

EMI Security Workshop.

John White (for the Security Task)

- Product Teams.
 - Argus. (AuthZ).
 - “General” Security.
 - ▶ Trustmanager, Util-Java, LCAS, LCMAPS, glexec, SCAS
 - VOMS.
 - Delegation/Proxy Renewal.
 - ARC HED.
 - **SAML.**
 - **AuthN.**
- Immediate milestones.
 - Security workshop.
 - ▶ See: <http://indico.cern.ch/conferenceTimeTable.py?confId=92643>
Go to Indico and follow the links.
 - “Data” security needs.
 - AAi needs of DCIs.

- HIP.
 - Trustmanager, Util-Java, Argus, Delegation(Java), STS.
- NIKHEF.
 - glexec, LCAS, LCMAPS, Argus, AuthN.
- SWITCH.
 - Argus, SLCS, STS.
- CESNET.
 - Proxy-Renewal, Delegation(C).
- INFN.
 - VOMS, Argus, AuthN, SAML.
- UWAR, FZJ.
 - AuthN, SAML, Argus*.
- UU, UiO
 - HED, AuthN, SAML, Argus*.

- **Milestone subjects.**
 - **GSI**
 - **SAML**
 - **Common AuthN libraries**
 - **AuthZ system**

- A definition of GSI to be removed is needed.
 - This is the “enhanced SSL” protocol.
 - Non-standard SSL part to be replaced by OpenSSL.
 - Not necessarily the gssapi generic API provided by globus.
- Areas identified that currently need GSI
 - Delegation.
 - SRM. Especially the srm-copy.
 - GSIftp (GridFTP).
- Need to understand the move to OpenSSL 1.0.x
- Requirement to move towards delegation services/port-types.
- Need to tabulate a list of components/effort/reward.
- VOMS and libraries are now GSI-free.
 - Can exist with both GSI and SSL clients.
- Message to IGE project.
 - An implementation of GSI compatible with OpenSSL.
 - A GSI-free version of GridFTP (**controversial**).

- ARC,gLite have SAML “capability” but...
 - No usage or DIRECT requests or requirements.
 - ARC progresses for interop purposes.
- UNICORE.
 - Has capability AND uses SAML within stack.
 - Uses own SAML library... openSAML2 lib not available in time.
 - Has draft profile. Documented.
- SAML-VOMS now exists in gLite production.
 - “Pull” mode needed (OK from VOMS PT).
- **Action: SAML “PT” needs to be formed.**
 - Coordinate the move to opensaml2 library.
 - Adopt to the UNICORE SAML profile.
 - Gather requirements from LCG (EGI) for SAML usage wrt AuthZ granularity.
 - SAML delegation wrt restriction of privilege.
 - Replacement of UVOS with SAML-VOMS.

- UNICORE.
 - Provided well-defined set of reqs on common AuthN.
- ARC.
 - Would like to switch to Argus for centralized authN as well.
 - Need thread friendly (not safe?) APIs.
- gLite.
 - Presented work related to VOMS libraries...
- Recognize that requirements on common AuthN lib needed.
- **Action.**
- Set up an AuthN PT. Initial composition
 - Oscar K., Daniel K., Joni H., Vincenzo C., Aleksandr K., Krzysztof B.
- By the end of July: (phone confs start soon)
 - **Provide a set of requirements on the authN common lib API.**
 - **Inventory of existing code.**
 - **Estimate of effort for missing parts.**

- **ARC.**
 - A move to Argus and common AuthN lib agreeable.
 - Comment on SAML profiles for different scenarios.
- **UNICORE.**
 - Questions on SPL and XACML.
 - Also willing to adopt Argus.
- **Action:**
 - Form a group to specify common SAML profiles for CEs.
 - Hopefully within the Argus PT?
 - Add ARC, UNICORE contacts.
 - **Clarify the full XACML spec within Argus or not.**

- Milestone at EGI Technical Forum.
 - AAI needs of DCIs.
-

- Milestone later this year.
 - Data and AuthZ (Argus)?.
- This needs work beforehand (during summer)
- Argus PT and DM task.