April 17, 2014

Globus World
March 5, 2014

XSEDE IdM Design Highlights

Randy Butler

XSEDE

Extreme Science and Engineering Discovery Environment

XSEDE Overview

XSEDE

Extreme Science and Engineering Discovery Environment

- The Extreme Science and Engineering Discovery Environment (XSEDE) is the most advanced, powerful, and robust collection of integrated digital resources and services in the world. It is a single virtual computing system that scientists can use to interactively share resources, data and expertise.
- Scientists, engineers, social scientists, and humanities experts around the world.

XSEDE Overview

- XSEDE integrates these resources and services, makes them easier to use, and helps more people use them.
  - XSEDE supports more than a dozen super-computers and high-end visualization and data analysis resources.
  - XSEDE's integrated, comprehensive suite of services connects with other high-end facilities and
  - campus-based resources, serving as the foundation for a national computing ecosystem.
- XSEDE's advanced digital services are common authentication and security mechanisms, global namespace and filesystems, remote job submission and monitoring, and file transfer services.

Why are we changing the way XSEDE handles Identity Management?

- Long range strategy to leverage what we hope is a bigger wave of development and advancement of identity and group management
- Leverage of a larger effort rather than building XSEDE specific solutions
- Leverage of 1 –to- Many versus N –to- N trust relationships

Driving Forces

- Identified by XSEDE Architecture and Design Team as essential to advancing US Science
- There are three major types of user interactions
  - Traditional HPC
  - Science Gateway
  - Campus Bridging

XSEDE A&D's Vision for Identity and Group Management

- Three subsystems need to be implemented
  - **Identity management** with federation
  - **Group management** with federation
  - **Profile (User/group) management** with federation

- It was expected that any solution would require extensive development, integration, testing and rollout periods

Identity and Group Federation

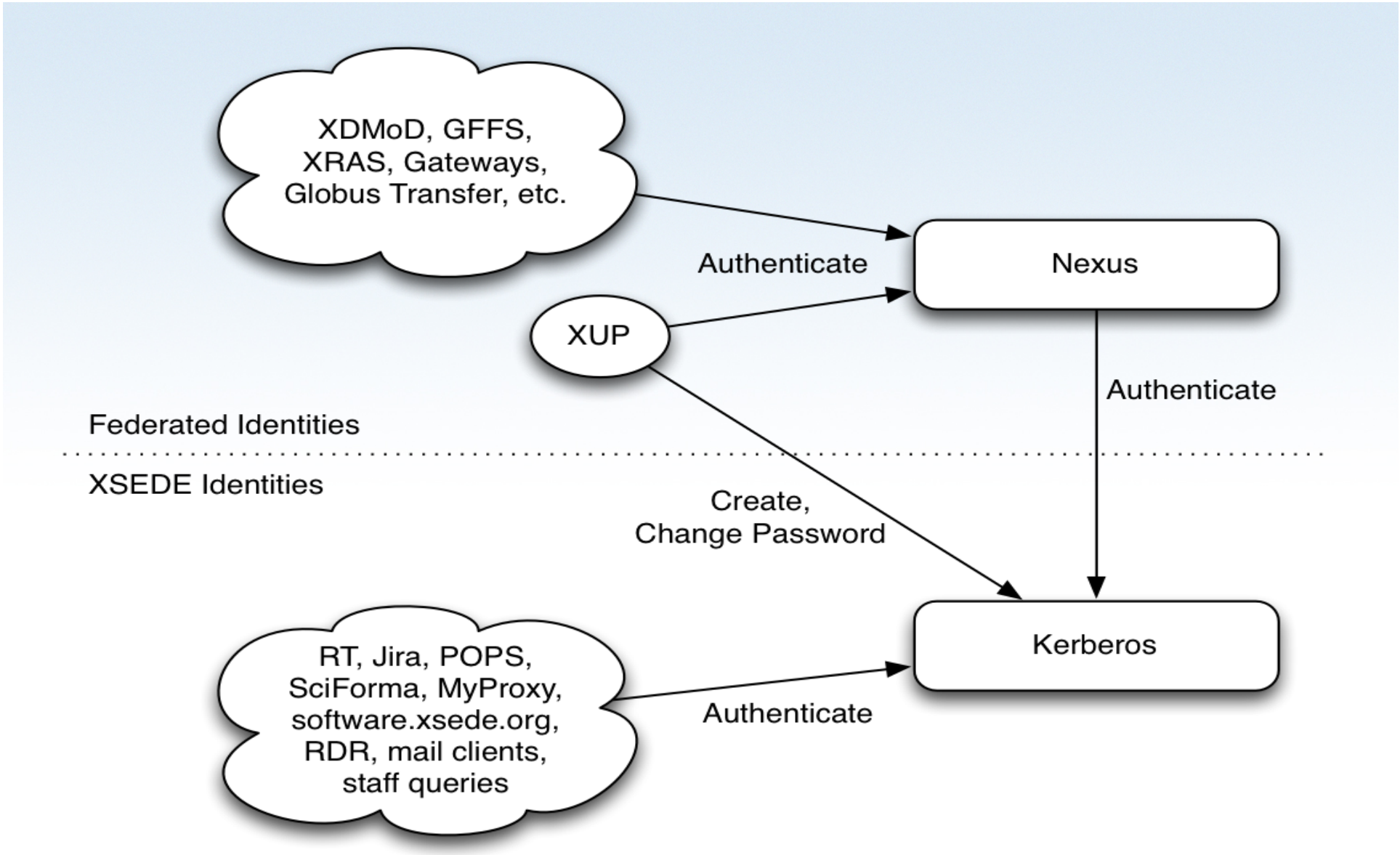
- **Identity federation** enables the portability of identity information across otherwise autonomous security domains
  - Enables credential holders from a trusted domain to securely access systems of another trusted domain seamlessly.
- **Group federation** and **metadata federation** for group definitions and user profiles, respectively

Advancing the XSEDE IdM system

- What existed
  - Set of requirements and use cases
  - High-level architecture
  - Understanding of the current XSEDE IdM system
    - XRAS, XUP, XDMOD, XDCDB, KDC, AMIE, etc…..
  - Proposal from the XUAS architects
- From these a cross-cutting team of stakeholders generated a draft design that meets the requirements & use case scenarios

Design Highlights

- Look and feel of XSEDE remains the same for XSEDE users
- The design incorporates Globus Nexus
- Support for Federated
  - Identities
  - Groups
  - Profile (to come later)
- Minimized Risk by maintaining the XSEDE KDC
- Phased rollout – two phased approach


XDMoD, GFFS,
XRAS, Gateways,
Globus Transfer, etc.
Authenticate
Nexus
XUP
Authenticate
Federated Identities
XSEDE Identities
Create,
Change Password
Kerberos
RT, Jira, POPS,
SciForma, MyProxy,
software.xsede.org,
RDR, mail clients,
staff queries
Authenticate

Globus Nexus Provides

- Federated Identities
  - Identity bindings
  - 3rd party authentication services
    - CILogon/Incommon
      Google
  - Identity profile metadata
  - Oauth 2.0 support
- XSEDE specific
  - Authentication to XSEDE KDC
  - Email coordination services
- Federated Group Management
  - Creation and distribution of group memberships
  - Group profile metadata

Nexus interface highlights

- No XSEDE passwords will be stored by Globus Nexus
- Nexus will not have KDC admin rights
- Nexus is back-ended by the XSEDE KDC for XSEDE domain identity authentication services
- Federated Identities will be authenticated via Nexus directly

No need to change legacy systems

- Legacy systems still authenticate directly via XSEDE KDC – no change
  - MyProxy
  - RT trouble ticket system
  - SDSC
  - Jira
  - Sharepoint
- If it isn't XRAS, XUP or XDMOD it doesn't need to change

"This work used the Extreme Science and Engineering Discovery Environment (XSEDE), which is supported by National Science Foundation grant number OCI-1053575."


Our reach will forever
exceed our grasp, but,
in stretching our horizon,
we forever improve our world.
XSEDE
Extreme Science and Engineering
Discovery Environment