DOE Grid Federation efforts

Tony Genovese
ATF team ESnet
Lawrence Berkeley National Laboratory

Outline

- Back Ground
  - Separation of Authentication and Authorization.
  - First Federation – EU Data Grid, Cross Grid
- Shibboleth Federations
- Commercial Federation efforts
- International Grid Federation
- Regional Policy Management Authorities (PMAs)
  - EU Grid PMA
  - AP Grid PMA
  - The Americas Grid PMA
  - DOEGrids Federation
- Global Grid Forum efforts
- New Federations and AuthN services
  - KCAs
  - Site Integrated Proxy services – SIPS
  - Host certificate service – Site SSL support
  - RADIUS Authentication Fabric - RAF

Back Ground

- Authentication Services in Grids
  - Grids Federations have separated the ***Authentication*** and ***Authorization*** problems.
  - Resource owners are responsible for Authorization.
    - Maps Authentication token to local access.
  - Authentication service providers are responsible for providing Strong Authentication tokens (Certificates).
- European Data Grid and Cross Grid
  - First Grid Federation
  - DOEGrids Joined to represent DOE and NSF scientists and Engineers.
- International Grid Federation
  - March 2003 Tokyo
  - Promote and coordinate Regional Policy Management Authorities.

Shibboleth Federations

- The initiative is facilitated by Internet2
- Shibboleth is a system designed to exchange attributes across realms for the primary purpose of authorization.
- It provides a secure framework for one organization to transmit attributes about a *web-browsing* individual across security domains to another institution.
- It is being used by higher education institutions including Penn State, North Carolina State University, Brown University, and the University of Washington
- The users can determine exactly which information about them is released.
- A Shibboleth federation: (shibboleth.internet2.edu)
  - Is a group of organizations who agree to exchange attributes using the SAML/Shibboleth protocols and abide by a common set of policies and practices.
  - A federation needs to supply a registry to process applications to the federation and distribute membership information to the origin and target sites.
  - This include distribution of the PKI components necessary for trust between origins and targets.
  - A set of agreements and best practices defined by the federation governing the exchange, use, and population of attributes before and after transit.
  - There should be a way to find information on local authentication and authorization practices for federation members.

Commercial Federation efforts

- Not focused on Grids – They are Web centric.
- Liberty Alliance: www.projectliberty.org
  - Working on Technical, Business and policy challenges of Identities and web services.
  - Open technology specifications
  - Business guidelines
  - Privacy controls in the specifications
  - Implementation certifications
  - Distributed solution VS the Passport centralized model
- Microsoft Passport: www.microsoft.com
  - Scaling back: repositioning to be used only by Microsoft and close partners – not a single sign on solution. It was not being adopted by business.
  - US and EU regulators put restriction on use – privacy laws.
  - IBM has joined Liberty and Microsoft ***may*** join.

International Grid Federation

- Set up in March 2003 – the Tokyo accord. WWW.GridPMA.org
- Goals
  - Promote trust peering between The Americas, European and Asian Pacific communities.
    - EU Grid Policy Management Authority
      - EGEE: Enabling Grids for E-science in Europe
    - Asian Pacific Policy Management Authority
      - APGrid: National Institute of Advanced Industrial Science and Technology
    - The Americas Grid PMA – new
      - Canada and USA (DOE)
  - Promotes the establishment of top level CA registries:
    - Trusted 3rd party repositories need for establishment of trust.
      - Root CA certificates, CA repositories and CRL publishing points.
    - EU Grid PMA registry – de facto (CNRS: French National Center for Scientific Research)
    - Asian Pacific CA registry (AP PMA)
    - TERENA TACAR (TERENA Academic CA Repository)
  - Use Global Grid Forum for publishing Standards and community best practices.

EU Grid PMA

- EU Grid PMA (www.eugridpma.org)
  - Replaced EDG and Cross Grid
  - Developed new charter based on GGF PMA charter template.
  - Represents CA and Relying parties.
  - 26 country level CAs, plus US members
  - DOEGrids full voting membership.
  - Manages the de facto minimum CA operational requirements.
  - Manages the primary list of trusted CAs.

Asian Pacific Grid PMA

- AP Grid PMA (www.apgridpma.org)
  - Formed Summer of 2004
  - Charter based on GGF PMA charter template.
  - Represents CA and Relying parties.
  - 12 country level CAs, and SDSC
  - Minimum operational requirement synced with EU's
  - Provides two levels of membership: Operational and Experimental.

The Americas Grid PMA

- Started Fall 2004
- Founding members
  - Canarie
  - Fermi National Accelerator Laboratory
  - DOEGrids
- Represent CA's from Scientific/Research communities in the Americas.
- Investigate Cross-signing and CA Hierarchies support for the community.
- Investigate alternative Authentication services.

DOEGrids Federation

- One of the largest PKI deployments in Grids
  - 1100 users and 1300 hosts/services
- 18 member board of directors
  - Representing: PNL, PPDG, NFC, ORNL, ANL, LBL, NERSC, ESG, FNAL, CERN LCG, NSF iVDGL and EPA NCC.
- It fosters community ownership and involvement.
- Designed to allow sites and organizations to easily deploy PKI.
- PMA is changing to meet Security challenges.
  - Formation of Rapid Response committee
    - Addresses Security incidents
  - Formation Policy review committee
    - Addresses possible policy changes needed to meet security requirements
- Could expand DOEGrids Scope to include any organization

Global Grid Forum

- **GGF efforts are driven by our community requirements.**
- **Developing National and International trust relationships has shown a need for common agreed upon practices.**
- **A number of Security Working Groups have been created to form Internationally recognized Community Best Practices.**
  - Grid CP
  - CA Operations
- **GGF community best practices documents published.**
  - **Grid CP:** Defines common issues in developing a community CP/CPS
  - **PDS:** PKI disclosure Statement, Defines a condensed publishing method for CP/CPS
  - **PMA charter:** Defines how to set up a Policy Management Authority
- **GGF currently under development**
  - **OCSP:** Will help facilitate real-time validation of identity certificates
  - **PKI profiling:** Will promote PKI innovation and deployment
  - **Grid federation requirements:** Will facilitate deployment of Trust federations.

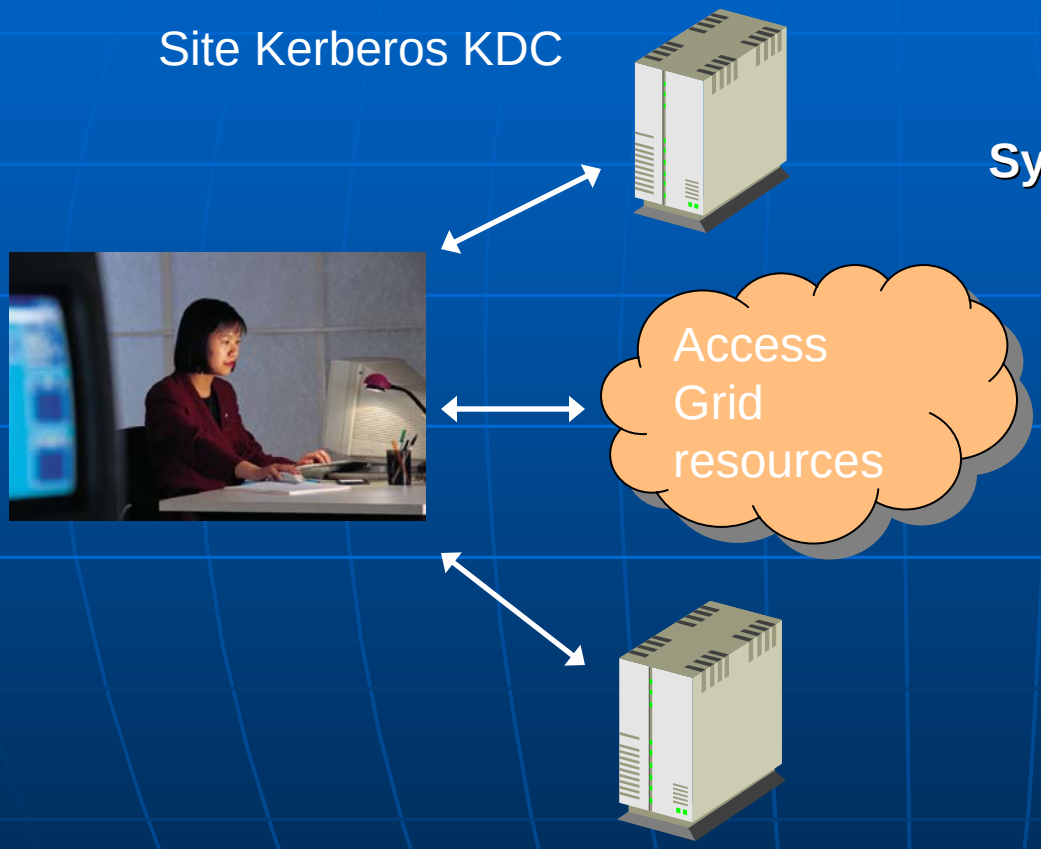
Global Grid Forum

- Community Documents
  - Grid CP/CPS
  - Policy Management authority
  - PKI Disclosure statement – copy right issue ABA
  - Certificate profile - tabled
  - Grid common naming practices – tabled
  - OCSP service requirements
  - Authentication Profiles - New

New Federations and AuthN services efforts

- SIPS - Site Integrated Proxy services
  - KCA example
- Site SSL support - Host certificate service
- RAF - RADIUS Authentication Fabric
- Expand scope of DOEGrids

Site Integrated Proxy services KCA example



Synopsis of steps for Grid User:

1. Register with Fermilab
   1. Get your Fermilab VID
   2. Get your Kerberos Principal
2. Install the Fermilab **KCA** certificate and signing policy;
3. Install the **KCA** client software;
4. Generate proxy access Grid

SSL Service Federation

System Admin

ESnet SSL Federation CA

Site or Organization Web servers

Synopsis of steps for System Admin:

Register with ESnet:

1. Get your ESnet Grid Admin account
2. Request and self approve host certificates.

Replaces:

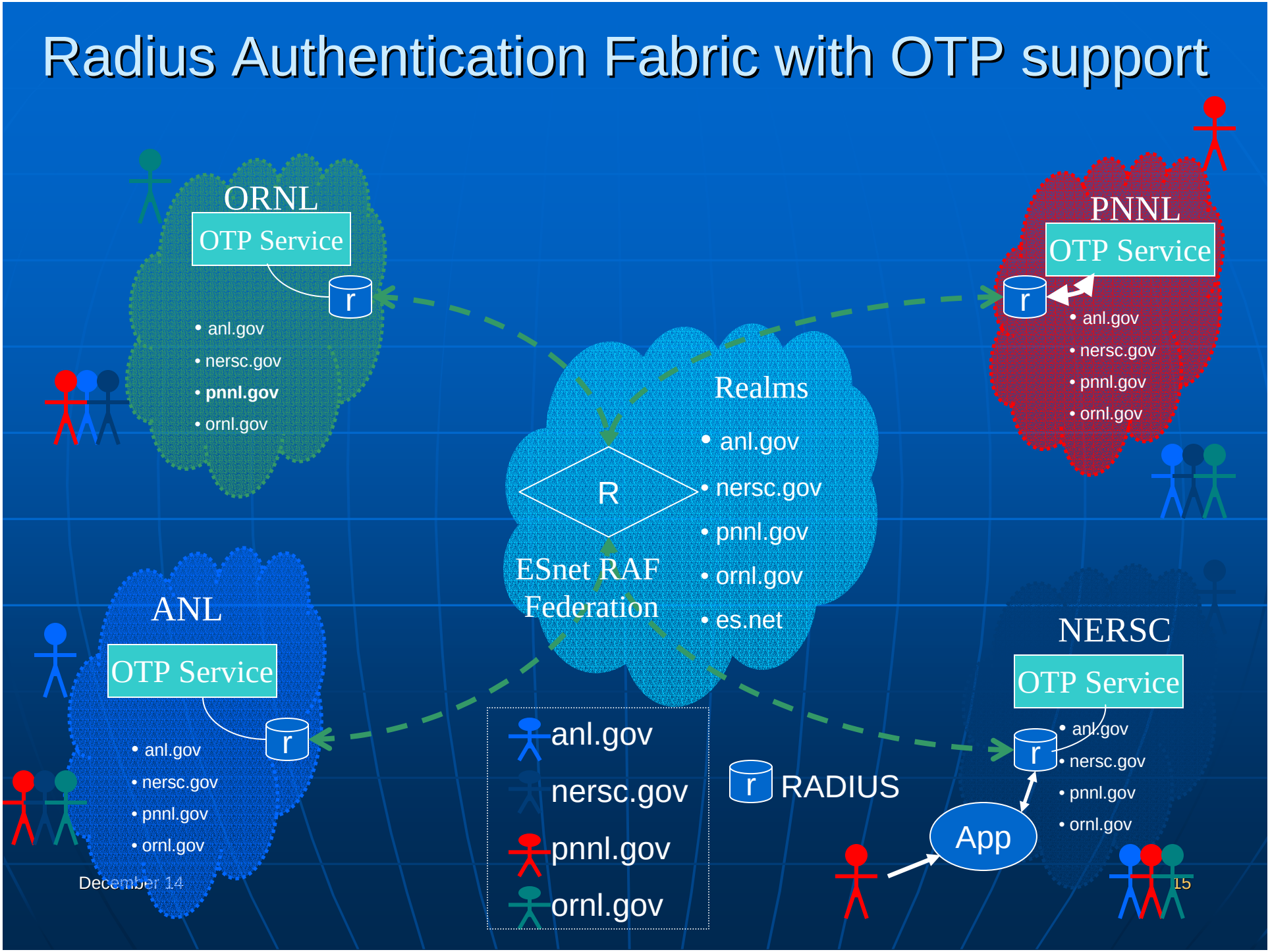
a. Self signed certificates

b. Commercial providers

Requires:

The Browser providers to add the SSL CA cert to their trusted list of CAs – this is to stops security warning pop-ups.

Radius Authentication Fabric with OTP support

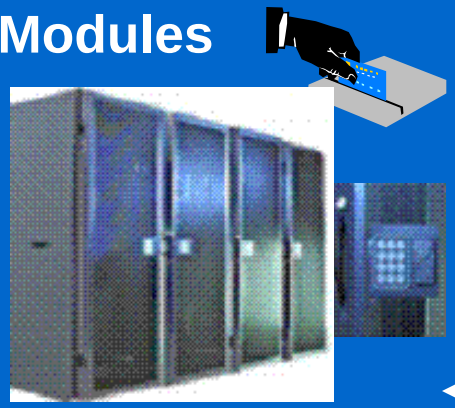


DOEGrids PKI Security

Offline Vaulted Root CA

PKI Systems

Hardware Security Modules



Access controlled racks

Secure Data Center

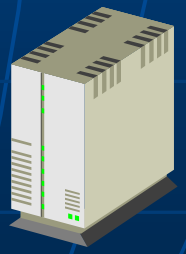
Building Security

LBNL Site security

Grid User

Fire Wall

Internet



Intrusion Detection