

Requirement 5: Frameworks to support seamless implementation of federated community cloud environments

Cloud Federation -- *Establishing Trust*

Dr. Craig A. Lee, lee@aero.org
Senior Scientist, The Aerospace Corporation

NIST Cloud Computing Forum & Workshop V
Washington, DC, USA
June 5, 2012

Cloud Federation

*When two or more clouds
under different administrative domains
must interact securely to form a general or
mission-specific federated Community Cloud*

Establishing Trust ~~Blind Trust?~~ **NO!**

Cloud Federation

*When two or more clouds
under different administrative domains
must interact securely to form a general or
mission-specific federated Community Cloud*

Establishing Trust ~~Blind Trust?~~ NO!

*Establishing well-known data, service and
user attributes, and processes whereby
cross-organizational policies can be
securely enforced*

Requirement 5: Priority Action Plans

PAP 1: Define Federated Community Cloud requirements and scenarios

PAP 2: Identify how hybrid cloud and cloud broker elements described in the cloud Reference Architecture can be leveraged and harmonized in Federated Community Cloud settings

PAP 3: Document current usage patterns and projected near-term trends in grid and cloud architectures with attention to tools used for effective support of federated user communities

PAP 4: Present analysis of grid communities' applicability to federated cloud communities, including technology, trust infrastructure, & governance

PAP 5: Assess intercloud efforts (e.g. SDO's) for applicability to Federated Community Clouds

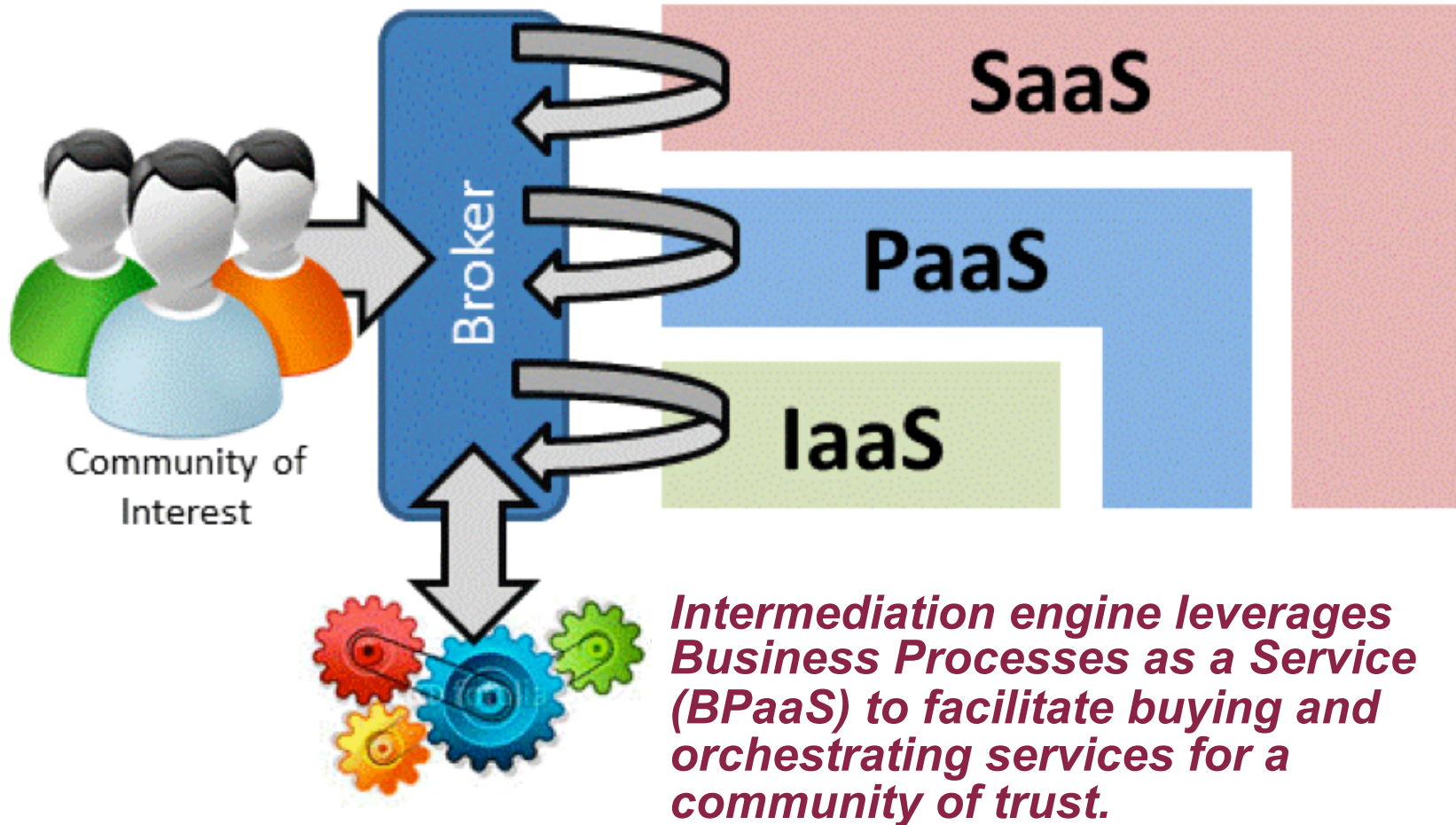
PAP 1A: Definition of Federated Community Cloud Requirements

- Privacy
- Security
- Compliance Adherence
- Trust Infrastructure
- Common Governance
- Private Communications

PAP 1B: Definition of Federated Community Cloud Scenarios

- Catastrophic Event Response
 - *Natural Events*
 - Hurricane Katrina
 - Haiti earthquake
 - Japanese Tōhoku earthquake and tsunami
 - *System Failure*
 - Bhopal, India
 - *Hostile Acts*
 - 9/11
- Specialized Distance Medical Care Emergency Trauma Response
 - *Dynamically Reconfigurable, Patient-centric, Integrated Trauma Medicine*

PAP 2: Leveraging Hybrid Cloud and Cloud Broker Elements in Federated Clouds



Reprinted by permission of NIST

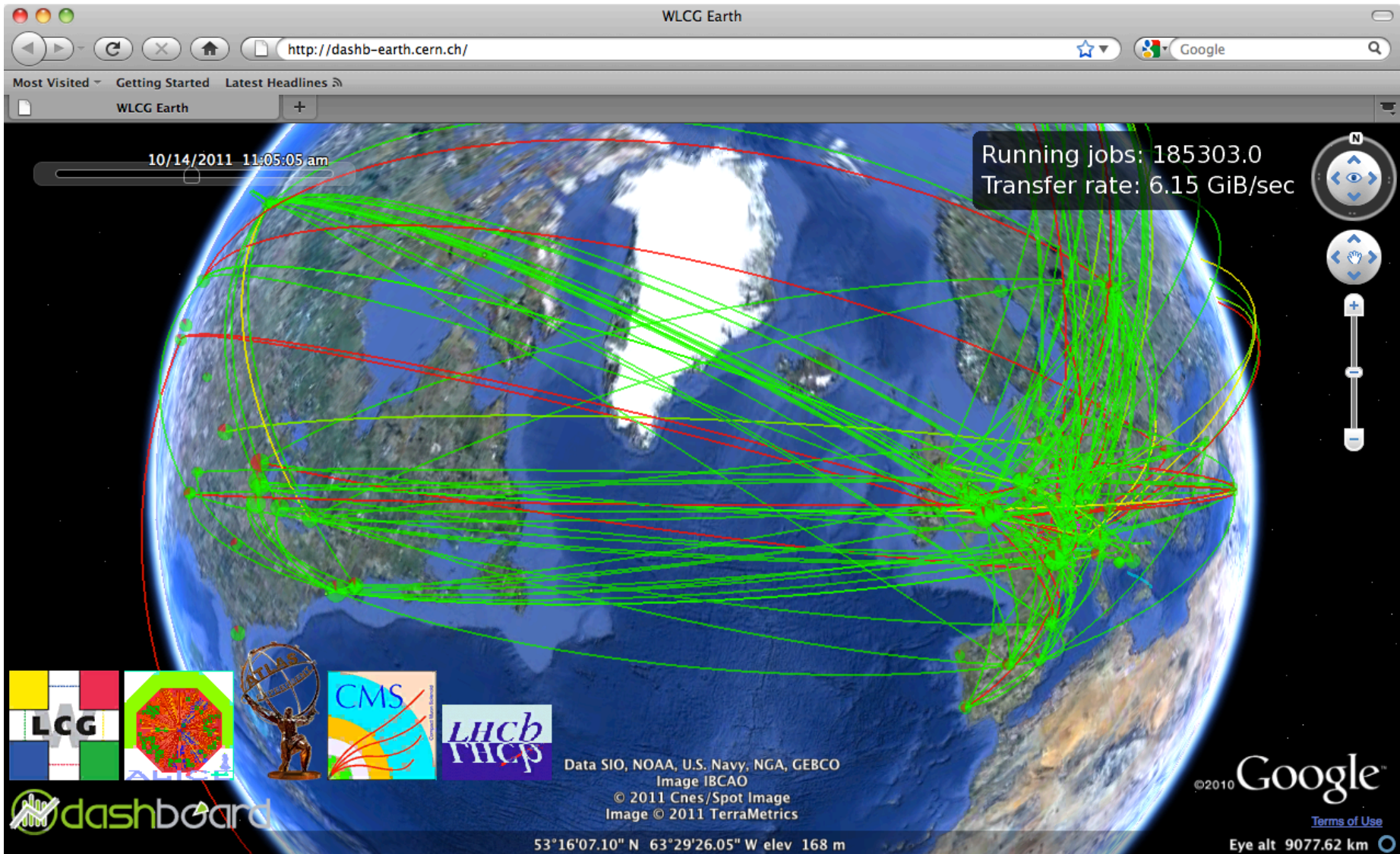
PAP 3: Current and Near-Term Trends & Tools to Support Federated Clouds (*Scant Overview*)

- Relevant Existing and Emerging OGF Standards
 - *Open Cloud Computing Interface (OCCI)*
 - *Federated Identity Management (FedSec-CG)*
 - *Managing the Trust Eco-System (CA Ops, AuthN/AuthZ)*
 - *Virtual Organization Management System (VOMS)*
 - *Service Agreements (WS-Agreement, WS-Agreement Negotiation)*
- Cooperative Agreements
 - *OGF OCCI and DMTF CIMI: Joint work registrar concerning these specs*
 - *OGF is now a Category A Liaison, ISO JTC1 SC38 on Cloud Computing*
 - *OCCI and SNIA DCMI: Four joint Cloud Plug-Fests – and counting*
 - *TM Forum, Cloud Security Alliance, IEEE, SIENA, GICTF, NIST and others*
- European Grid Initiative (EGI) Federated Cloud Task Force
 - <https://wiki.egi.eu/wiki/Fedcloud-tf:FederatedCloudsTaskForce>
- Federated Identity Management for Research Collaborations
 - CERN-OPEN-2012-006: <https://cdsweb.cern.ch/record/1442597>



Scale of this Effort: *Worldwide LHC Computing Grid*

WLCG Dashboard: <http://dashb-earth.cern.ch>

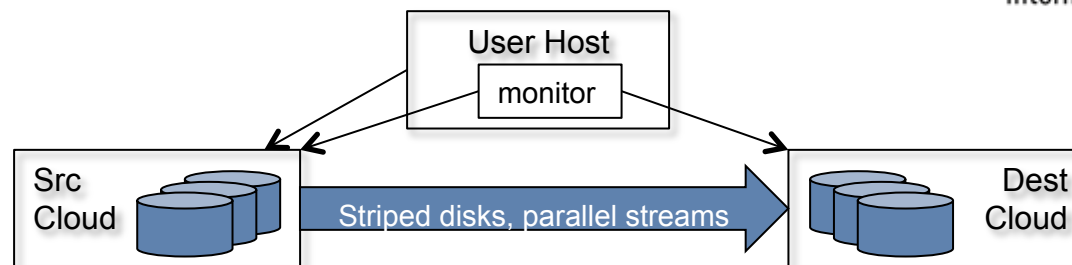


PAP 4: Grid Applicability to Federated Clouds

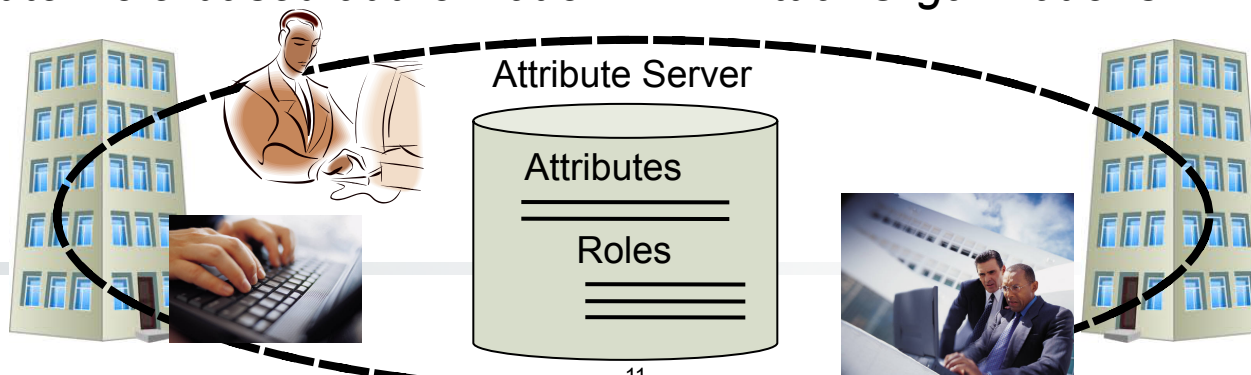
- Identity Provisioning: Many Technical Methods
 - *Kerberos, Shibboleth, OpenID, PKI w/ X.509 Certificates, ...*
- What does it mean to Federate Identity?
 - *Users (and Non-Person Entities) must be associated with user attributes*
 - Users may also be associated with *roles* – a pre-defined set of attributes
 - *Semantic interoperability of user attributes must exist*
 - Organizations must agree on what user attributes mean
 - *Organizations must be able to authenticate users based on these attributes*
- What does it mean to Enforce Policy?
 - *Data and services must also be associated (tagged) with attributes*
 - *Semantic interoperability of data and service attributes must exist*
 - ***Policy can be defined as the allowable combination of user, data and service attributes***
 - **Who can do what with what**
 - *Organizations must be able to authorize user requests based on policy*
 - A well-defined policy language to enable cross-organizational policies

A Case Study: International Grid Trust Federation, www.igtf.net

- Provides trust accreditation among federation members
- Specifies how PKI Certificate Authorities are configured and operated
- AP/EU/TAG Policy Management Authorities verify compliance
 - *Self-audits with peer review, site visits, etc.*
- IGTF members trust certificates signed by each other's CAs
- What does this enable?
 - *Single Sign-On → Reuse of electronic identities*
 - *Delegation of Trust → Secure, third-party operations*



- *Attribute/Role-based authorization → Virtual Organizations*



PAP 5: Other Applicable Intercloud Efforts for Federated Clouds

- Alliance for Telecommunications Industry Standardization (ATIS)
- IEEE
 - *P2301 Working Group: Cloud Profiles*
 - *P2302 Working Group: Interclouds*
- Global Inter-Cloud Technology Forum (GICTF)
 - *Technology Task Force*
 - *Service Usage Task Force*
- Open Grid Forum (OGF)
 - *www.ogf.org*



Summary and Next Steps

Need to establish well-known data, service and user attributes, and processes whereby cross-organizational policies can be securely enforced

- Need well-defined:
 - *User, data and service attribute schemas*
 - *Roles and role names*
 - *Policy language(s)*
- Prior agreement on, or well-defined negotiation of, attribute semantics
- Coordination among trust eco-system efforts
 - *NIST National Strategy for Trusted Identity in Cyberspace (NSTIC)*
- Integration with existing federal security mechanisms
 - *Federal PKI infrastructure*
- Evaluation of attribute granularity on system performance
 - *Fine-grained data access control may be performance prohibitive*
- • More experience!

Questions?

All trademarks, service marks, and trade names
are the property of their respective owners.