

Making Computational Resources Accessible to APS Users

The Players

- Rachana Ananthakrishnan (MCS – Security)
- Francesco DeCarlo (APS – LDRD)
 - ◆ decarlo@aps.anl.gov
- Dan Fraser (MCS PI – LDRD)
 - ◆ fraser@mcs.anl.gov
- Raj Kettimuthu (MCS – Data)
 - ◆ Mike Link, John Bresnahan
- WanTao Lee (LDRD Integration)
- Brian Tieman (APS - LDRD)
 - ◆ tieman@aps.anl.gov

Outline

- Current Usage Scenario
- Requirements for user access
- Proposed components
- Usage scenarios enabled
- Deployment Discussion

Current Usage Scenario

- PI and group are granted experiment access
 - ◆ Beam line access in order of days
 - ◆ Facility access in order of months
- Beam line data stored in local machine under single account
- Data staged to intermediate storage under a common account
- Quasi-real time processing of the data
- Transferred to home institution
 - ◆ Anonymous FTP server
 - ◆ USB sticks

Current Scenario Drawbacks

- Data acquired by user on shared beam account
 - ◆ Accessible to other users
- No standard provisions for transfer of data to intermediate storage
 - ◆ Frequent users use copy to move data
- No offsite access to data in intermediate storage
 - ◆ Requires staff intervention
- Not good performance on off-site data transfer

Requirements

- **Data:**
 - ◆ Allow for transfer of the acquired data to a remote location of user's choice.
 - ◆ Protect experiment data such that access is restricted to only scientific group participating in that experiment
 - ◆ Data encryption as an option
- **Security policy**
 - ◆ Access policy on scientific group, rather than per user.
 - ◆ Track individual user access for audit purposes
 - ◆ Support for individual users belonging to multiple groups
- **Credentials**
 - ◆ Low overhead mechanism to issue credentials to users
 - ◆ No shared passwords or credentials
 - ◆ Light weight user clients for credentials management and data download
 - ◆ Automated trust root provisioning of client machines

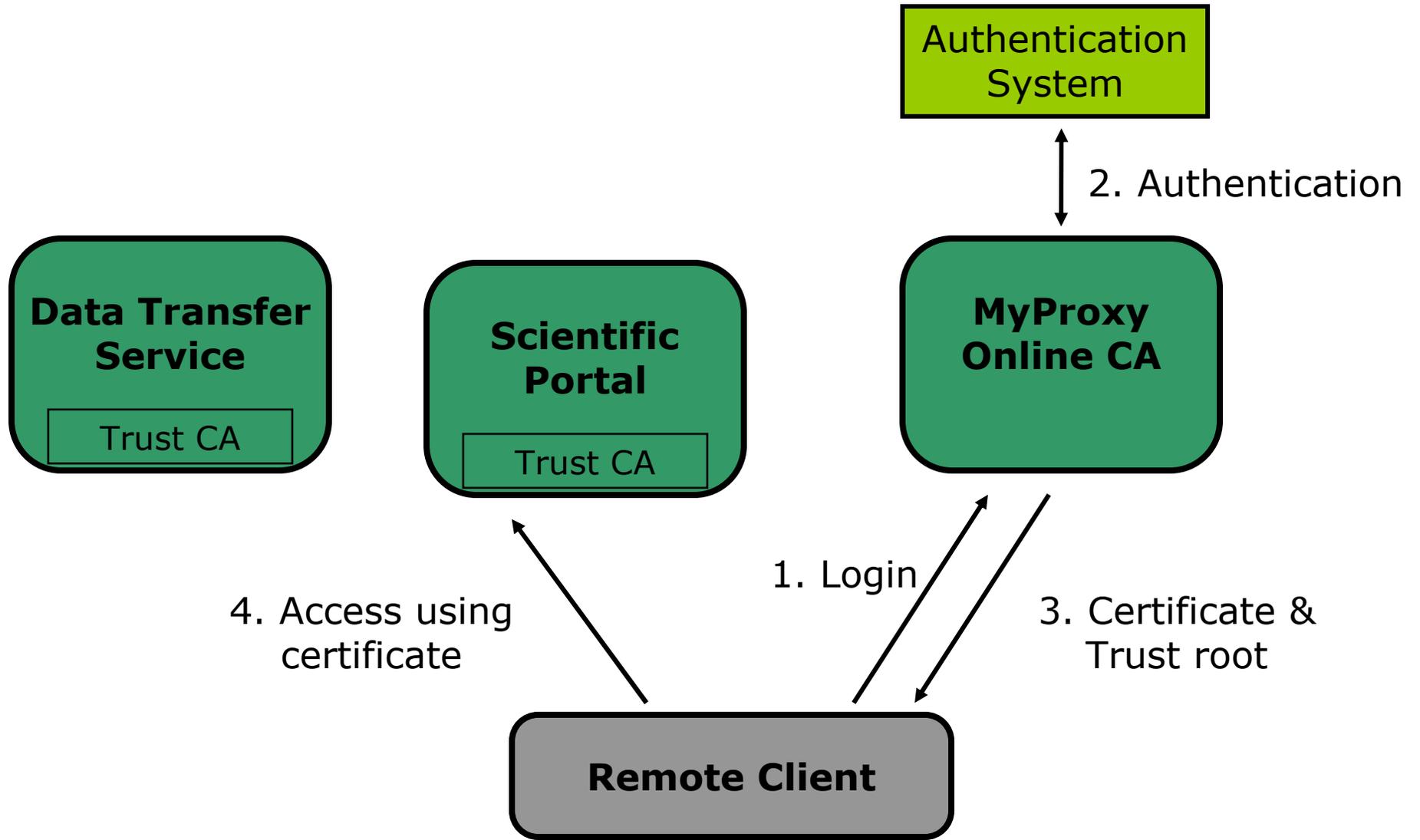
Proposed Components

- **Credential Service**
 - ◆ Issues short lived certificate to authenticated users
- **Data Transfer Service**
 - ◆ Provides fast and reliable remote download of data to user resources
- **Mapping Software**
 - ◆ Maintains mapping from user certificate to local account on APS machines
- **Scientific Portal**
 - ◆ Provides secure and efficient access to local computational resources

Credential Service

- MyProxy Online CA
 - ◆ Developed at NCSA and part of Globus Toolkit
 - ◆ Issues short term credentials to authenticated users
 - ◆ Any authentication system can be plugged in using PAM module
 - ◆ Auto provisioning of trust roots
 - Trusted Certificate Authorities and Certificate Revocation Lists
- MyProxy Clients
 - ◆ Endpoint available to remote users
 - ◆ Client package as separate deployment, including Java clients and API
 - ◆ MyProxy login and log-out

MyProxy Online CA Use



Data Transfer Services

- GridFTP
 - ◆ High-speed data transfer service
 - ◆ Transfers files off standard file system
 - ◆ Server runs as a service listening at well known endpoint
 - ◆ Client library in Java and C

Mapping Software

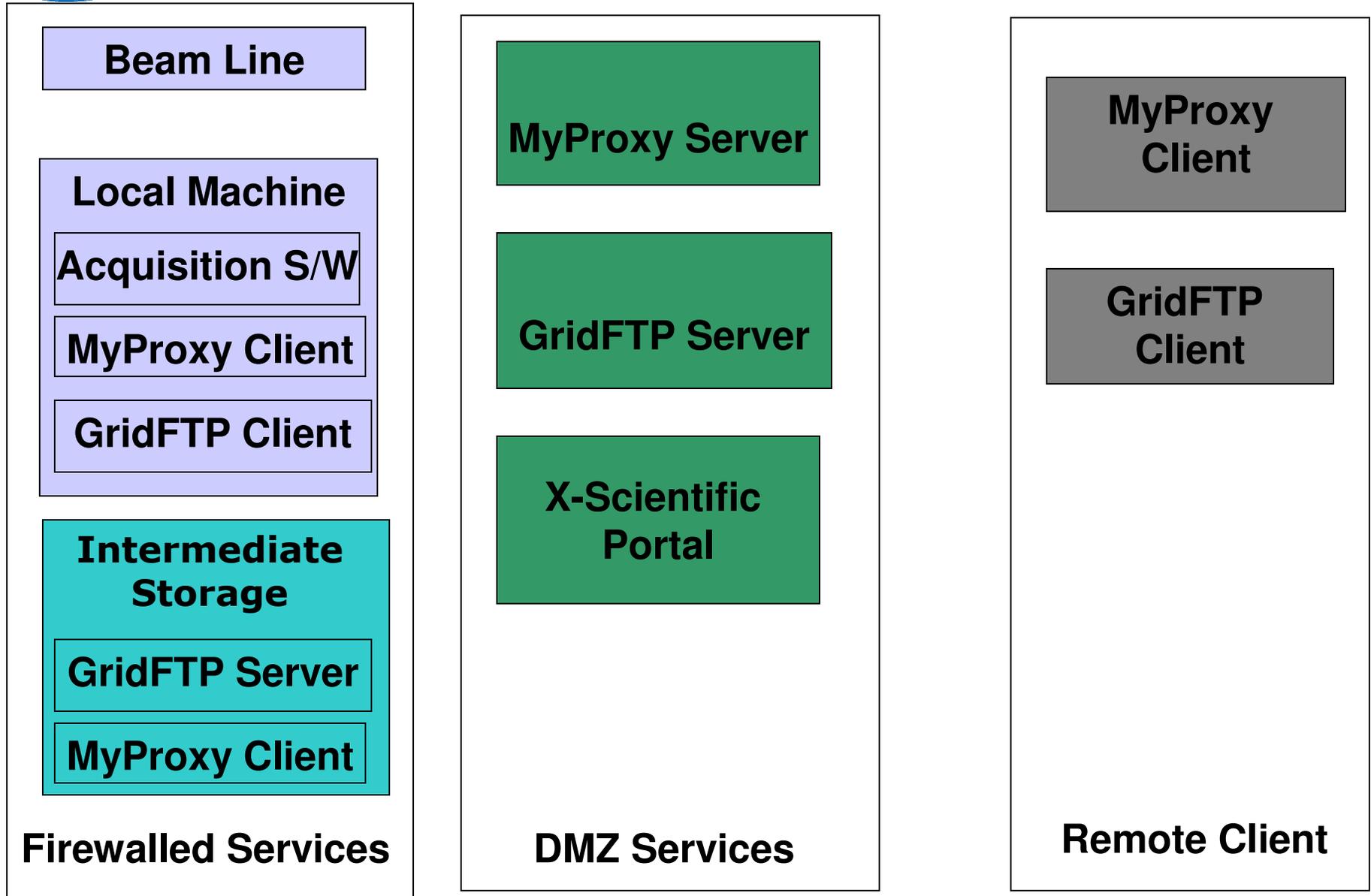
- Gx-map
 - ◆ Locally installed software
 - ◆ No remote access
 - ◆ User from local machine requests mapping to account
 - ◆ User certificate identity mapped to local account logged in
 - ◆ Eliminates administrative overhead of mapping user

Scientific Portal

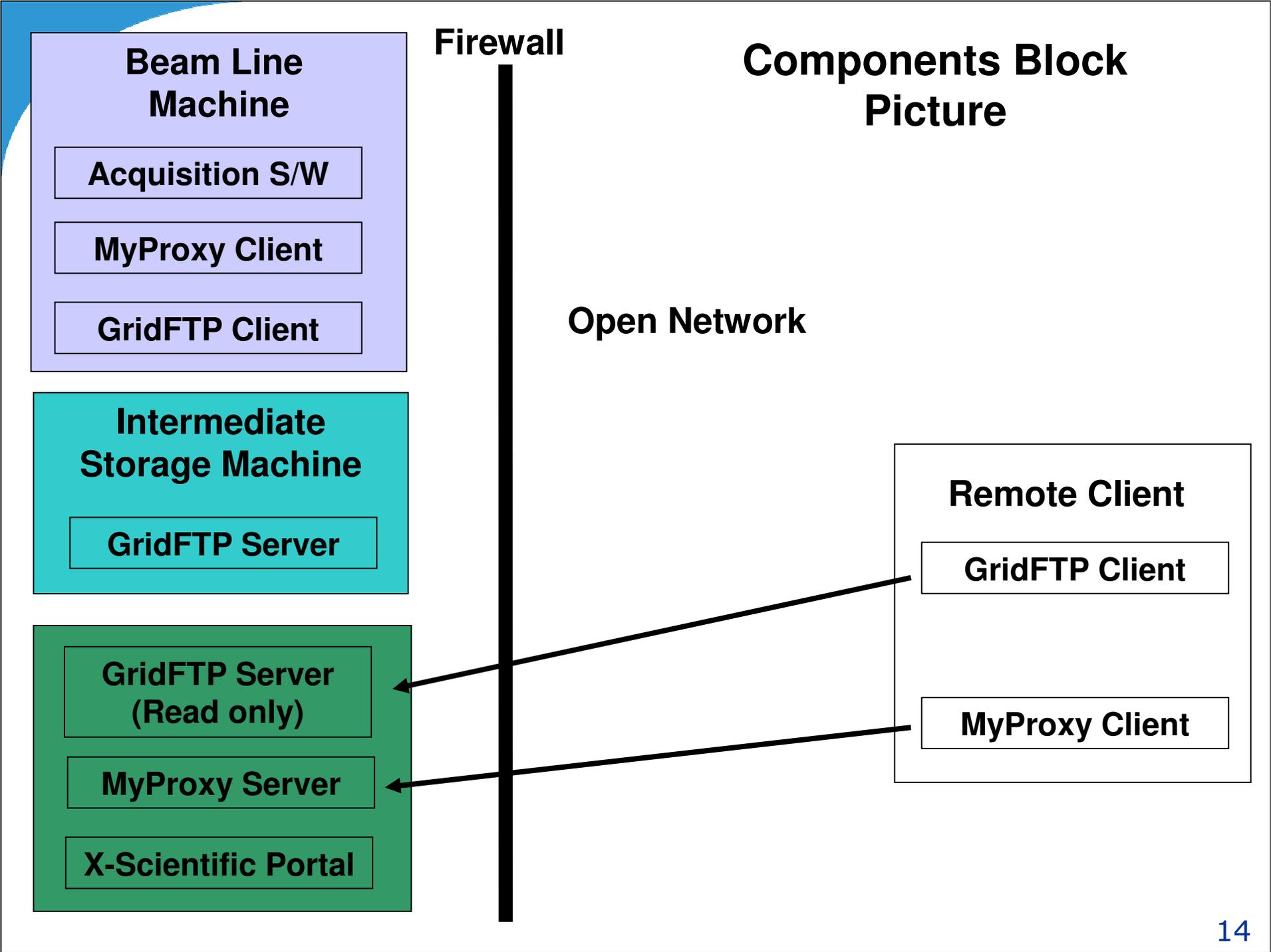
- Provides access to local computational resources
 - ◆ Access to scientific applications as services
 - Tomography
 - High Energy X-Ray MicroDiffraction
 - X-Ray Photon Correlation Spectroscopy
 - ◆ End user processes own data
 - ◆ Can workflow data processing with data movement to leverage other computational facilities outside the APS



Components Block Picture



Components Block Picture



Usage Scenario

- Setup:
 - ◆ Alice and Bob in scientific group (SG1)
 - ◆ Group granted account on intermediate storage (SG-group1)
 - ◆ Alice and Bob granted individual accounts on authentication system
 - ◆ Each user logs onto SG-group1 and runs gx-map

Usage Scenario Cont.

- **Beam Machine Access**
 - ◆ Alice uses MyProxy Client to obtain credential
 - ◆ Uses the GridFTP client to initiate real time transfer of acquired data to SG1-group account
 - ◆ Delete local data at end of run
 - ◆ MyProxy log-out to remove local credential
 - ◆ Similar access for Bob to same group account, but his own credential

Usage Scenario Cont.

- Remote access
 - ◆ Alice from remote machine contacts MyProxy Online CA
 - Credentials and trusted CA/CRLs downloaded
 - ◆ Run GridFTP client to initiate transfer of data
 - Only data in SG-group1 can be accessed because of mapping
 - ◆ MyProxy log-out to delete credential once download is complete
 - ◆ Similar access to Bob

Usage Scenario Cont.

- Individual user in multiple users
 - ◆ Alice belongs to SG-group1 and SG-group2
 - ◆ Obtains credentials from MyProxy OnlineCA using individual account login
 - ◆ While using transfer clients, choose account to use: SG-group1 or SC-group2

Suggested Deployment

