Short Lived Credential Service SLCS

Tony J. Genovese

Lawrence Berkeley National Laboratory

USA

November 29, 2005

Outline

- **Background**
- **What is SLCS?**
- **Document overview**
- **Examples**
- **Issues and Status**
- **Future Profiles?**

Background

- IGTF WG's work on Grid Authentication
- Establish Authentication Profiles at GGF
  - Handle trust mitigation in dissimilar Authentication systems
- SLCS is our second profile
  - Classic X.509 profile – maintained by EUGridPMA
- SLCS is maintained by TAGPMA
- It is derived from the EUGridPMA minimum requirements, version 4.0.

What is SLCS

- A translation of a local site's native Identity to a Grid Identity.
  - A KCA can translate a local Kerberos Identity to a Grid Identity.
  - MyProxy can be integrated to some sites
    - Active credential repositories – different AuthN profile.
- Identity is validated by site security office
- Leverages Site help desk and customer support
- Possible local site service candidates:
  - Kerberos, Windows Domain, LDAP, One Time Password and Long term Certs.

SLCS Profile sections

- **Identification**
  - **Title, version, date and OID**
- **General Architecture**
  - **A SLCS is an automated system to translate the local site identity into a Grid identity. End entity identity validation is based on the local site authentication system.**
- **Identity**
  - **Every DN in a short lived certificate must be linked to one and only one End Entity at the Site/Organization.**

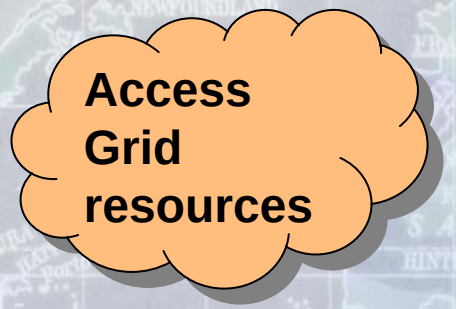
SLCS profile sections cont'

- **Identity Translation rules**
  - **A SLCS must describe in their CP/CPS:**
    1. **How the identity (DN) assigned in the certificate is unique within the namespace of the issuer.**
    2. **How it attests to the validity of the identity.**
    3. **How it provides accountability, show that they have verified enough identity information to get back to the physical person any time now and in the future**
- **Operational Requirements**
  - **Security controls for: Data center, System, CA private key, etcetera…**
  - **Certificate and CRL profile**

SLCS profile sections cont'

- Site Security
  - Protection of Private key , authorized personnel.
- Publication and Repository responsibilities
  - Each SLCS authority must publish for their subscribers, relying parties and for the benefit of distribution by the PMA and the federation …
- Audits
  - Must keep records… must accept audit by other accredited CAs…
- Privacy and confidentiality
  - Accredited SLCS CAs must define a privacy and data release policy compliant with the relevant national legislation.
- Compromise and disaster recovery
  - The SLCS CA must have an adequate compromise and disaster recovery procedure…

Example: KCA



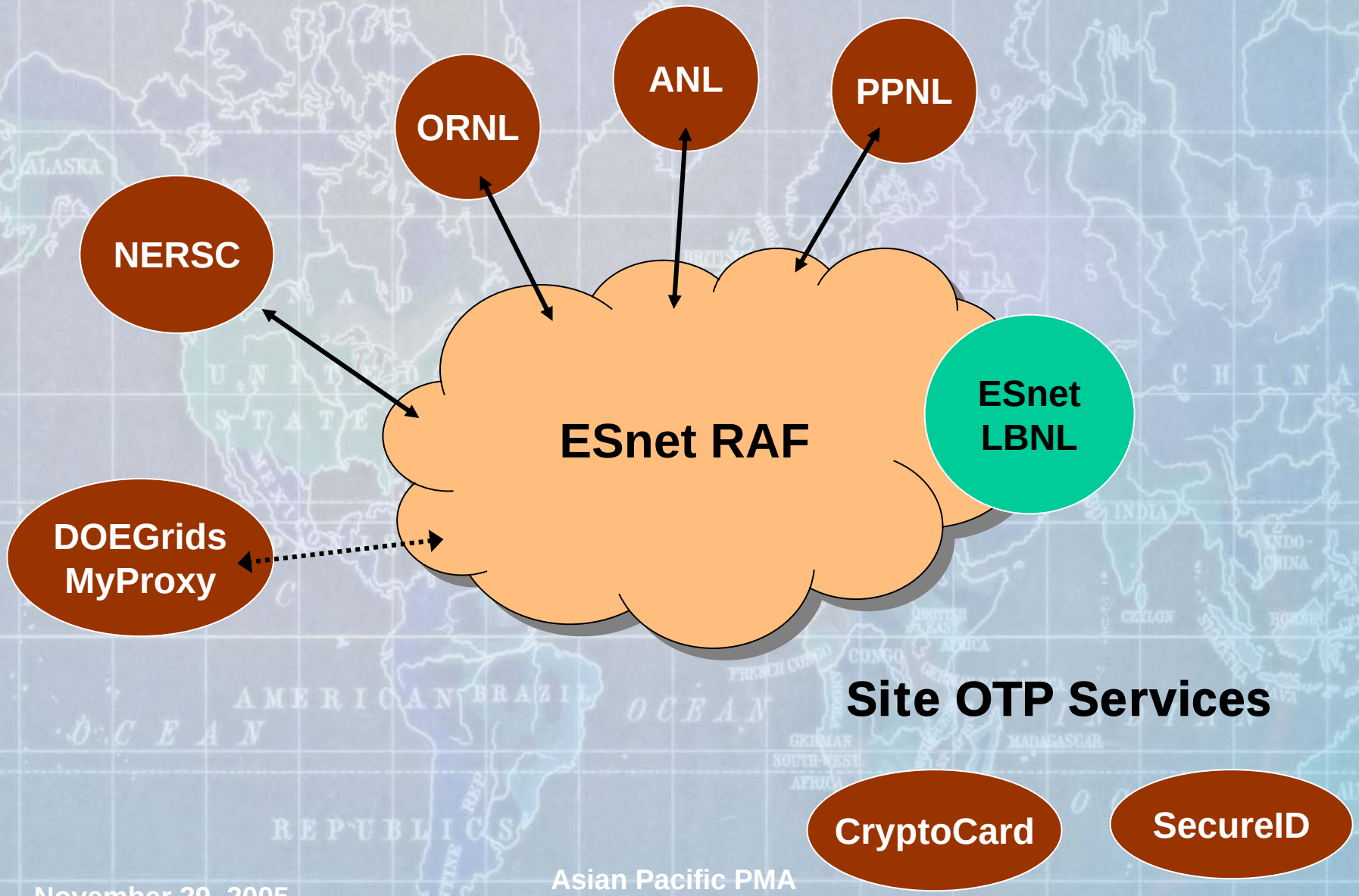
Site Kerberos KDC

Proxy generator
KCA

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

Example: RADIUS multi site MyProxy



Issues and Status

- Name recycling
  - Sites reuse names after some period
  - Relying parties want Grid identities to be unique for all time.
- Clarification of operations
  - End entities must be able to sign Proxies
  - Non-issue covered by Proxy RFC?
- Status
  - Voting started on version 1.1
    - Scheduled to Complete December 7th

Future Profiles ?

- Active Credential Stores
  - MyProxy - with long term certificates
- Radius Federations
  - Eduroam profile
- Common Minimum profile?
  - Basic operations all profiles must conform to.