CERN IT Department

IAA @ CERN

A Federated World

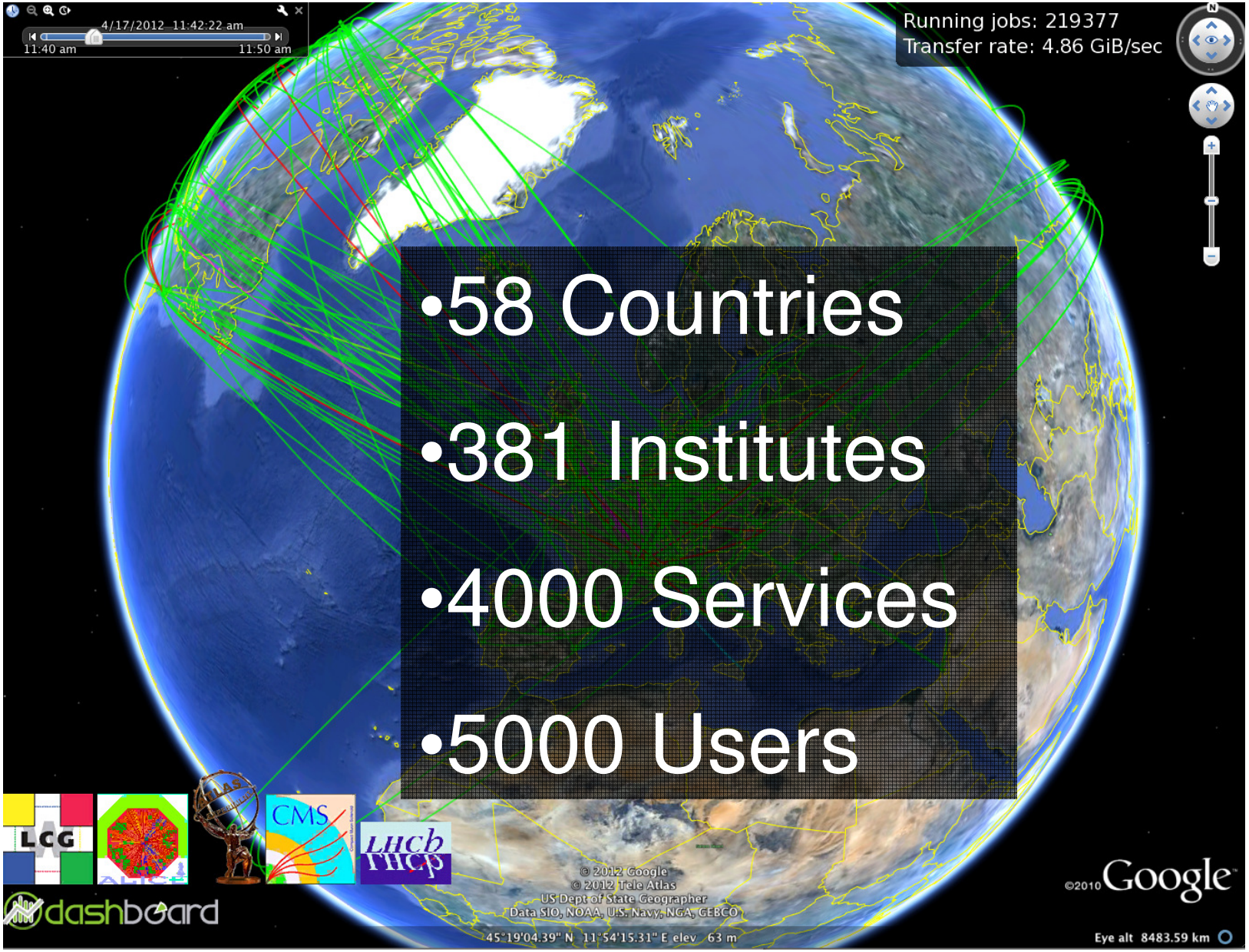
CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Three Areas Of Activity

- Grid Authentication
- Authentication at CERN
- Federated Identity Management

WLCG

CERN IT Department



Policy Framework

CERN IT Department

- Grid Security Policy
- Grid Acceptable Use Policy (*Users*)
- Grid Site Operations Policy (*Resource Provider*)
- Site Registration Security Policy
- VO Operations Policy (*Attribute Authority*)
- Virtual Organisation Registration Security Policy
- Virtual Organisation Membership Management Policy
- VO Portal Policy
- Traceability and Logging Policy
- Security Incident Response Policy
- **Approval of Certificate Authorities**
- Policy on Grid Pilot Jobs
- Policy on the Handling of User-Level Job Accounting Data

IGTF

- International Grid Trust Federation
  - 10 years of experience (est. 2003)
  - Common policies and guidelines
    - Between three Policy Management Authorities (PMAs)
      - APGridPMA covering Asia and the Pacific
      - EUGridPMA covering Europe, the Middle East and Africa
      - The Americas Grid PMA covering Latin America, the Caribbean and North America
    - Members of a PMA are also members of the IGTF
      - Identity providers, CAs, etc.
    - Accreditation Guidelines
  - Provides trust anchor distribution

CERN Identity Management

CERN IT Department

- 44K Accounts
  - 10% Staff
  - 65% Users (Affiliated and Non-affiliated)
  - 25% Other (Retirees, Contractors, Club Members)
- Require different Levels of Assurance (LoA)
  - High LoA: CERN account (multi factor)
    - Access to sensitive resources (HR DB)
  - Medium LoA: CERN account
    - Access to resources (Create a VM instance)
  - Low LoA: Any registered FedID account
    - Access to non-sensitive resources (Wiki edits)
  - No LoA: OpenID, unregistered FedID
    - Access to public resources (CERN Clubs, Indico, email lists etc.)

Preparing To Federate

- Split authentication and authorization
  - For all CERN services
- Authentication
  - Single Sign-on
    - Shibboleth IdP already rolled out
    - Extension allows using FedIDs, OpenID etc.
- Authorization
  - No agreement on the semantics of attributes
    - CERN acts as an Attribute Authority
      - Registration is in any case required
- Defining and agreeing on policy
  - The ownership and use of CERN computing resources and services
- Federation pilot with Brookhaven
- *Bottom up approach*

Federated Identity Management

CERN IT Department

- Workshops on identity management
  - Initiated by the IT leaders of EIROforum
- FIM paper describes
  - The needs of the research communities
  - The status of the activities in the FIM domain
  - The specific use cases
  - The common vision for FIM
  - The key stages of the roadmap
  - A set of recommendations to ensure implementation
- *Top down approach*