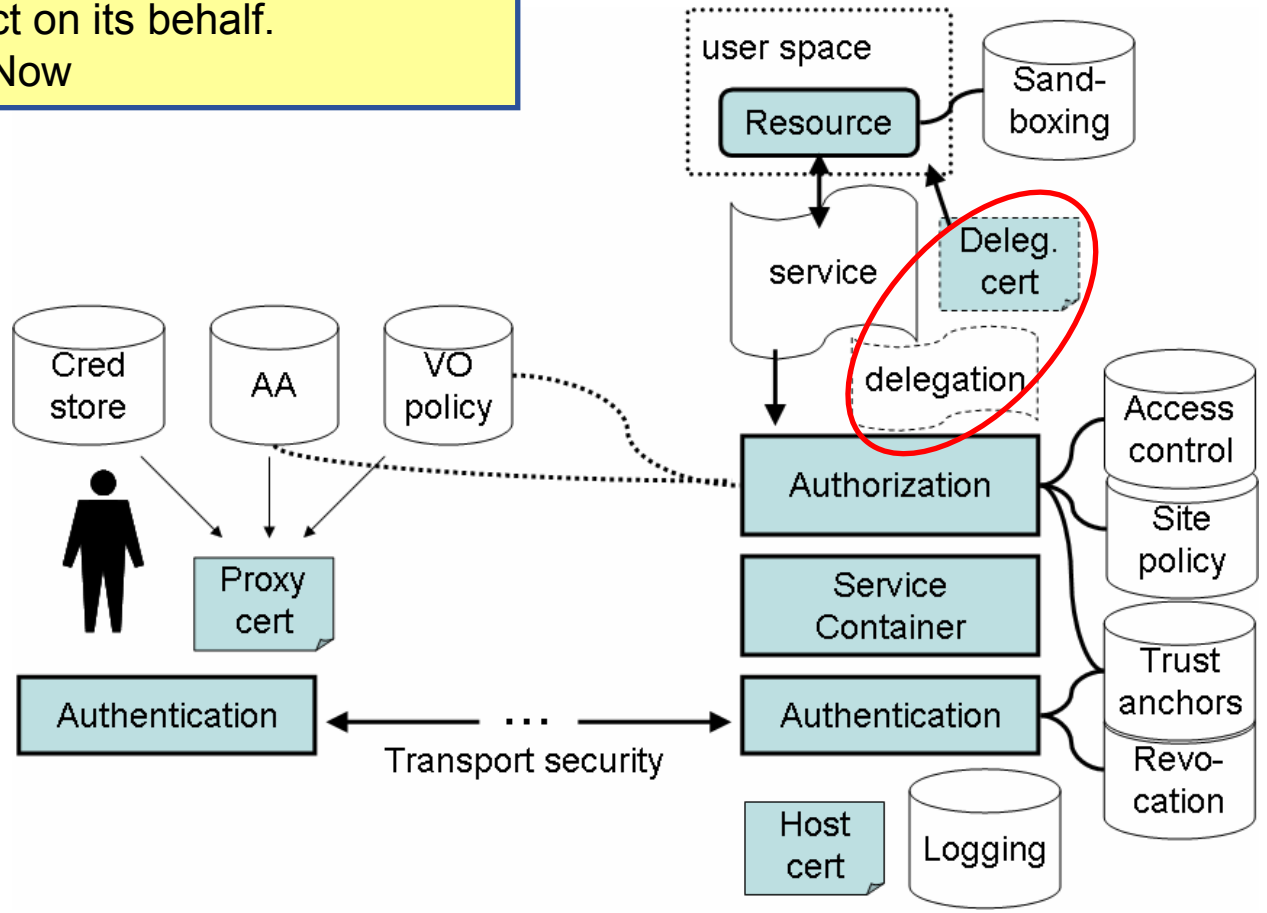
Services - Authorization

Authorization framework enables local collection, arbitration, customization and reasoning of policies from different administrative domains, as well as integration with service containers and legacy services.
Fulfilled/Time frame: Yes/Now



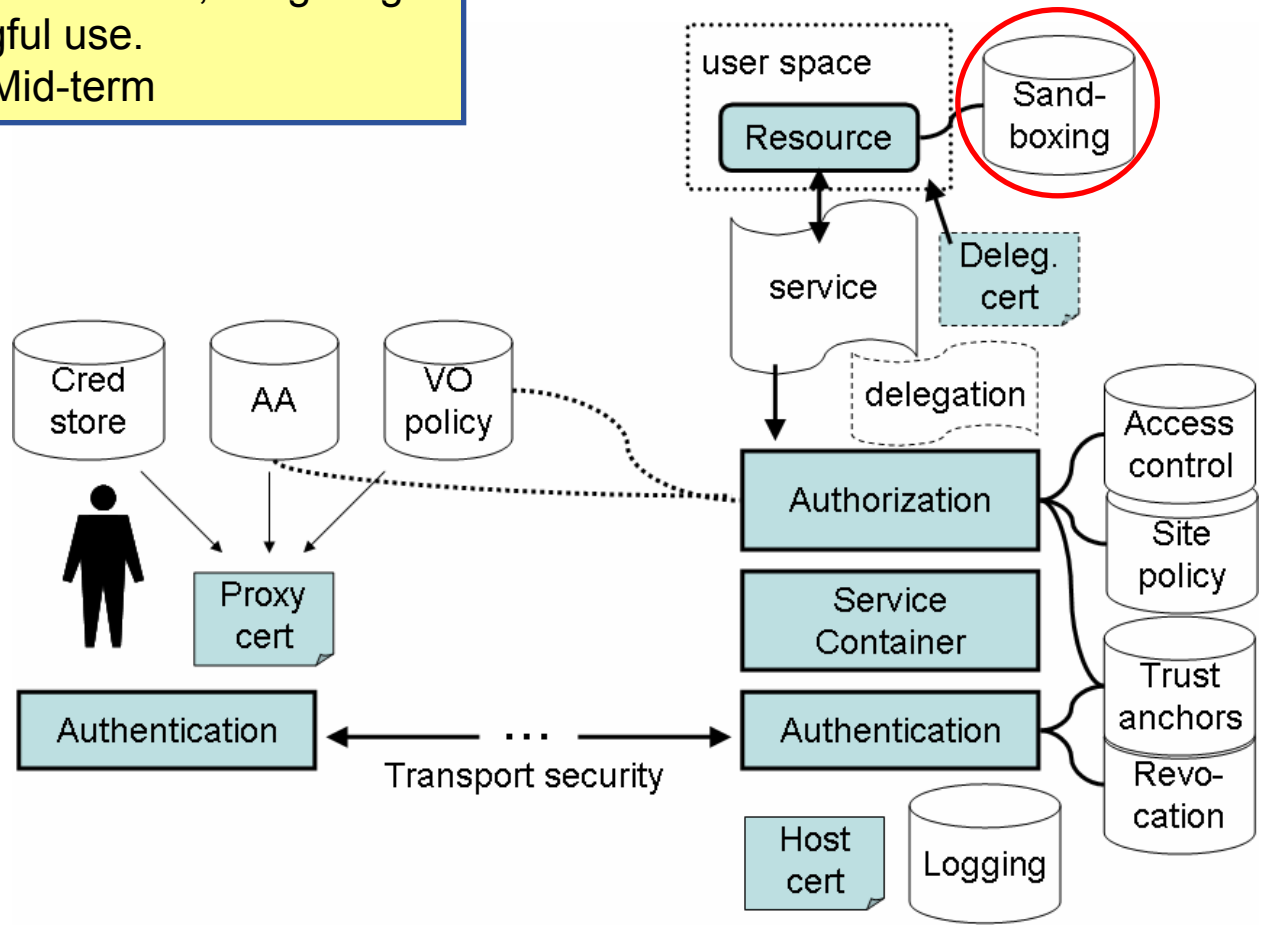
Services - Delegation

Delegation - Allows for an entity (user or resource) to empower another entity (local or remote) with the necessary permissions to act on its behalf.
Fulfilled/Time frame: Yes/Now



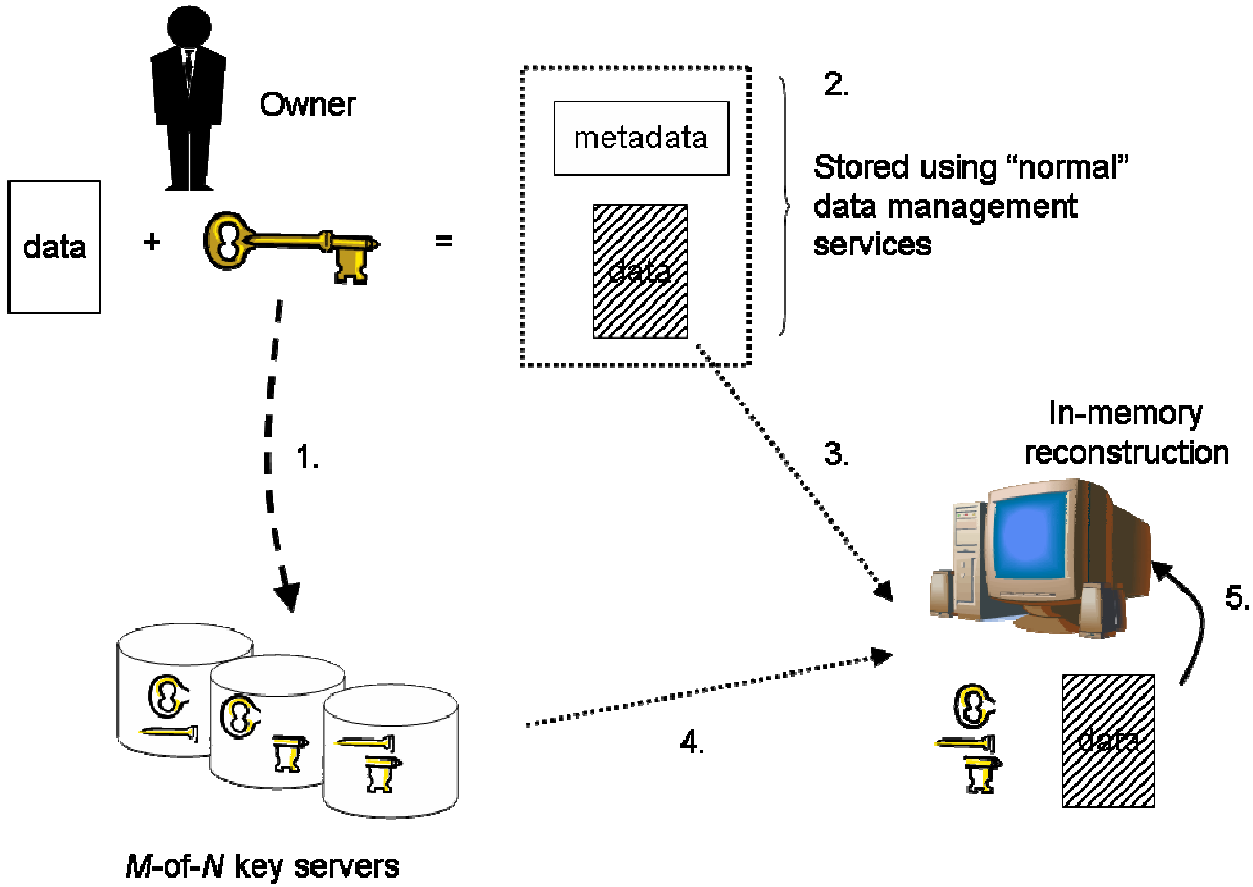
Services - Sandboxing

Sandboxing - Isolates a resource from the local site infrastructure hosting the resource, mitigating attacks and malicious/wrongful use.
Fulfilled/Time frame: Yes/Mid-term



Services - Data Key Management

Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
Fulfilled/Time frame: Partially/Mid-term

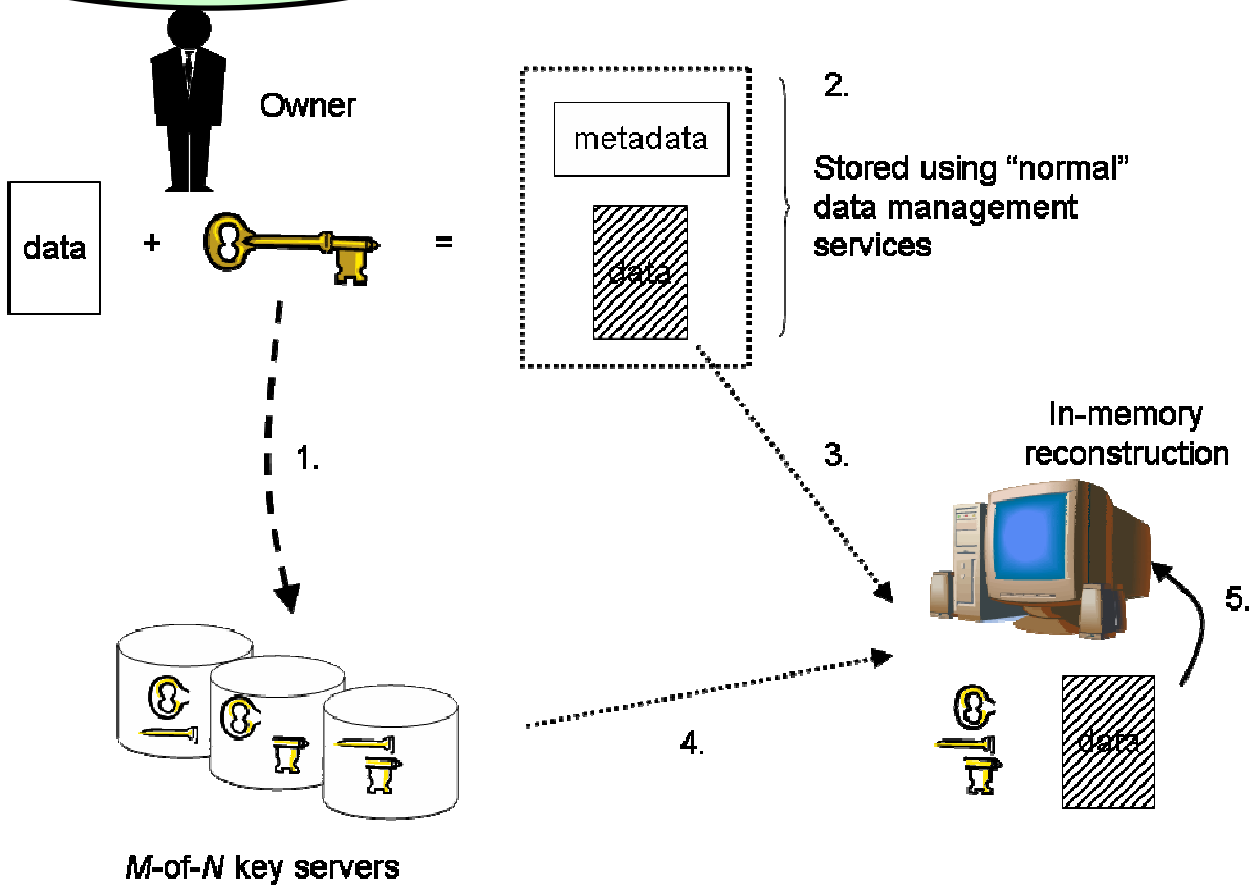


Services - Data Key Management

Requirement:
Solution: En… storage of dat…
Fulfilled/Time fra…

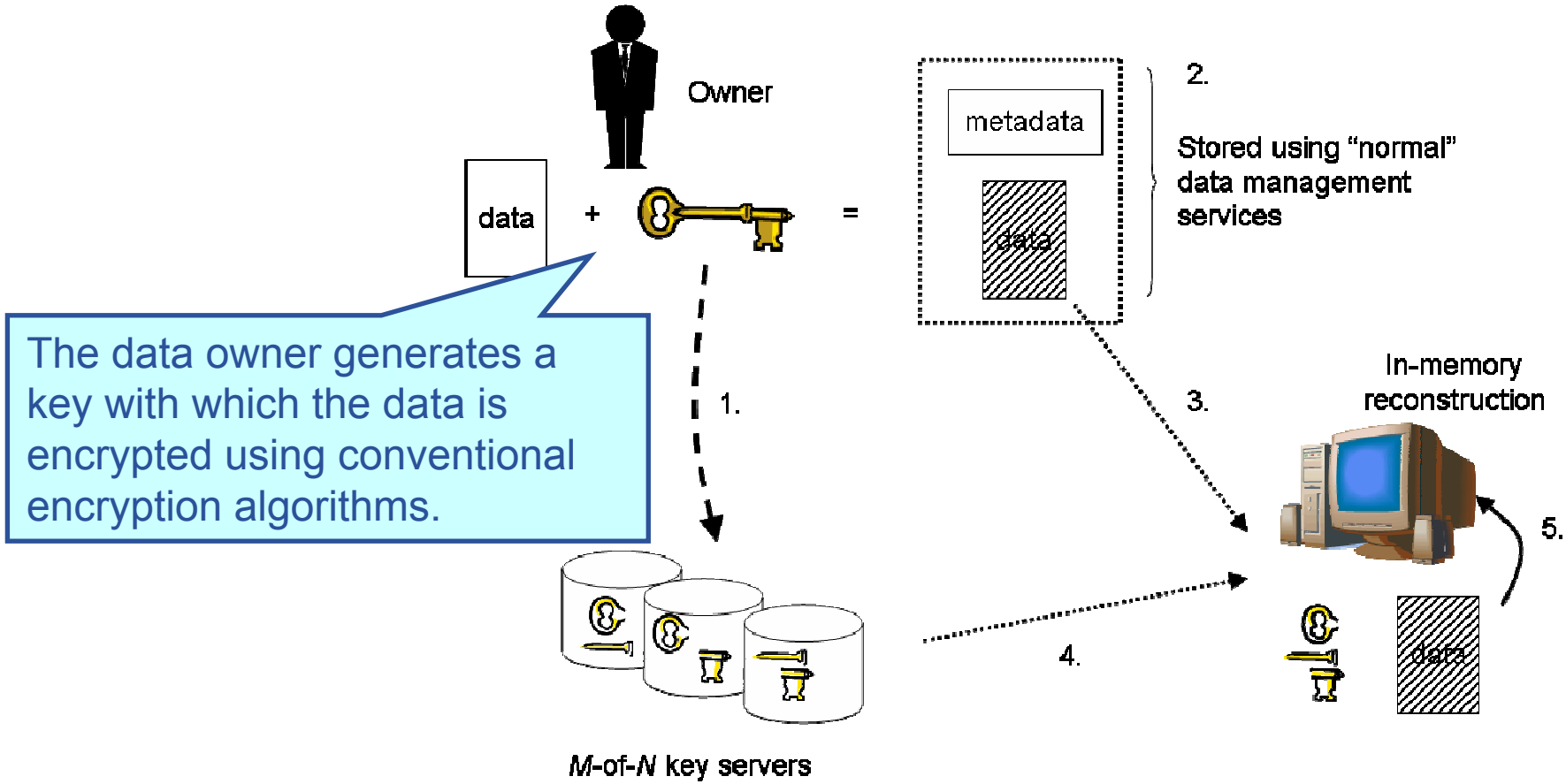
…istributed
…ntiality concerns

Challenging security requirement from applications



Services - Data Key Management

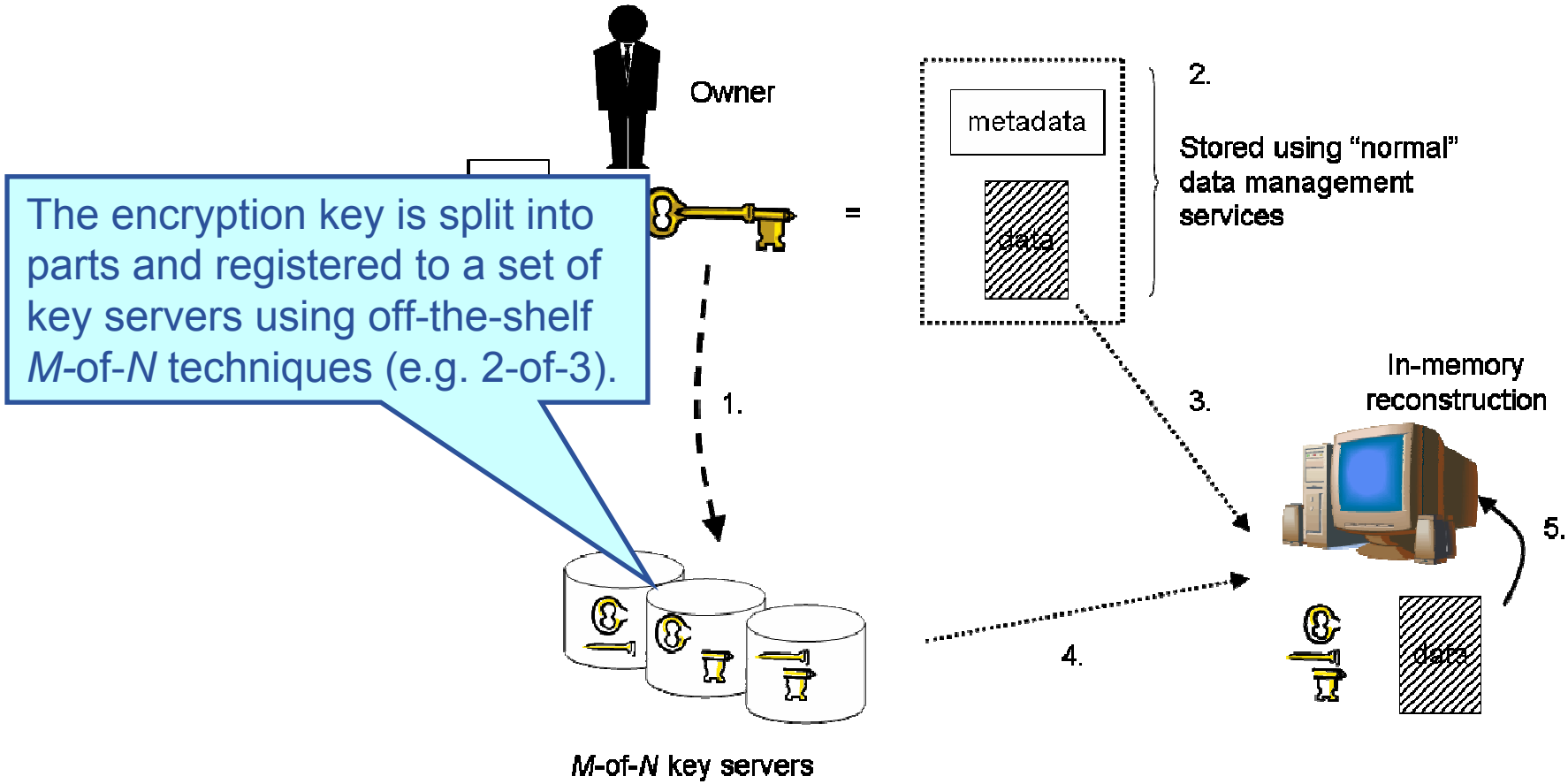
Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
Fulfilled/Time frame: Partially/Mid-term



The data owner generates a key with which the data is encrypted using conventional encryption algorithms.

Services - Data Key Management

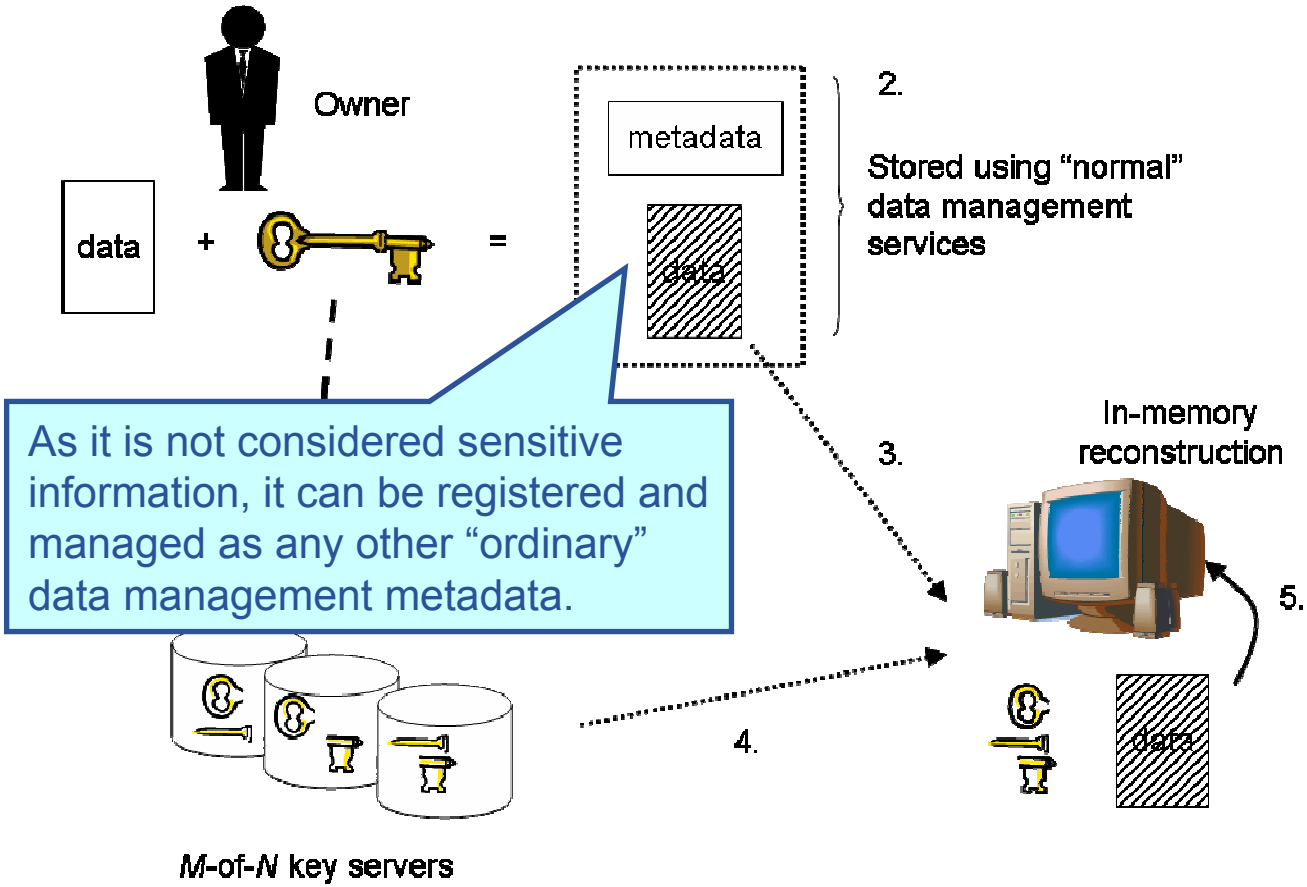
Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
Fulfilled/Time frame: Partially/Mid-term



The encryption key is split into parts and registered to a set of key servers using off-the-shelf *M*-of-*N* techniques (e.g. 2-of-3).

Services - Data Key Management

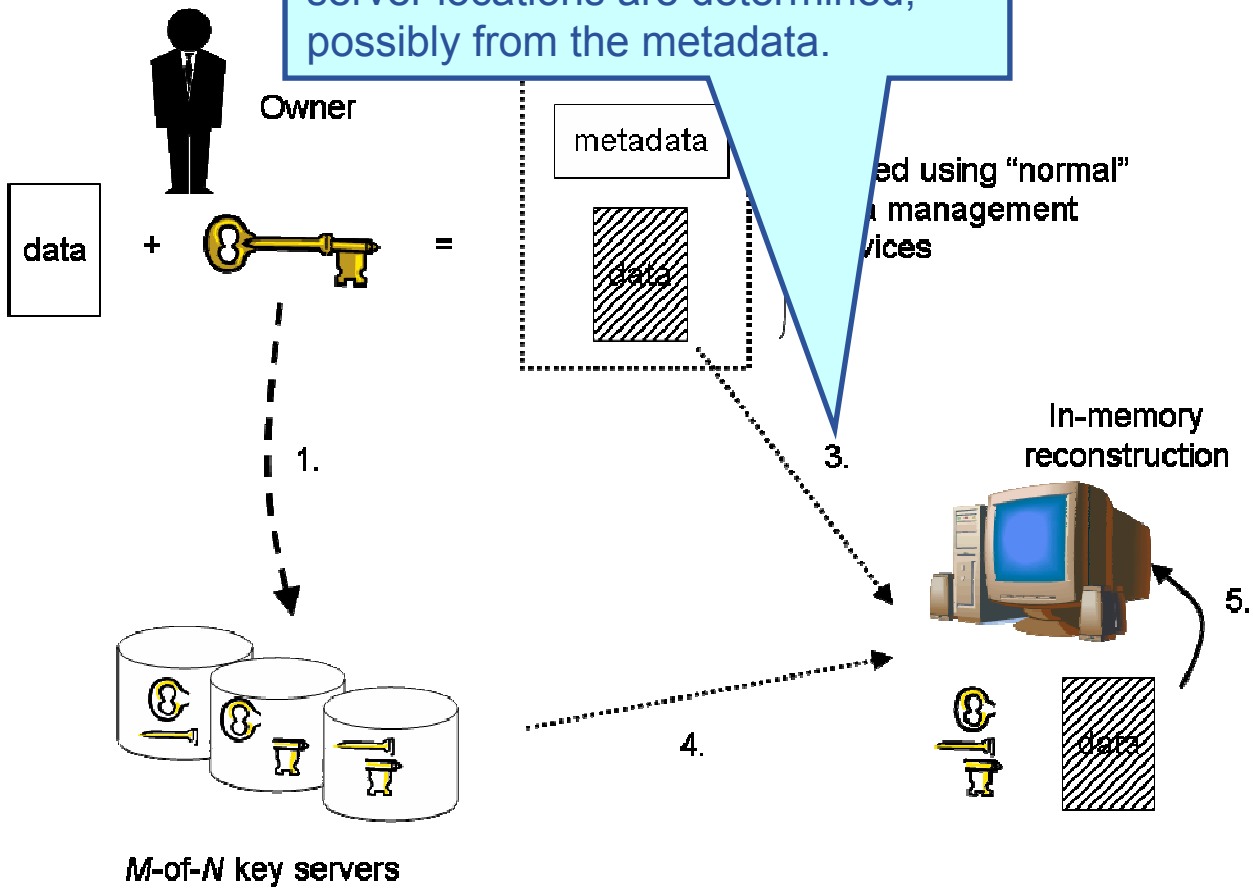
Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
Fulfilled/Time frame: Partially/Mid-term



Services - Data Key Management

Requirement: Data Privacy
Solution: Encrypted data storage.Ena
storage of data for applications with pr
Fulfilled/Time frame: Partially/Mid-te

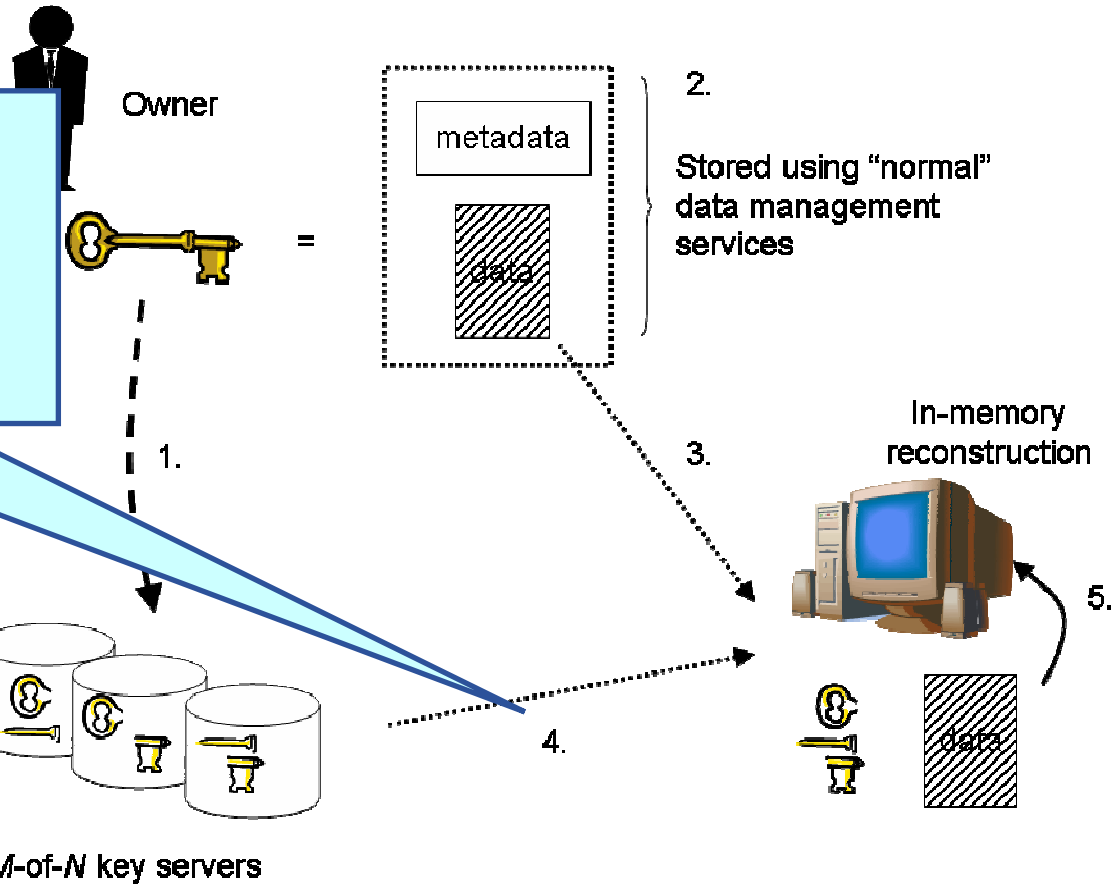
When reconstructing, a copy of the encrypted long-term storage data is retrieved using the standard data management services. The key server locations are determined, possibly from the metadata.



Services - Data Key Management

Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-term distributed storage of data for applications with privacy or confidentiality concerns
Fulfilled/Time frame: Partially/Mid-term

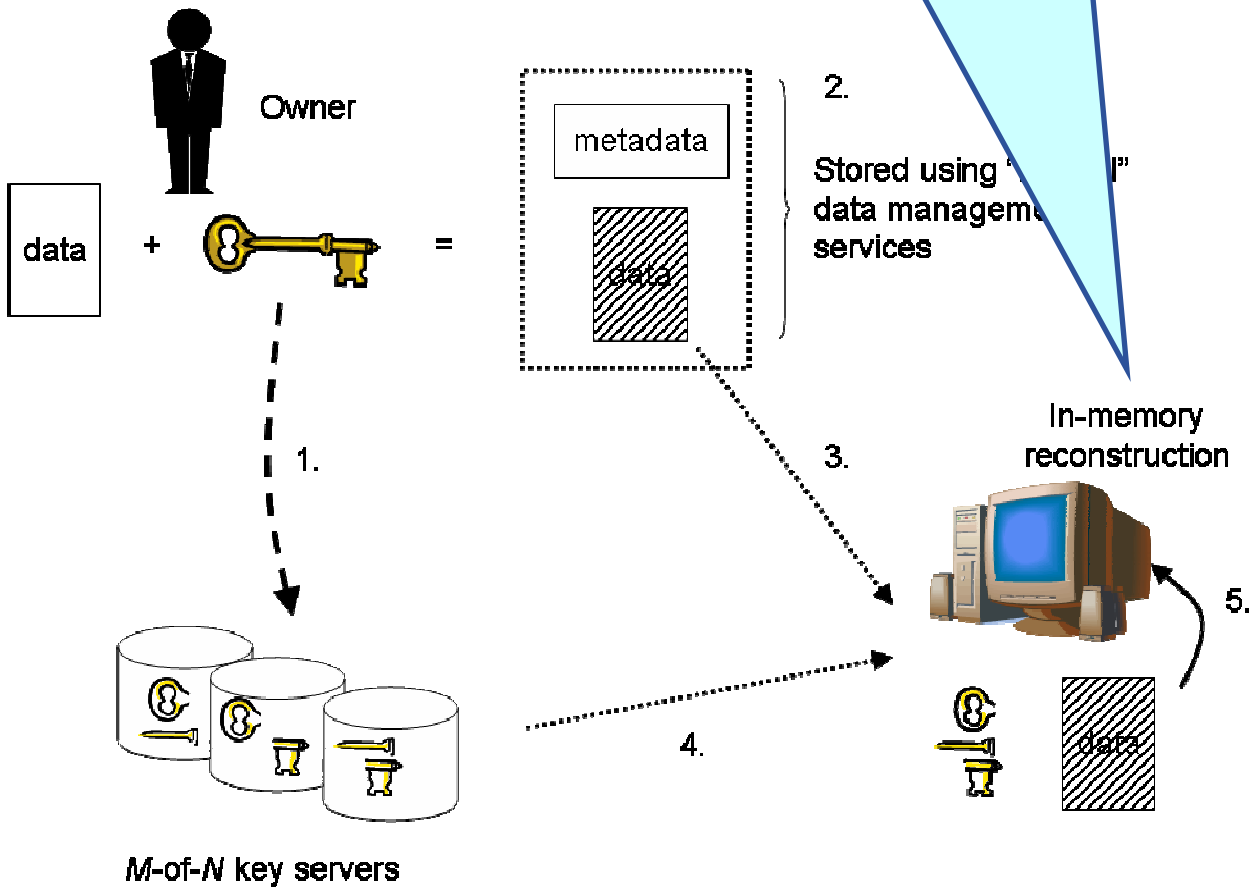
A process authenticates (using delegated credentials with the proper authorization attributes) to the key servers and reconstructs the original encryption key in runtime memory.



Services - Data Key Management

Requirement: Data Privacy
Solution: Encrypted data storage.Enables long-t
storage of data for applications with privacy or co
Fulfilled/Time frame: Partially/Mid-term

The data is decrypted into plaintext in local memory, or possibly onto a temporary file on local disk.



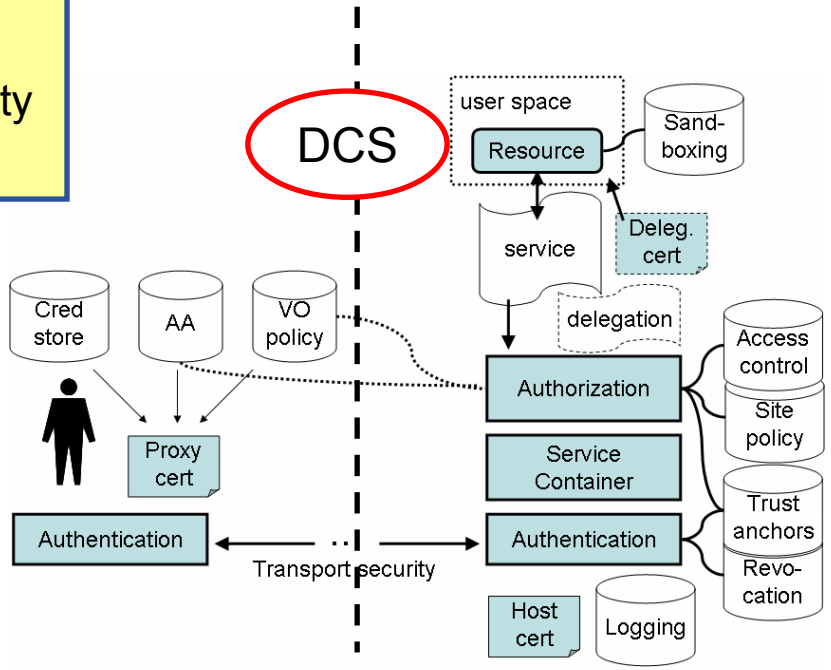
Services - Dynamic Connectivity Service

Requirement: Non-homogenous network access

Issue: Conflicting requirements:

Sites: ‘worker nodes’ shall have no global connectivity

Apps: ‘worker nodes’ must have global connectivity



Solution, security-wise: Enables applications to communicate despite heterogeneous and non-transparent network access:

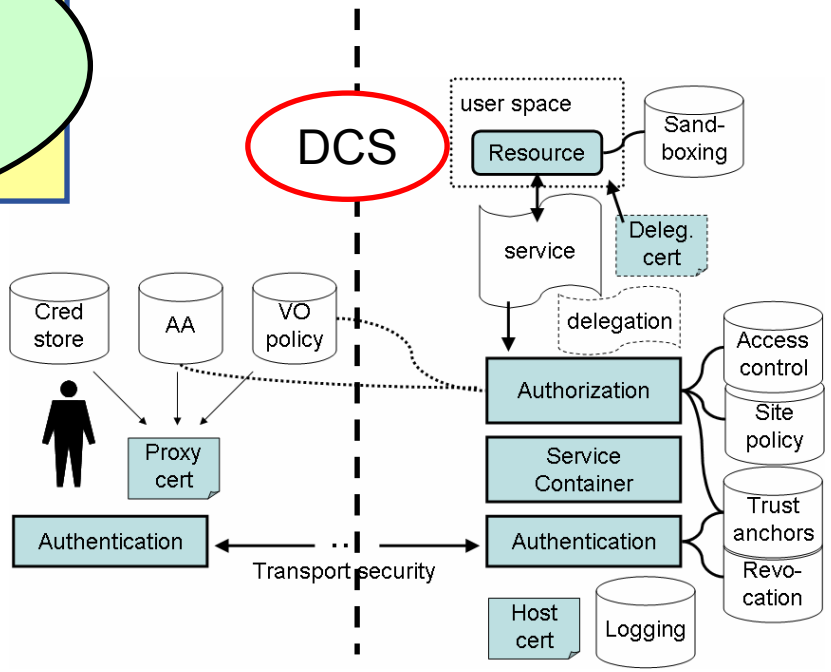
- Policy-controlled connections to the outside world
- Compliant to work in JRA4

Fulfilled/Time frame: Yes/Future

Services - Dynamic Connectivity Service

Requirement: No
Issue: Conflicti
Sites: 'worker n
Apps: 'worker node

Challenging security requirement from applications

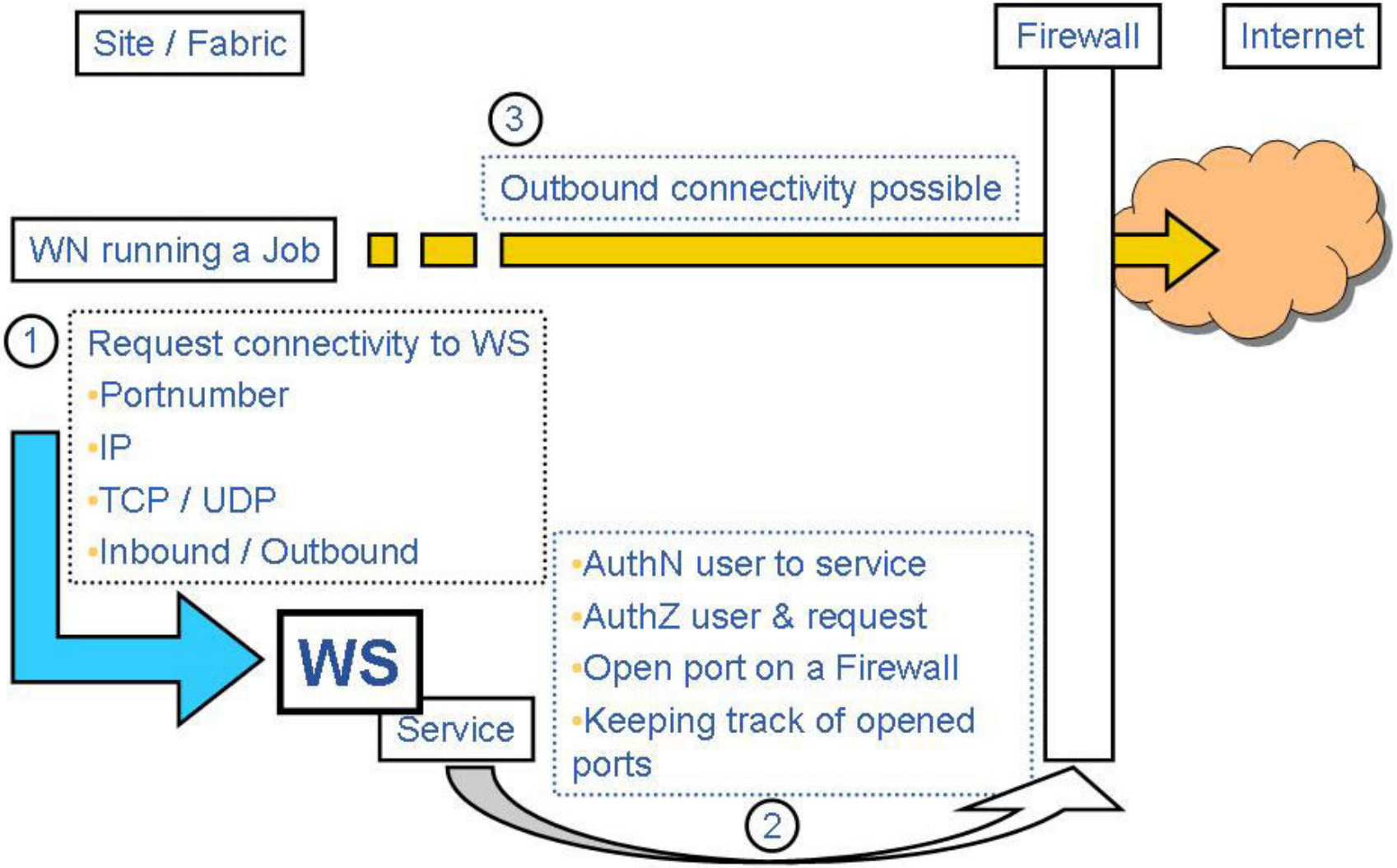


Solution, security-wise: Enables applications to communicate despite heterogeneous and non-transparent network access:

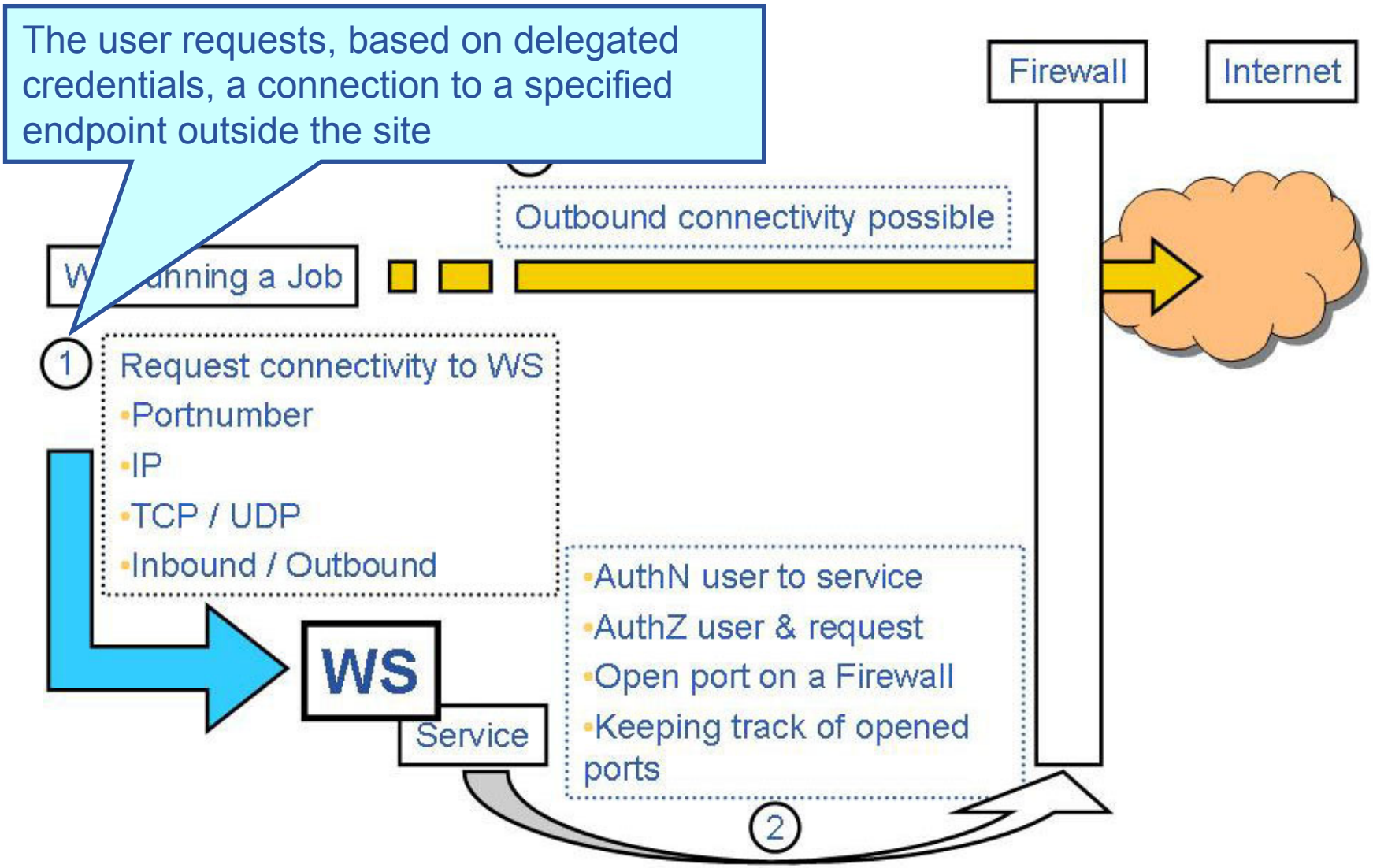
- Policy-controlled connections to the outside world
- Compliant to work in JRA4

Fulfilled/Time frame: Yes/Future

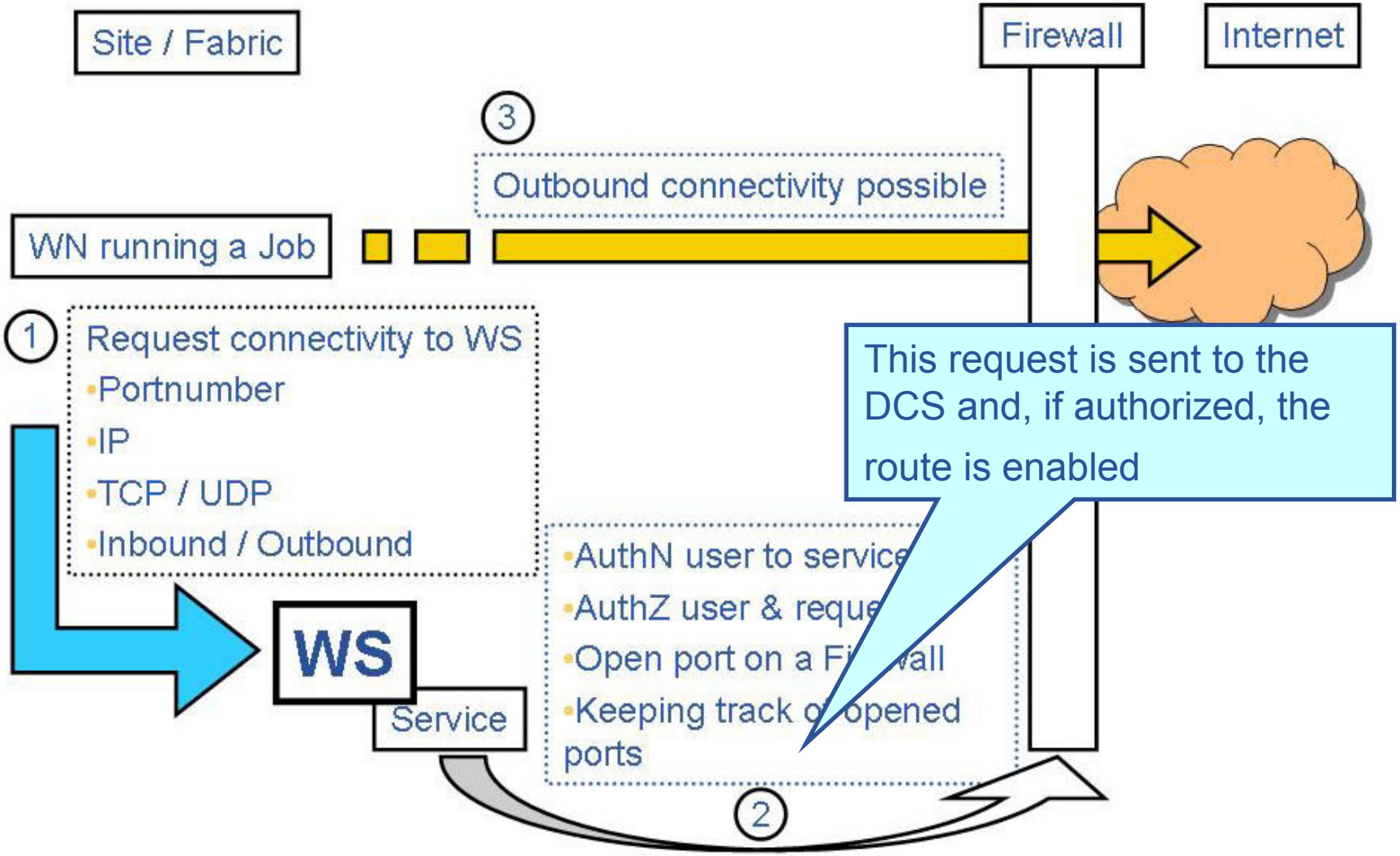
Services - DCS (Getting outbound connectivity from a Worker Node)



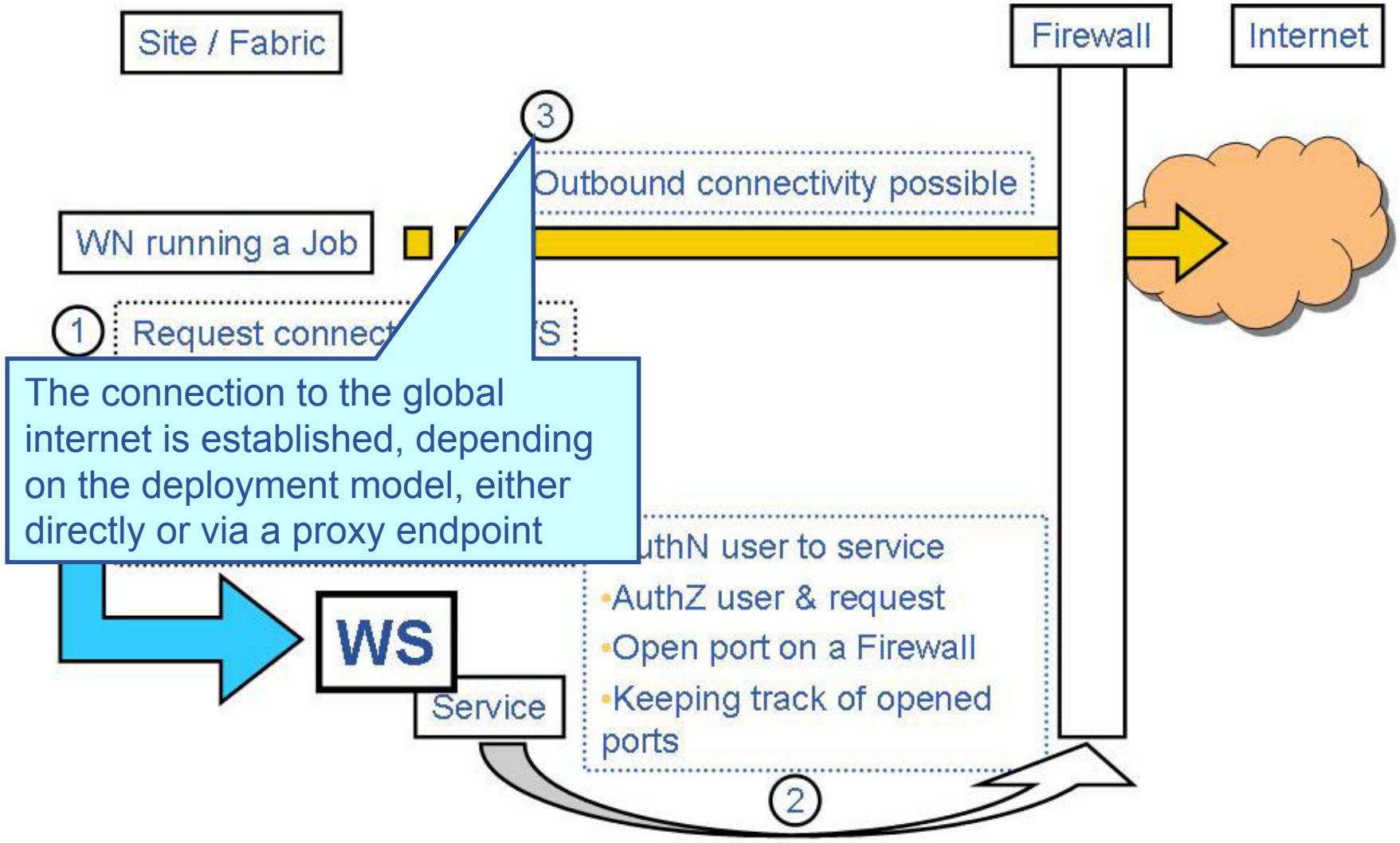
Services - DCS (Getting outbound connectivity from a Worker Node)



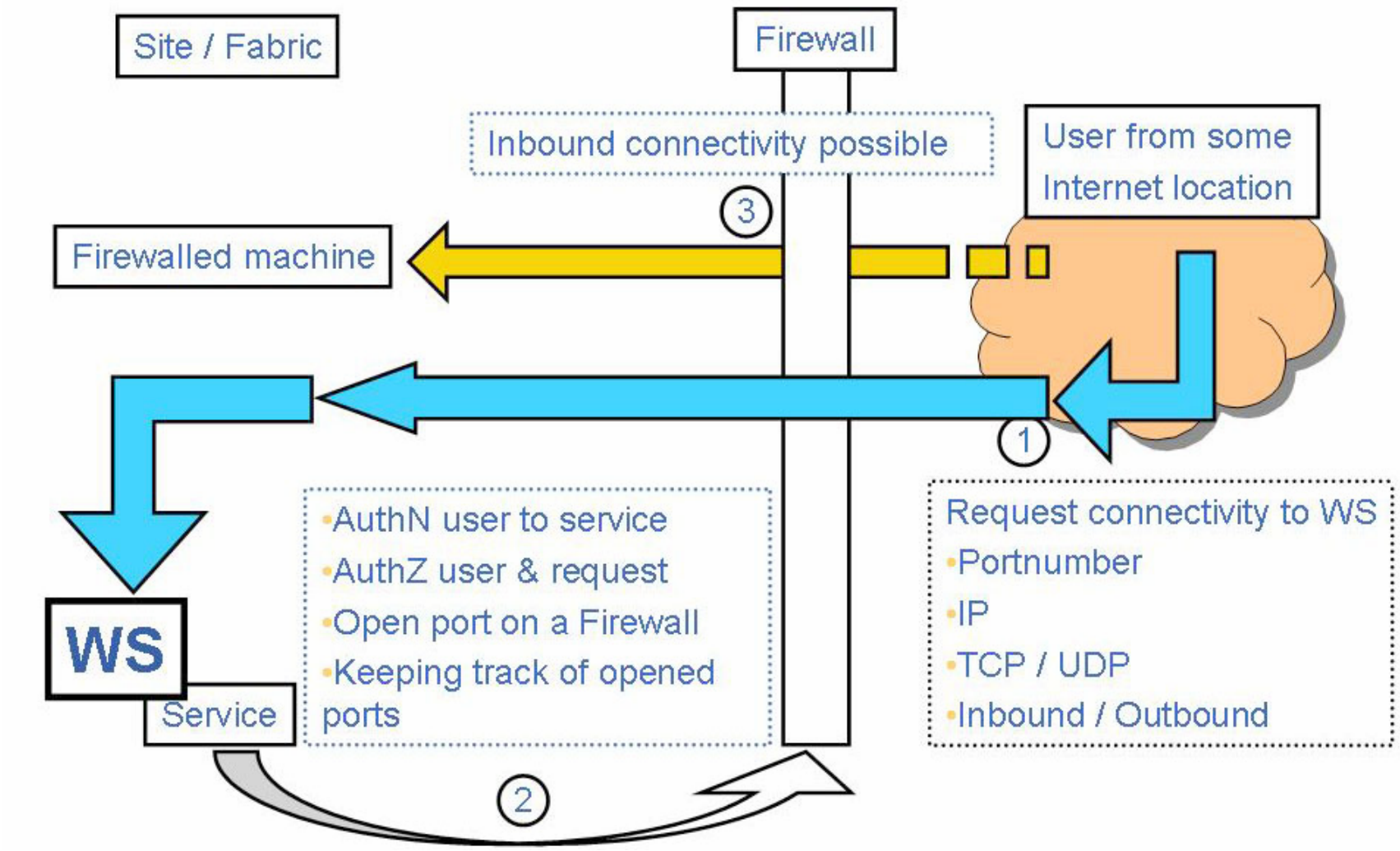
Services - DCS (Getting outbound connectivity from a Worker Node)



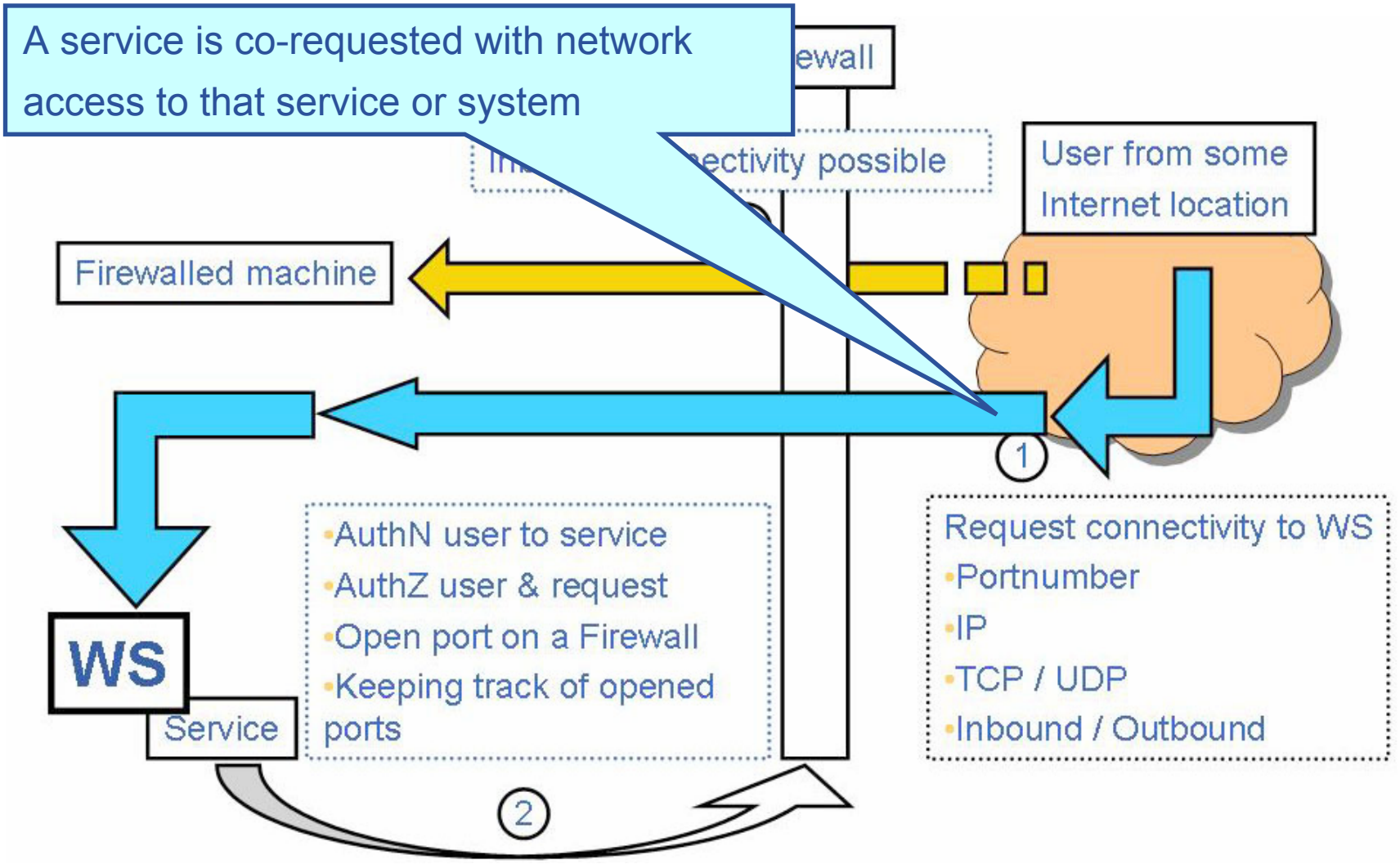
Services - DCS (Getting outbound connectivity from a Worker Node)



Services - DCS (Getting inbound connectivity from outside the site to a site-local service)

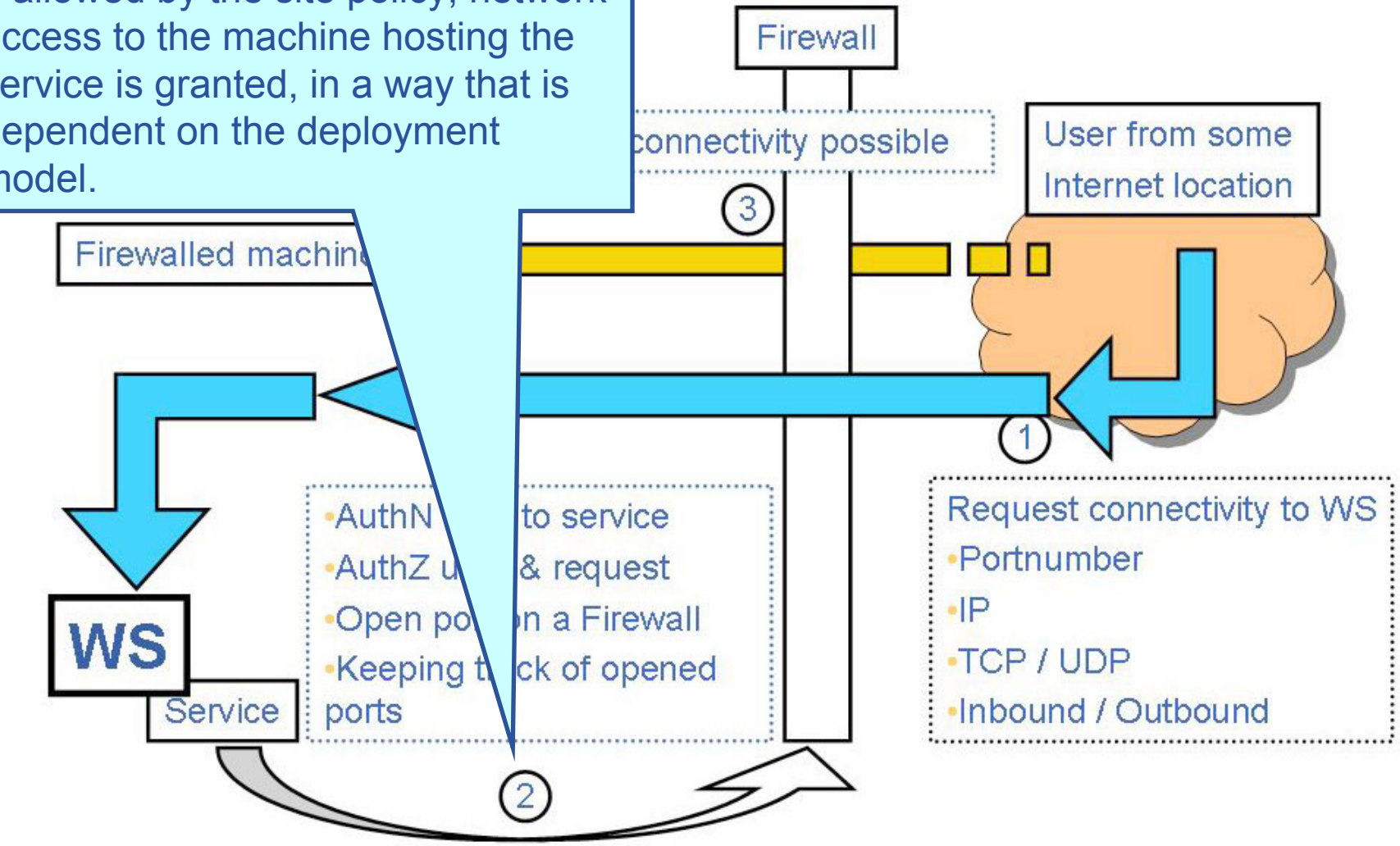


Services - DCS (Getting inbound connectivity from outside the site to a site-local service)

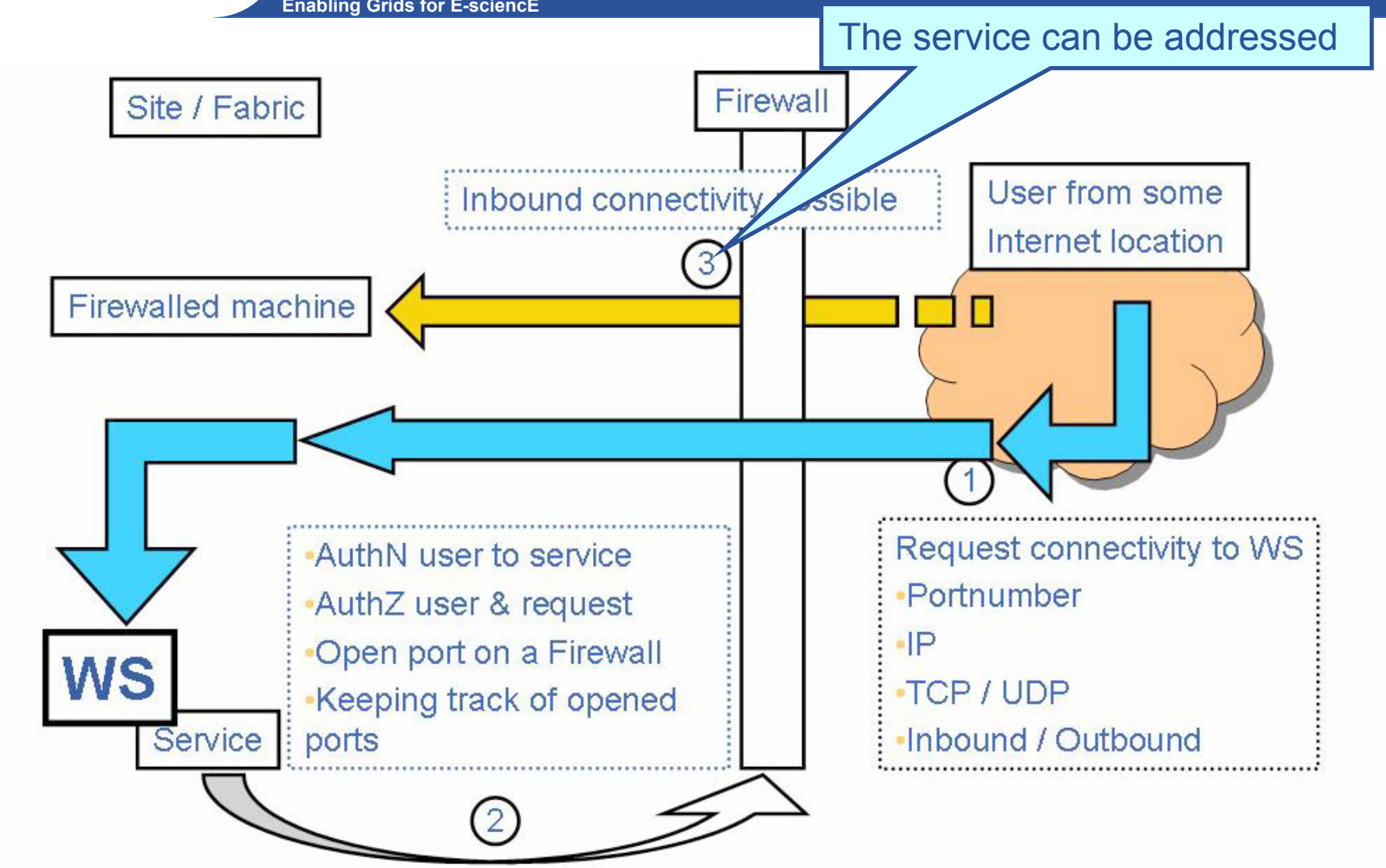


Services - DCS (Getting inbound connectivity from outside the site to a site-local service)

If allowed by the site policy, network access to the machine hosting the service is granted, in a way that is dependent on the deployment model.



Services - DCS (Getting inbound connectivity from outside the site to a site-local service)



Integration and development

- JRA3 is, from start of the project, part of the JRA1 development - as the Northern Cluster.
- All software development at JRA3 follows the processes of JRA1.
- See previous presentation from JRA1.

Plans and status - gLite release 1

Module candiates for gLite release 1:

- **SOAP over HTTPS**
  - Implements transport layer security for web services.
- **Authorization framework**
  - A java rendering of the pluggable authorization framework
- **VOMS support for authorization**
  - The Virtual Organization Membership Service (VOMS) is used for managing the membership to VOs and as attribute authority.
- **Resource Access Control (LCAS, LCMAPS, gatekeeper)**
  - Resource access control is based on Local Centre AuthZ Service (LCAS) and Local Credential MAPping Service (LCMAPS). The Globus WorkSpace Service (WSS) is used for account management.

Plans and status – Later releases of gLite

- **Ready for later releases of gLite:**
  - Message level security
  - Delegation
  - Grid enhancements for OpenSSL (part of 0.9.7/0.9.8, i.e. the Feb/March release of OpenSSL)
  - Dynamic Connectivity Service (work ongoing)

- **Updated release plan to be presented and decided at next MWSG, Feb 23-24**

- **JRA3 has also contributed in:**
  - WorkSpace Service (WSS) - a EGEE and Globus collaboration
  - Coordinating and collaborating with JRA1 security work (VOMS)
  - LCG security work (VOMS Admin)

Plans and status – Next 9 months

- PM10-12 gLite release 1
- PM12 First revision of the Security operational procedures document
- PM12 Framework for policy evaluation accepted in GridPMA policies and determination of the CA service authorities for EGEE.
- By PM12 all EU memberstates active in Grid projects will have a national accredited Authority.
- PM16 Global Security Architecture document is revised, with input from operations, applications, and external collaborating infrastructure projects.
- PM18 Second revision of the Security operational procedures document.
- PM18 A documented assessment of the work and experience gathered with the basic accounting infrastructure already deployed. To highlight what remains to be done to provide a secure, deployable quota allocations and enforcement mechanism.

Plans and status – A word on collaboration

Next period:

- JRA3 will work with GGF to define and prototype a WS proposals and standards based delegation method.
- JRA3 will lead an EU workgroup on security.
- All general security aspects will continue to be performed in collaboration with other grid initiatives such as DEISA, OSG, Diligent, NextGrid, CoreGrid, eIRG, TF-EMC2, TF-CSIRT, the Baltic states and Asian initiatives.

Summary

Top 3 achievements so far:

- Security architecture in place, minor revisions expected during the following 9 months.
- Significant contribution to EUGridPMA (chair) and standardization work (co-chair of GGF Security).
- Security components to gLite: continuous work. 4 modules in release 1.

Major Issues, and their mitigation:

- Geographically distributed teams; Mitigation: cross activity groups, more F2F meetings, esp. in the handing over of security modules.
- Conflicting/challenging security requirements from applications; Mitigation: proposed solutions meeting the requirements a much as possible.

Questions and answers

Technical questions: David Groep

Questions about the activity: Ake Edlund