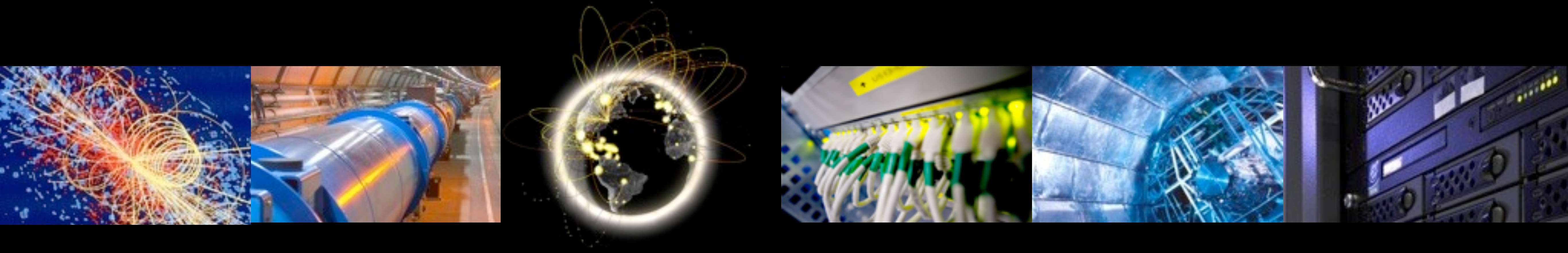
WLCG Group

Update on the security TEG

GDB, 18th April 2012



General update

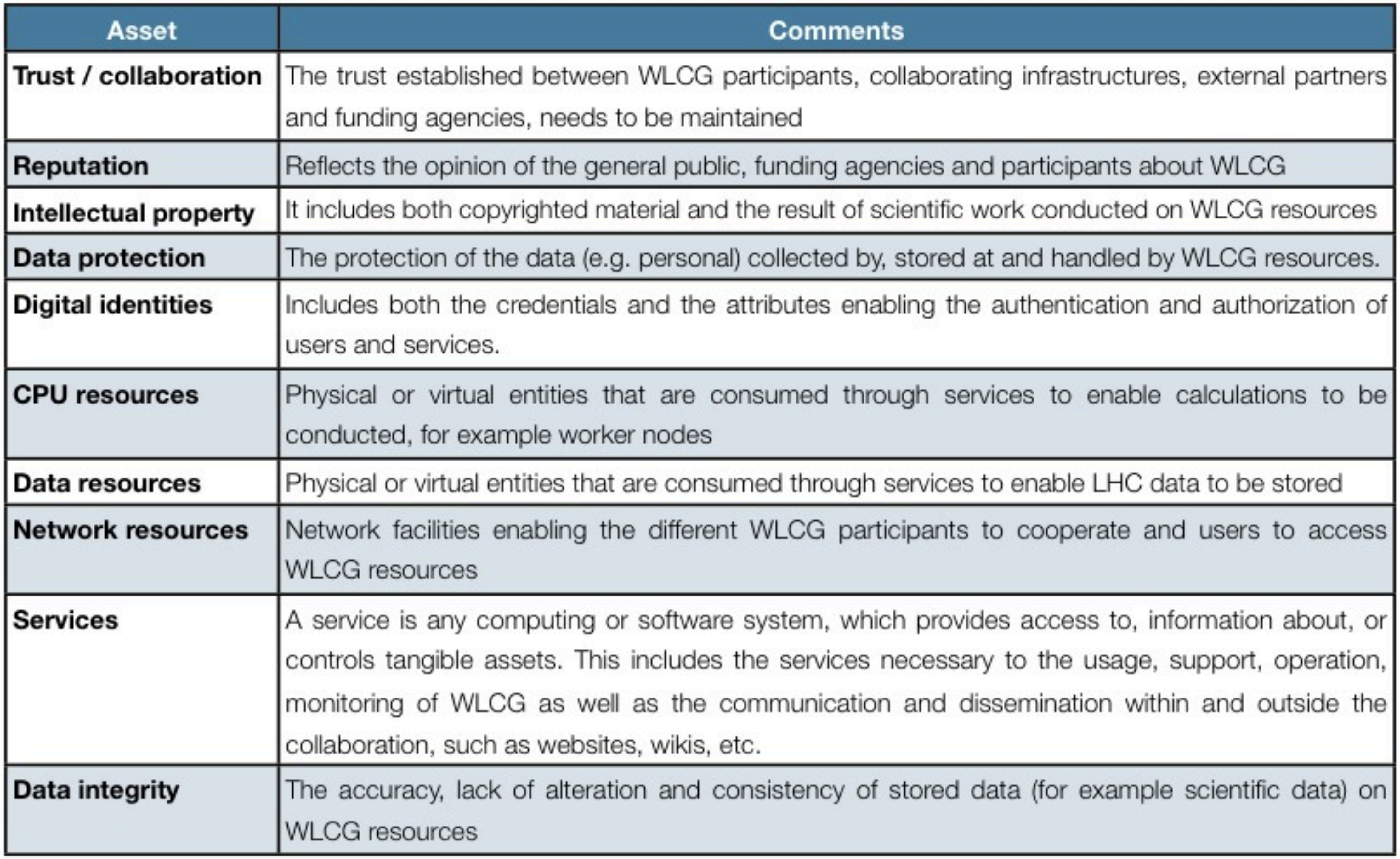
- 5 different subtasks
  - WLCG risk assessment
  - AAI on the worker nodes
  - AAI on the storage systems
  - Identity federation
  - Usability vs Security
- All details at:
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG
- Steffen Schreiner writing his thesis, resigned as a co-chair

Risk analysis

- Current status
  - Document complete
  - Waiting for feedback - document submitted to the MB
- Todo
  - Prepare recommendations
- Timeline
  - Gradual delivery until the end of 2012

Risk analysis

- It is the goal of the security teams to protect WLCG assets



Asset	Comments
Trust / collaboration	The trust established between WLCG participants, collaborating infrastructures, external partners and funding agencies, needs to be maintained
Reputation	Reflects the opinion of the general public, funding agencies and participants about WLCG
Intellectual property	It includes both copyrighted material and the result of scientific work conducted on WLCG resources
Data protection	The protection of the data (e.g. personal) collected by, stored at and handled by WLCG resources.
Digital identities	Includes both the credentials and the attributes enabling the authentication and authorization of users and services.
CPU resources	Physical or virtual entities that are consumed through services to enable calculations to be conducted, for example worker nodes
Data resources	Physical or virtual entities that are consumed through services to enable LHC data to be stored
Network resources	Network facilities enabling the different WLCG participants to cooperate and users to access WLCG resources
Services	A service is any computing or software system, which provides access to, information about, or controls tangible assets. This includes the services necessary to the usage, support, operation, monitoring of WLCG as well as the communication and dissemination within and outside the collaboration, such as websites, wikis, etc.
Data integrity	The accuracy, lack of alteration and consistency of stored data (for example scientific data) on WLCG resources

Risk analysis

- Highlighted the need for fine-grained traceability
  - Essential to contain, investigate incidents, prevents re-occurrence
- Aggravating factor for every risk:
  - Publicity and press impact arising from security incidents
- 11 separate risks identified and scored. Top risks:

Risk
Misused identities ("SSH"-type included)
Attack propagation between WLCG sites
Exploitation of a serious OS vulnerability
Threats originating from trust services
Negative publicity on a non-event
Insecure configuration leading to undesirable access
Insufficient protection of information leading to sensitive data leakage
Incidents on resources not bound by WLCG policies
Exploitation of a serious VO/middleware software vulnerability
Data removal/corruption/alteration
DoS from an external organisation

AAI on the WN

- Current status
  - Work in progress, report available
- Main conclusions
  - Fined grained traceability required
  - Physical identity switching for MUPJ needed
  - A status report has been prepared
- Issues
  - Lack important stake holders in the discussions
  - Needs to be addressed to achieve coherent recommendations
  - A number of topics yet to be discussed

AAI on the WN

- Several areas would need further discussion or are yet to be addressed, including:
  - The use and transport of credentials on the WN, including delegation, propagation, revocation and traceability.
  - The implementation of security controls (e.g. blocking/banning end users, credential revocation) and who should operate them.
  - The ownership of the traceability information. Is it OK to split the traceability information between VOs and sites?
  - The security implications of virtualization on the WN
  - The security implications of submitting jobs to external clouds
  - The network connectivity requirements of the experiments
  - The longer term future of the security model of the WN
- Timeline
  - Gradual delivery until the end of 2012

AAI on the storage systems

- Current status
  - Work in progress, report available
- Main conclusions
  - Traceability improvements are needed
  - Efforts required to improve our data protection (permissions) issues on the different SEs
  - Several data ownership issues need to be addressed
- Future work
  - Specific recommendations to be provided (June 2012)
  - Longer term future to be discussed (June 2012)
- Issues
  - Difficult to get contributions from Security TEG members
  - Good collaboration with the storage TEG - should we merge?

Other subtasks

- Identity Federation
  - Status: work in progress, no report available
  - Work is ongoing in different forums
  - Security TEG members to provide comments on proposed model
  - Status report expected before June 2012
- Usability vs Security
  - Status: work in progress, interim report almost ready
  - Status report expected before June 2012

WLCG Worldwide LHC Computing Grid