



Paralleldatorcentrum

omii europe

open middleware infrastructure institute

Interoperability Security Concerns

Fredrik Hedman, KTH

February 2007

San Diego, California, USA



OMII-Europe?



Paralleldatorcentrum

- **Vision: “to provide interoperability solutions to the major e-infrastructure providers to facilitate integration of heterogeneous grid platforms”**
- **Impartial broker of interoperable grid mw: gLite, Globus, Unicore, CROWN, ...**
- **8 partners in Europe + partners in China and US**
- **New proposal coming for FP7: “more of the same”**
- **Infrastructure Integration, JRA3 (FJZ, INFN, KTH): security+interoperability**



Progress...



Paralleldatorcentrum

Definition of a common security technology base:

- CSI synopsis + document 0.1.3 +HPCP profile
- OGSA Security Profile 1.0? (Secure Channel & Core)
- SAML 2.0

Credential provisioning in UNICORE

- Authentication: proxy X.509 verification support (solved)
- Authorization: enable VO attributes extraction & enforcement (in progress)

Credential Management for Grid Applications (starting)

- MyProxy plus VOMS as a backend
- PURSe or other portal-like web frontend
- Plugin for UNICORE GUI Client



Progress...

- Information Services (gLite, UNICORE)
- OGSA – BES
- VOMS
- Portal



Paralleldatorcentrum



Technical Challenges



Paralleldatorcentrum

Authentication & Authorization Mechanisms:

- Common authentication: solved
- Authorization mechanisms: challenge, e.g. attribute certificates

Re-Engineering:

- Evolving middleware components need to interoperate with the developed profile,
- e.g. Proxy certificates in UNICORE5, full integration of VOMS with MyProxy support and PURSe into UNICORE5/6

Credential Management

Prototype credential management system



Extension for UNICORE5



Paralleldatorcentrum

Authentication:

- **Proxy X.509 Credentials accepted at UNICORE Gateway**
- **AJO's signed by Proxy certificates processed by NJS**

Authorization:

- **VO attributes embedded within proxy certificates**
- **Extracted by NJS during UUDB authz phase**
- **Enforcement (?)**

Integration:

- **User registration through PURSe with MyProxy/VOMS backend**
- **GUI client Plugin that leverages stored credentials**



PURSe



Paralleldatorcentrum

Steps in integrating PURSe with UNICORE for User Registration

- Enhancement of Registration classes
- Enhancement of UNICORE clients

Utilization of Portlet technology

- Enhance the PURSe portlets implementation
- Integration
- Security tightdown
- Web Interface



Concerns...



Paralleldatorcentrum

- **Attribute certs (RFC 3281) into OpenSSL?**
- **Adding TLS authz to gnuTLS?**
- **XACML3.0, adding delegation?**
- **Proxy certs v.s. Explicit trust delegation?**