JRA3

Åke Edlund
On behalf of JRA3

EGEE 8th All-activity meeting
January 18-19, 2006
CERN, Switzerland

www.eu-egee.org
www.glite.org

Information Society and Media

Content

- ✓ **Outstanding work in EGEE-I**
  - ✓ Deliverables and milestones
  - ✓ gLite
- ✓ **Response to the reviewer's recommendations**

Outstanding work in EGEE-I
Deliverables and milestones

- ✓ **Deliverables**
  - ✓ DJRA3.4 (PM24-> PM22) KTH - Expected to be on time
    - ✓ Assessment of security infrastructure report
    - ✓ PM22, not PM24 as planned
- ✓ **Milestones**
  - ✓ MJRA3.10 (PM24->PM21) UvA - Sent to reviewer on time.
    - ✓ Security operational procedures (Second and third revision)
    - ✓ Merged with MJRA3.8

No issues preventing successful project completion

Outstanding work in EGEE-I

gLite

LCMAPS/LCAS

- Finer grained error codes; Implement globus C authZ callout interface to be able to plug lcas and lcmaps into gt3 and gt4 services; refine the proxy lifetime checking

JobRepository

- Integration into gLite 1.5

Java key handling for encrypted storage

- Biomed DICOM server is in java: need for key generation and splitting in java

Mutual authz for biomedical applications

- The clients that store medical data want to be sure that the server they send the data to is authorized to store that data

Double certs for glite IO

- File access service gives assertion that the user is allowed to access a file, but the actual storage element also needs the user's credentials. So, the solution is to create a SAML assertion in FAS and embed that into the user's proxy. That way the storage element gets both

glexec

- Extended functionality; Finer grained error codes; Integration w Condor on the CE

Response to the reviewer's recommendations

"Prioritize the various security related tasks and requirements at the user and system level in order to come up with a list of intermediate goals towards a fortified Grid suitable for commercial deployment."

Applications: through the Technical Coordination Group (TCG) the long term, as well as the intermediate term, goals are prioritized according to applications requests.

Industry: The final security assessment (DJRA3.4) will be presented to industry partners, for feedback.

Response to the reviewer's recommendations

"Spearhead the effort of prioritizing the security requirements via the industrial partners starting with their own requirements and with their experience interacting with others."

See previous slide. Input is today given by the EGEE Industry partners, DATAMAT, and the Industry Forum representative. In addition we participate in direct meeting with industrial interest groups, e.g. from Life Science, Finance, Biomed. Input from Life Sciences are given through the security knowledgeable NA4 representatives in the Middleware Security Group. In GGF16 EGEE security representatives will organize a half day workshop especially inviting the Life Sciences WG.

Response to the reviewer's recommendations

"Track and actively contribute to the activities of the newly established IGTF (International Grid Trust Federation), conveying their experiences about prioritization of the security requirements."

- ✓ JRA3, through the EUGridPMA, was one of the main contributors in the launching of IGTF together with APGridPMA, TAGPMA
- ✓ David Groep (JRA3) is the first chair of IGTF. And will continue to be a member of IGTF.
- ✓ The current chair of IGTF is also a member of JRA3 and of MWSG and JSPG. Ensuring the feedback of IGTF experiences about prioritization of the security requirements.

Response to the reviewer's recommendations

"Outline and plan a series of stress tests of the security infrastructure."

The testing of the security infrastructure is divided into two parts, service attacks and the operational side's response to the attacks.

At this stage, and for the rest of the project, security analysis is our favoured method of testing security, with walk throughs and exercises for operational side.

For the middleware input is given from the operational side, if logging etc is done properly or not. For actual holes in middleware security code reviews of the critical parts and basic smoke testing are part of these tests. For example we now have a set of test certificates, running the set against all the services gives us a valuable input whether the authentication works as it should.

See also next slide, regarding external security audits.

Response to the reviewer's recommendations

"Conduct deliberate external attacks by 3rd party contractors."

- ✓ Not in EGEE-I. There is no place for this in the current plan.
- ✓ This is one of the deliverables of JRA2/Security Coordination in EGEE-II.
- ✓ First investigations and meetings with such 3rd party contractors have been initiated, together with SA1/OSCT manager Ian Neilson.

Response to the reviewer's recommendations

"Address the interoperability of the various Grid security mechanisms, existent and planned, with established security procedures."

- ✓ Interoperability is one of the main goals of the Middleware Security Group (MWSG).
- ✓ This has been very successful between EGEE and OSG, and has been promoted by GGF to be used as an example of pair-wise interoperability of Grids.
- ✓ To extend the interoperability effort, MWSG now includes DILIGENT, DEISA, SEEGRID and GRIDCC as members.
- ✓ Naregi Japan is also in close contact with MWSG and have met regularly the last year. New meeting focusing especially on Naregi needs is planned for beginning of March.
- ✓ Example of interoperability workshops co-organized respectively organized by EGEE:
  - GGF16, "Grid Authorization - Interoperability Here & Now"
  - HPDC15, "EGEE Workshop on Management of Rights in Production Grids"

Summary

The JRA3 outstanding work in EGEE-I is on time, both regarding Deliverables and milestones and gLite.

So, no issues preventing successful project completion.

Note: MJRA3.9 "Accounting" will be presented separably end of today by John White.