EUROPEAN MIDDLEWARE INITIATIVE

Security Architecture Document

John White, Helsinki Intsitute of Physics
for EMI Security Team.

EMI All-Hands meeting, November 2, 2012, Budapest

Contents

EUROPEAN MIDDLEWARE INITIATIVE

- **The Task.**
- **Proposal.**
- **Work.**

The Task

EUROPEAN MIDDLEWARE INITIATIVE

- Produce a “Security Architecture” document.
- Follows the outline given at:
  https://twiki.cern.ch/twiki/pub/EMI/EmiJra1T4Security/EMI-TechDoc-xxxxxx-EMI_Security_Architecture_Assessment-v0.1.pdf
  EGEE-III-MJRA1_4.pdf
- “The main idea is to describe what security means for distributed systems like grid, what are the major functions, how they are implemented in EMI in terms of common services and specialized services, federated identities, how security is managed (software fixes, threats response, coordination bodies) and what security-related international collaborations EMI is part of. The document is then closed with a chapter describing recommendations for future works and areas for improvement."
- **How do we handle this?**

Proposal

EUROPEAN MIDDLEWARE INITIATIVE

- Base our document on EGEE-III MJRA1.4.
  - Also take material from UNICORE Security Architecture document.
  - Is there an ARC Security Architecture document? (No)
- Drop EGEE-III MJRA1.4 into EMI template.
  - Some sections can remain unchanged.
  - Some need to be re-written by the appropriate experts.
  - A few new sections will be needed.

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 2.1 Definition of Security Architecture (Definition of security architecture or framework in general and in the context of distributed grid computing, basic principles)
  - **Mostly from EGEE MJRA1.4. I need input from all on this!**
- 2.2 Trust, Authentication and Authorization: A Terminology (Definitions of the most important concepts)
  - **Mostly from EGEE MJRA1.4. John.**
- 2.3 Virtual Organization, Sites and Common Grid Services (Definitions, brief description of the major grid services and how security applies to them)
  - **Directly from EGEE MJRA1.4. John.**
  - **Will need checking by UNICORE and ARC. Krzysztof,Weizhong**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 3 Authentication
  - **Directly from EGEE MJRA1.4 . John.**
- 3.1 Identity Credential Formats
  - **Directly from MJRA1.4. John.**
- 3.2 Bootstrapping Authentication
  - **Directly from EGEE MJRA1.4. John.**
- 3.3 EMI Common Authentication Libraries
  - **New text from CANI PT.**
- 3.4 Enforcing Validity Constraints
  - **Directly from EGEE MJRA1.4 (John, input from ARC/UNICORE)**
- 3.5 Revocation
  - **Directly from EGEE MJRA1.4 (updating by Oscar).**
- 3.6 Certificate Renewal
  - **Directly from from EGEE MJRA1.4. John.**
- 3.7 Delegation
  - **Text from EGEE MJRA1.4 updated by Paul Millar.**
- 3.8 Renewal of Proxy Certificates
  - **Text needs updating by Daniel K.**
- 3.9 Anonymity, Privacy, Pseudonymity
  - **Text from EGEE MRA1.4 to be updated by Henri M**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 4 Federated Identities
- 4.1 STS
  - **New text from Henri**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 5 Authorization
- 5.1 Introduction
  - **From MJRA1.4. John**
- 5.2 VOMS and UVOS
  - **Text from MJRA1.4. Andrea for VOMS. Bernd for UVOS.**
- 5.3 Policy definition and management
  - **New text on XACML and SAML profiles. Valery and Andrea.**
- 5.4 Argus AuthZ service
  - **Text from MJRA1.4. Need updating by Valery and Andrea.**
- 5.5 Identity Switching on the Worker Nodes
  - **Text from MJRA1.4. Need updating by Oscar/Mischa.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 6 Data Mamagement
- 6.1 Unencrypted Data Storage.
  - **From MJRA1.4. John**
- 6.2 Encrypted Data Storage.
  - **This is the Hydra section. John.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 7 Logging, Tracing and Auditing
  - **Updating of text from Mischa/Oscar/David G.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 8 Security Management and Threats Handling
  - **New text from Mischa/Oscar/David G.**
- 8.1 Software Security Management
  - **New text from Mischa/Oscar/David G.**
- 8.2 Bug fixing, Emergency Releases, etc.
  - **Text from Andrea C.**
- 8.3 Grid Services Security Assessment.
  - **Elisa Heyman**
- 8.4 Security Response Teams and Coordination Bodies
  - **Need to ask text from Morris and/or David G.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 9 Assessment, Strengths, ideas for improvement
  - **This comes from everyone. Free form...**

Timeline

EUROPEAN MIDDLEWARE INITIATIVE

- Deadline from project office: Dec 15th (Dec 14th)
  - Internal reviewable version: Dec 7th.
  - Individual contributions: Nov 23rd.
  - Workable document: Nov 9th.
- Therefore, be ready in one week...
- **Please NOT SEND me whole versions of the {.doc .odt} document to be merged.**
- **Text files only!**

The End

EUROPEAN MIDDLEWARE INITIATIVE

- **Questions?**
- **Comments?**
- **Complaints?**