EUROPEAN MIDDLEWARE INITIATIVE

Security Architecture Document

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

EMI All-Hands meeting, October 30, 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,Aleksandr**
- 2.4 Authentication
  - **Directly from EGEE MJRA1.4 . John.**
- 2.4.1 Identity Credential Formats
  - **Directly from MJRA1.4. John.**
- 2.4.2 Short-Lived Credential Services
  - **Modify text to refer to STS. Henri.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 2.4.3 Bootstrapping Authentication
  - **Directly from EGEE MJRA1.4. John.**
- 2.4.4 Enforcing Validity Constraints
  - **Directly from EGEE MJRA1.4 (John, input from ARC/UNICORE)**
- 2.4.5 Revocation
  - **Directly from EGEE MJRA1.4 (updating by Oscar).**
- 2.4.6 Certificate Renewal
  - **Directly from from EGEE MJRA1.4. John.**
- 2.4.7 Delegation
  - **Text from EGEE MJRA1.4 updated by Paul Millar.**
- 2.4.8 Renewal of Proxy Certificates
  - **Text needs updating by Daniel K.**
- 2.4.9 Anonymity, Privacy, Pseudonymity
  - **Text from EGEE MRA1.4 to be updated by Henri M.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 2.4.10 EMI Common Services and Libraries
- 2.4.10.1 CANI
  - **New text from Zdenek,Daniel,Aleksandr,Krzysztof.**
- 2.4.11 ARC, gLite and UNICORE Security Services
- 2.4.11.1 VOMS, UVOS, etc.
  - **Text from Andrea,Krzysztof.**
- 2.5 User Key Management
  - **Update text from EGEE MJRA1.4 by Henri M.**
- 2.5.1 Hydra

  This does not make sense. Should be in 2.8. John
- 2.6 Authorisation
- 2.6.1 Policy Definition and Management
  - **New text on XACML profile from Valery.**
- 2.6.2 Argus
  - **Updated text from EGEE-III MJRA1.4. Valery,Andrea.**
- 2.7 Identity Switching
- 2.7.1 glExec
  - **Updated text from EGEE-III MJRA1.4. Mischa,Oscar.**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 2.8 Data Management, Encryption, Confidentiality
  - **John.**
- 2.9 Federated Identities
- 2.9.1 STS
  - **New text from Henri**
- 2.10 Logging, Tracing, Auditing
  - **Text from EGEE MJRA1.4 to be edited by ???**
- 2.11 Security Management and Threats Handling
  - **This needs to be written by a member of EGI SVG (Oscar?)**
- 2.11.1 Software Security Management
- 2.11.1.1 Bug fixing, Emergency Releases, etc.
  - **Who can write this?**
- 2.11.2 Grid Services Security Assessment.
  - **Elisa Heyman**
- 2.11.3 Security Response Teams and Coordination Bodies
  - **Is this the same as 2.11?**

Work tasks

EUROPEAN MIDDLEWARE INITIATIVE

- 2.11.4 International Collaborations
- 2.11.4.1 OGF, IGTF, etc
  - **Who can write this?**
- 2.12 Assessment, Strengths, Areas for Improvement
  - **No idea...**

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?**