LIGO Identity and Access Management

Technical Overview

The Problem

- The LIGO Scientific Collaboration is comprised of over 900 scientists from 22 nations on five continents.
- Application domains we serve:
  - web: wikis, document database, etc
  - grid computing (Globus toolkit - X.509)
  - collaboration tools: email lists, etc.
  - others: code repositories, custom apps,

The Requirements

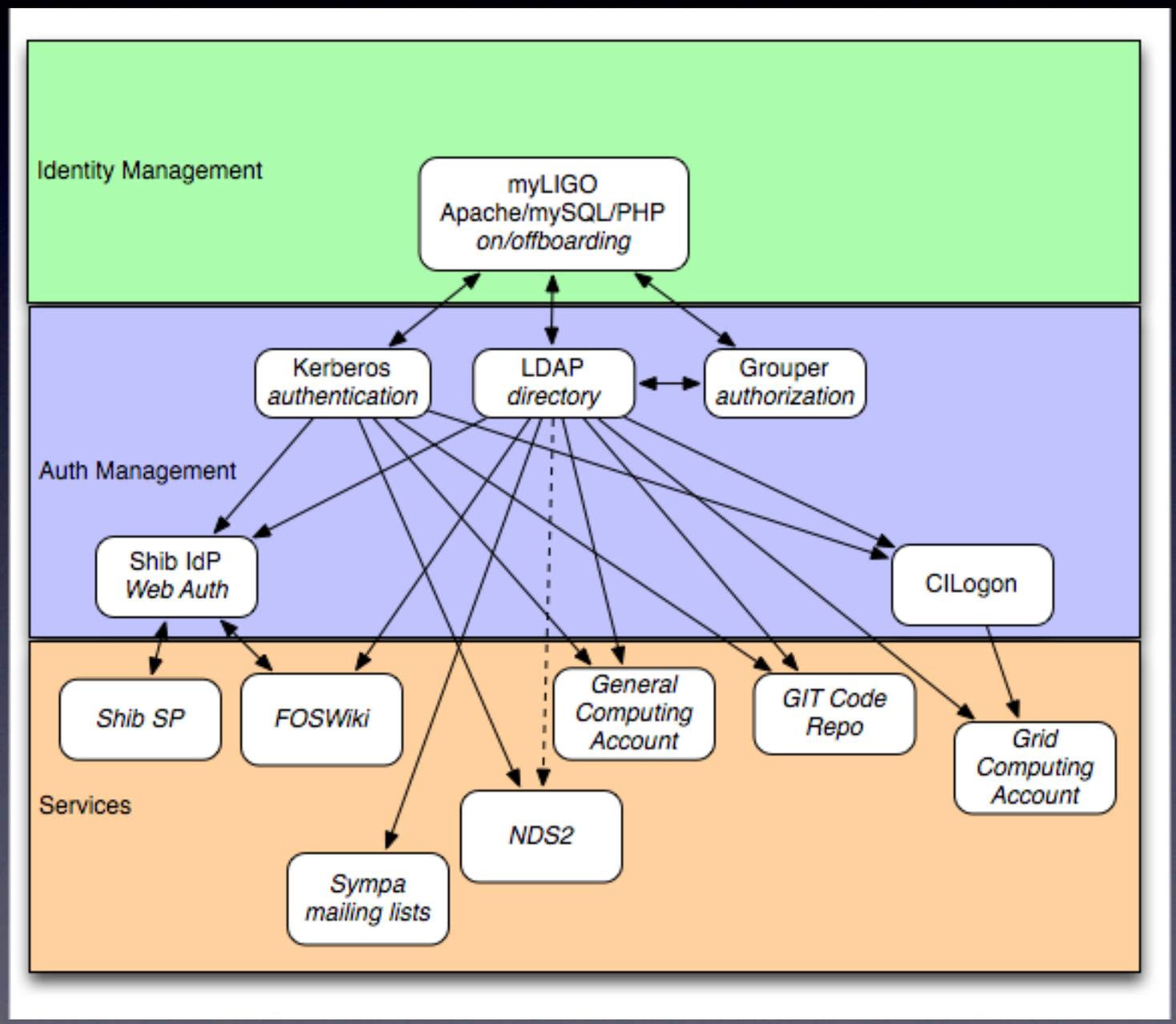
- Provide single sign-on solution (SSO) across application domains for LIGO users.
- Provide seamless onboarding for users when the join LIGO.
- Provide Identity Management platform for management with reporting functions.
- Provide redundancy and failover so that interferometer sites can operate independently from central infrastructure.

The Components

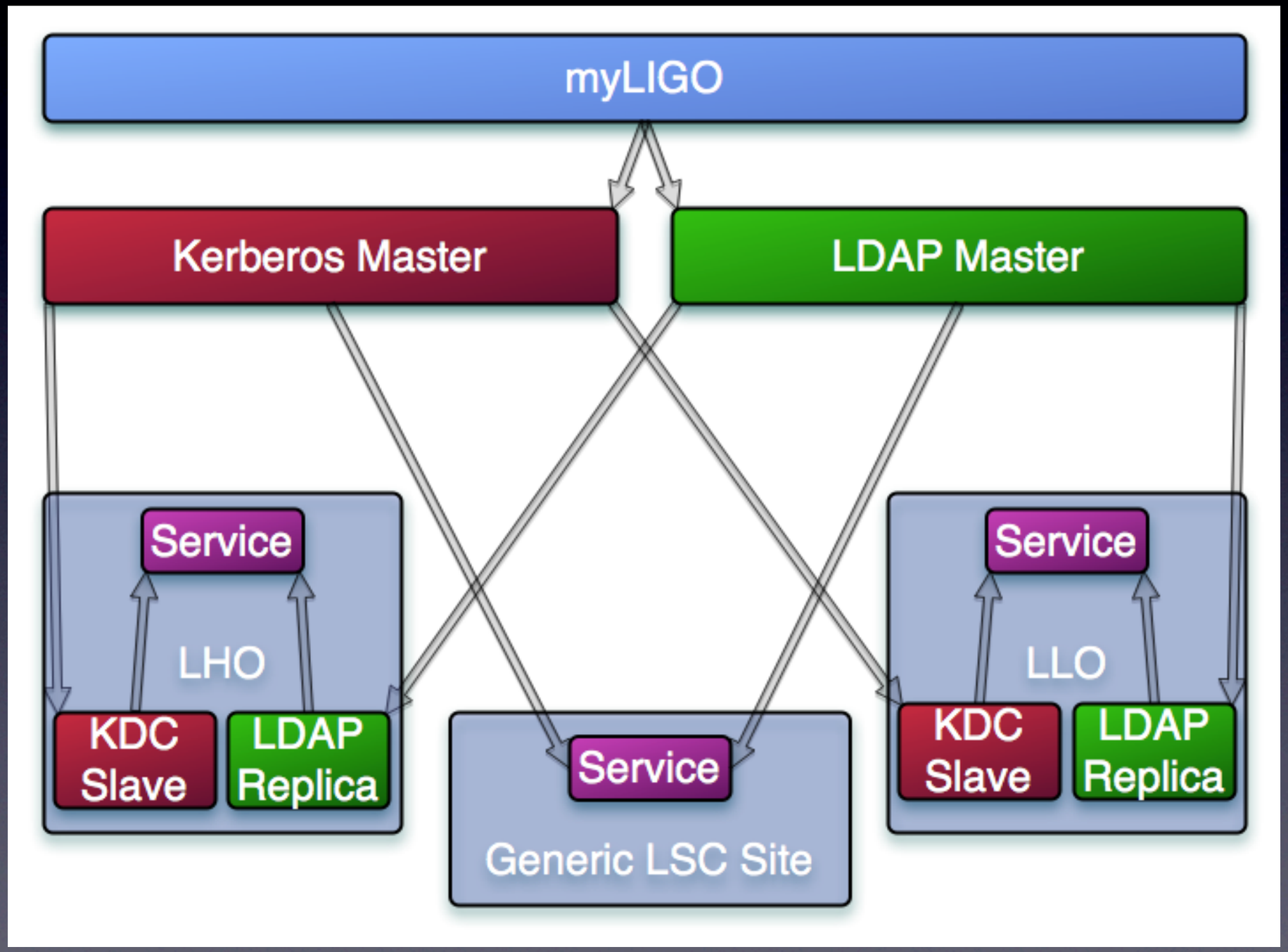
- Core components to infrastructure:
  - myLIGO: user registry. PHP and MySQL.
  - LDAP: directory store and attribute authority.
  - Kerberos: credential store and authentication.

- Auxiliary component:
  - Grouper: creates ACL groups in LDAP.
  - Shibboleth: provides SSO web authN/Z.
  - CILogon: converts kerberos authN into grid certificate.

Component Layers



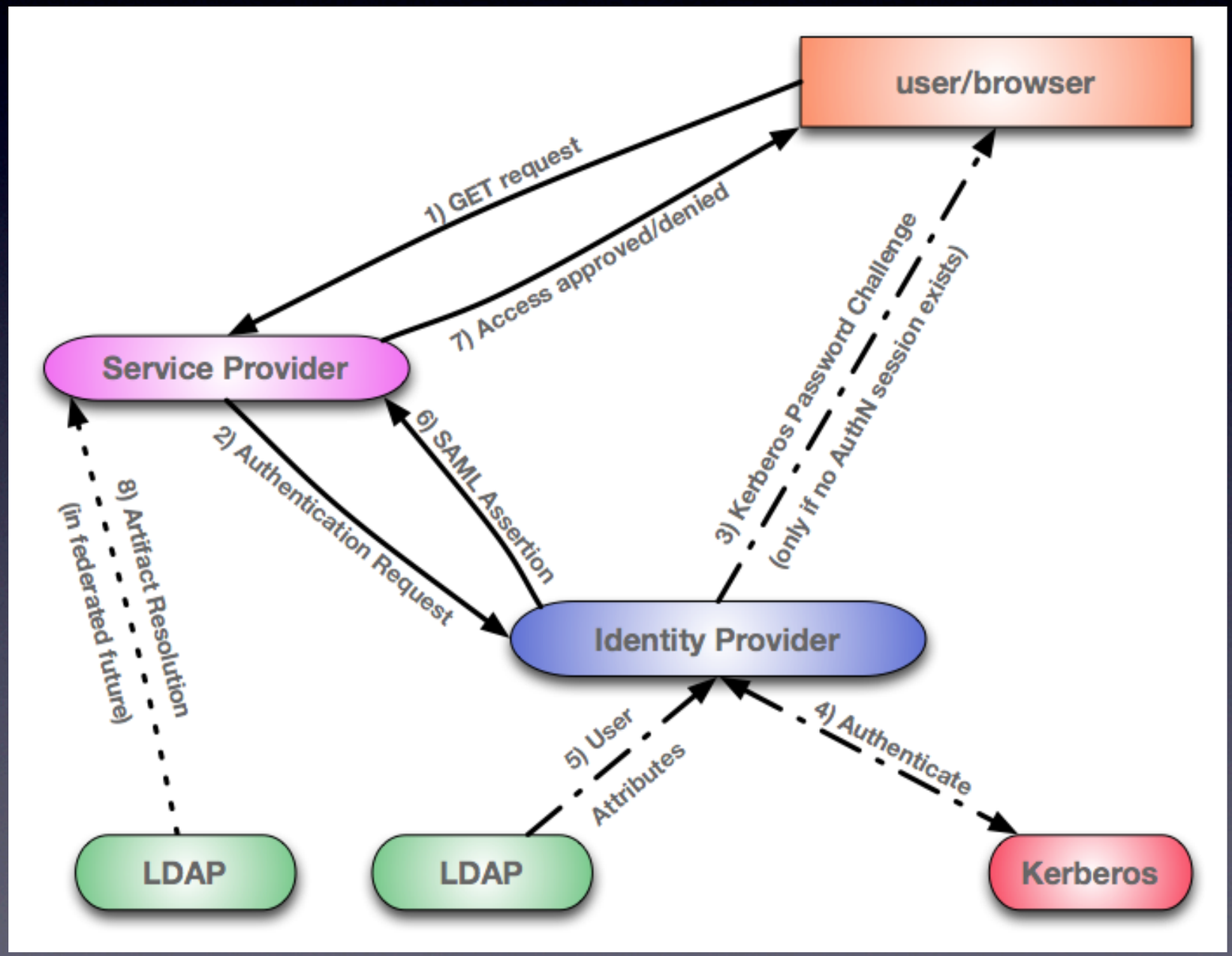
Core Redundancy



Application Domains: Web

- Shibboleth SSO across ligo.org domain.
- Five IdPs, ~125 SPs in metadata.
- Federated with InCommon.
- Uses LIGO.ORG realm KDC as credential store.
- Uses ligo.org LDAP as attribute authority.

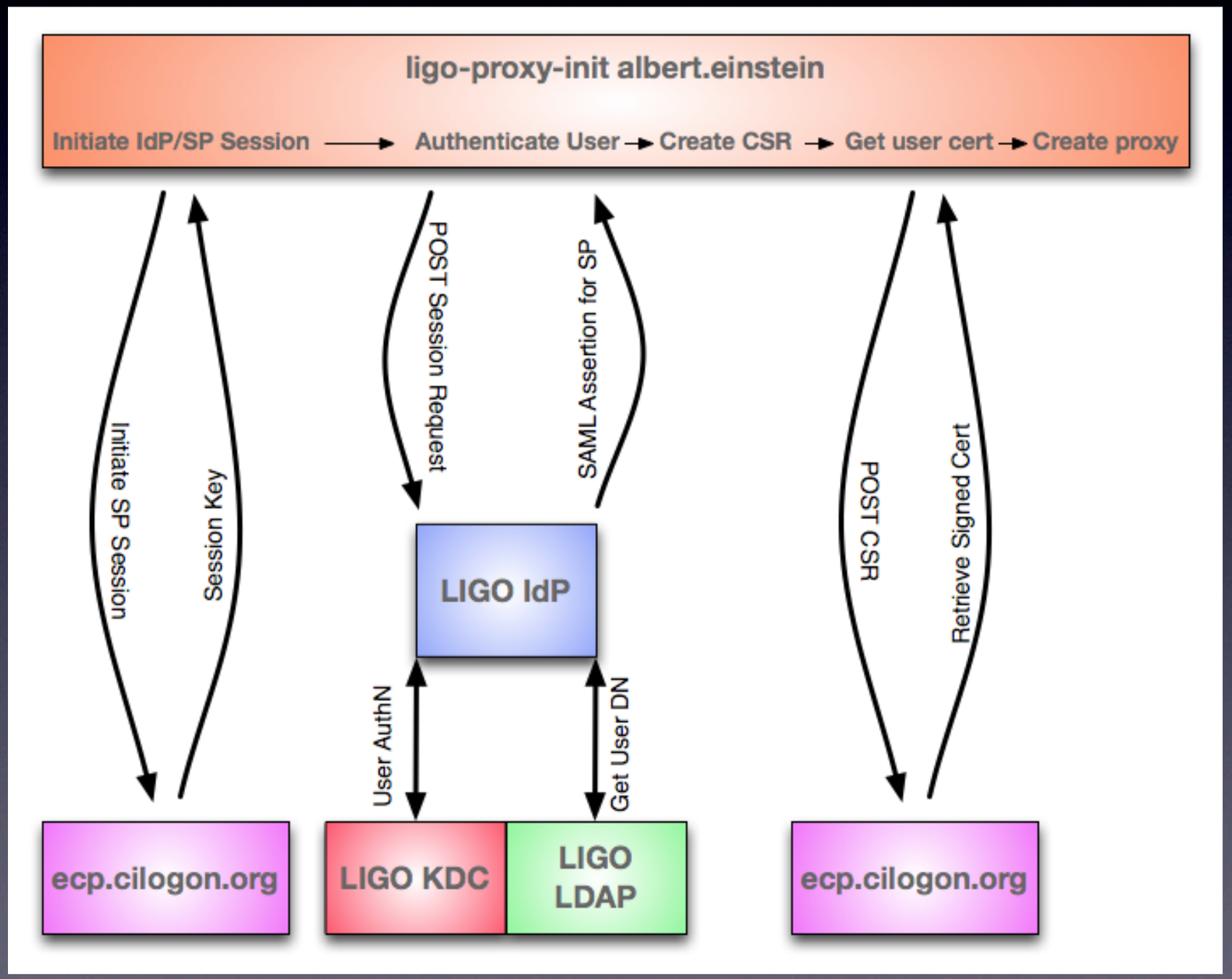
Application Domains: Web



Application Domains: Grid

- Based on SAML ECP and CILogon (http://www.cilogon.org/).
- User gets SAML assertion from LIGO IdP
  - Pass certificate DN and authentication assertion to CILogon SP.
  - Short-lived certificate and grid compliant proxy are issued by CILogon CA.

Application Domains: Grid



Application Domains: Other Services

- Other LIGO services also leverage LIAM infrastructure for AuthN/Z:
  - Mailing list subscribers stored as groups in LDAP, managed with grouper.
  - SVN and GIT repositories authenticate against kerberos.
  - Custom applications like NDS2 authenticate against kerberos.

Directions

- LIAM is moving toward leveraging federated identities for authentication of internal and external collaborators.
  - LIGO was an early InCommon member.
  - LIGO is a key contributor to developing COManage (Internet2 federated collaboration management platform).
  - LIGO is playing leading role in international inter-federation efforts.

LIGO and the IAM Community

- LIGO is a leader in identity management for large virtual research organizations:
  - many invited talks every year on how we do IAM.
  - early members of Shibboleth Consortium.
  - invited to serve on various advisory panels, committees, etc