Overview of OGC Testbed-14 D023 (OGC 18-090r1) Federated Cloud Engineering Report

Dr. Craig A. Lee, lee@aero.org
Senior Scientist
The Aerospace Corporation

OGC Innovation Program and Testbed-14 demo day
ESA/ESRIN, Frascati, Italy
January 24, 2019

OGC®
Making location count.

Goal

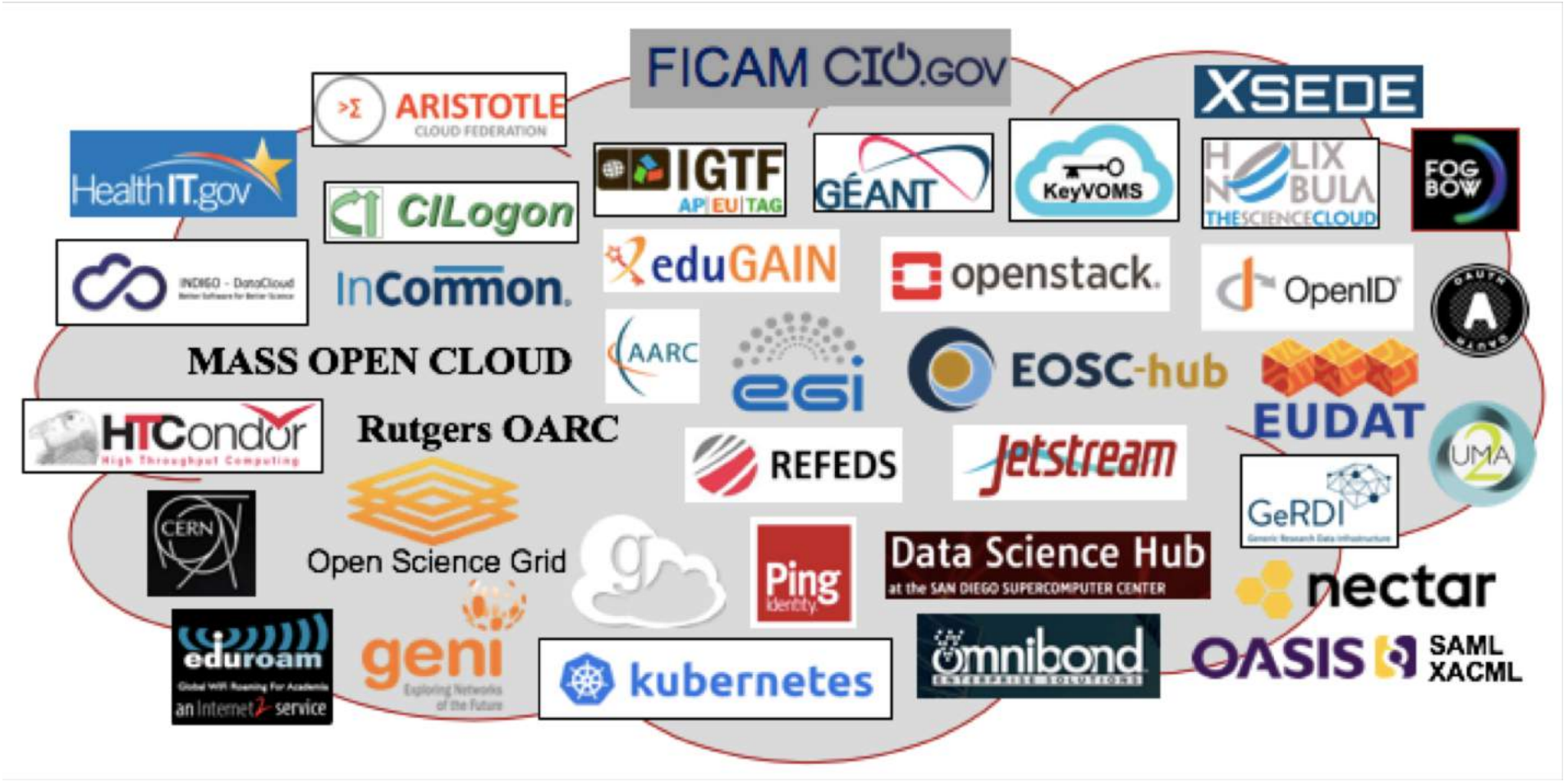
- **Evaluate the Testbed-14 federation efforts**
- **Make recommendations for future work**

Approach

- Understand the cloud – and general – federation design space
  - Use the NIST Federated Cloud Reference Architecture as a "yardstick"
- Understand the current landscape of federation systems and tools
  - Survey a wide range of existing systems, tools, and standards
  - ~32 surveyed with 11 more identified
- Evaluate the federation components built in Testbed-14
  - Authorization Server
  - Mediation Server
  - Workflow Securitization
  - Federated Cloud Securitization
- Derive insights and make recommendations

OGC®

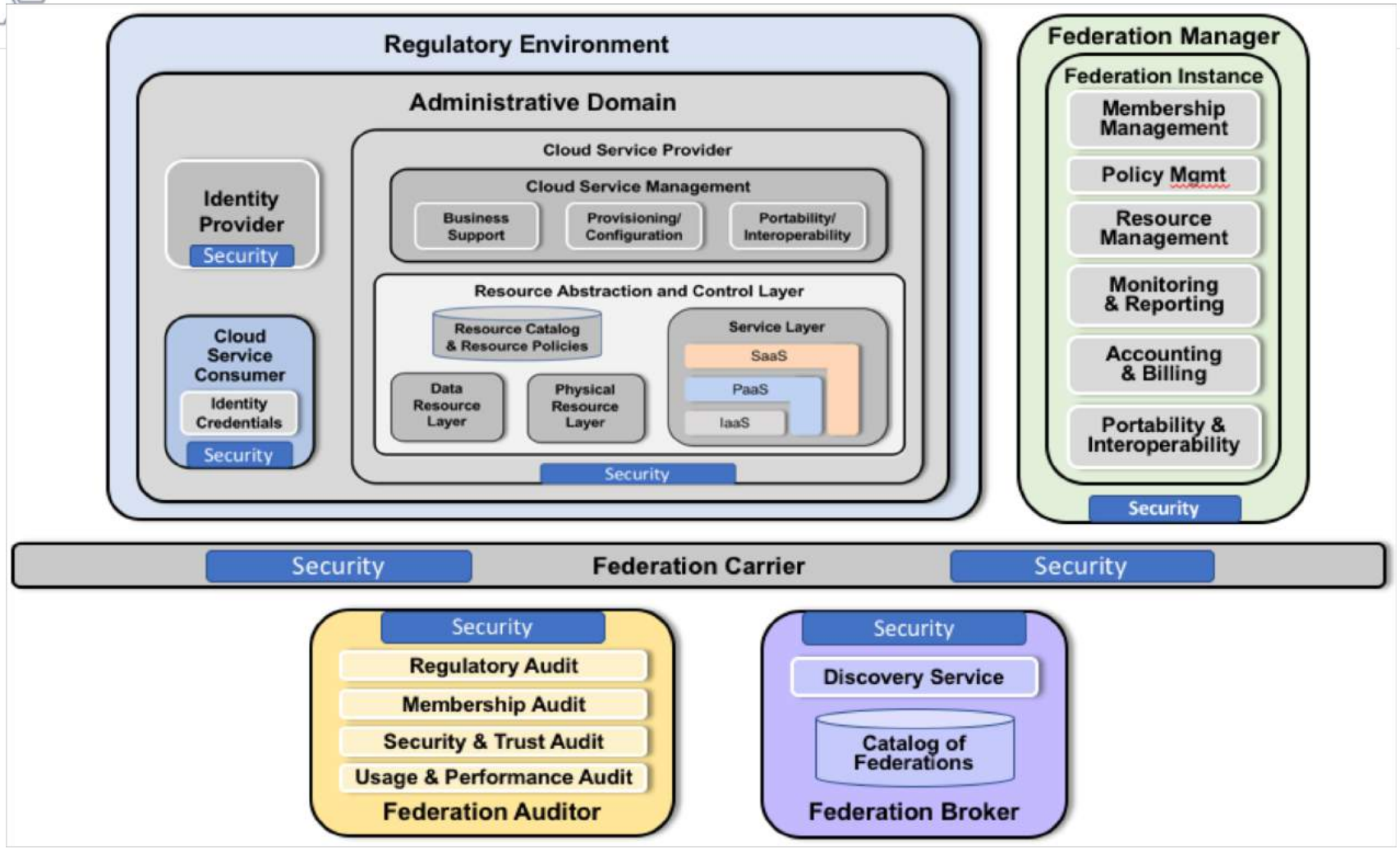
The Federation Landscape: A Logo Cloud



How can we make sense of all this?

OGC®

One Possibility:
The NIST Federated Cloud Reference Architecture (draft)



This is a Conceptual Actor/Role-Based Model!
It is not prescriptive of any particular implementation approach

OGC®

Fundamental Insights Realized in Testbed-14

- Existing federation-relevant systems are commonly:
  - External *federation providers with "baked-in" governance*
  - For a narrow fixed purpose, e.g., cloud infrastructure services
  - *Not* easy *to deploy your own federated environment with tailored* purpose and *governance*
- Existing, federation-relevant standards based on the assumption of operating in the open Internet where anybody can attempt to invoke a service
  - For example: OpenID, OAuth, OpenID Connect, UMA
  - No assumption of any pre-existing relationships (beyond basic trust relationships) to govern the collaboration among partners
- Federation-specific models explicitly manage these relationships
  - For example: the NIST Federated Cloud Reference Architecture
  - Resource discovery and access policies can be jointly agreed upon and enforced by federation members

Recommendations

1. Clearly define and demonstrate how federated identity can be consistently managed and used.
2. Clearly define and demonstrate how the scope of attributes and authorizations can be used to consistently manage federated environments.
3. Clearly define and demonstrate how resource discovery and access can be consistently managed across all participating administrative domains.
4. Clearly define and demonstrate how federation administration is done.
5. Strategize on the development and use of federation deployment models.
6. Clearly identify and evaluate implementation trade-offs with regards to practical adoption issues, e.g., modifications to existing services.
7. Investigate and evaluate the benefits and necessary investment for developing purpose-built standards and tooling.
8. Develop awareness and understanding at the organizational level of the purpose and need for Trust Federations.

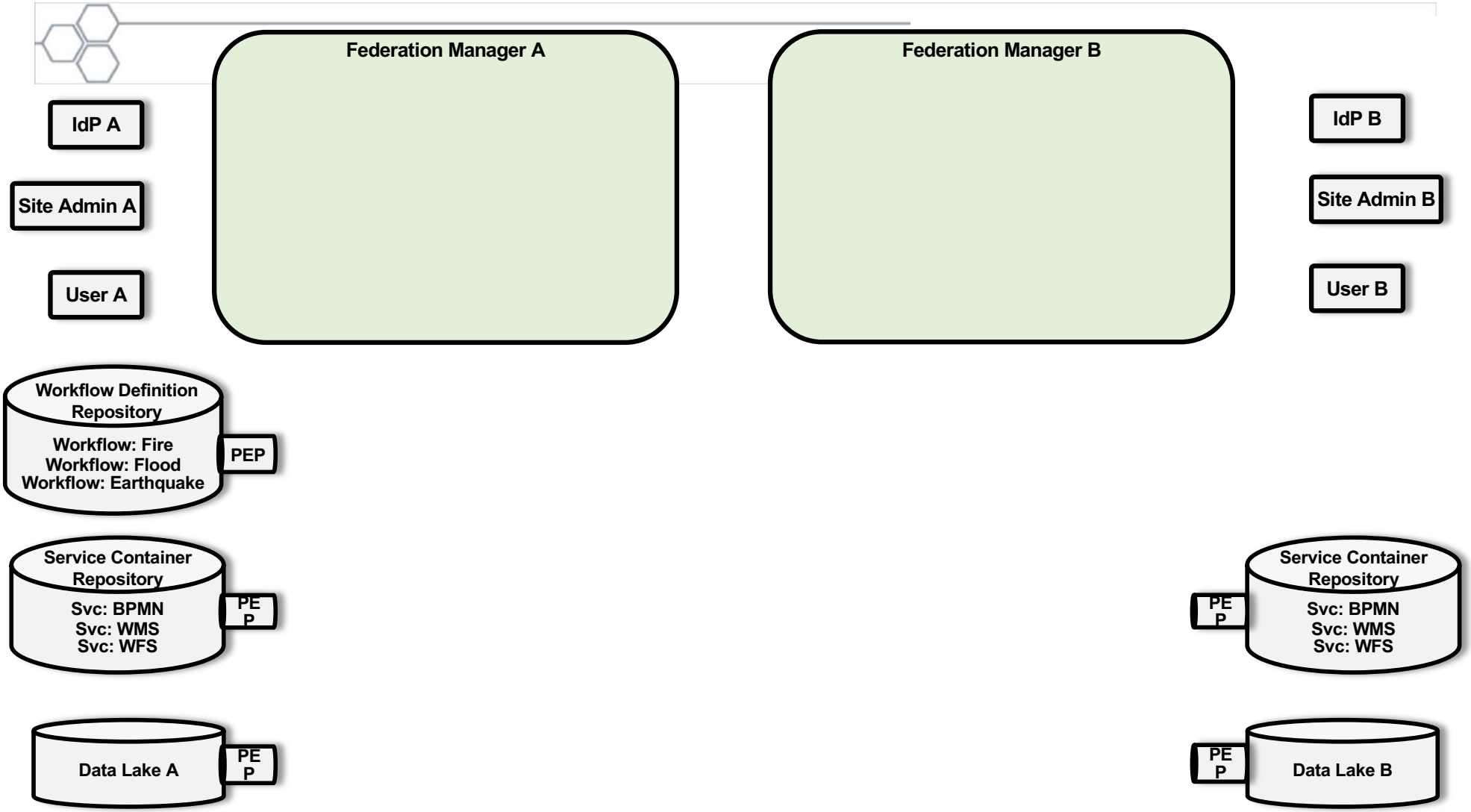
R2 is in progress to revise/expand the survey section

OGC®

Beyond TB-14: Going from Conceptual to Concrete

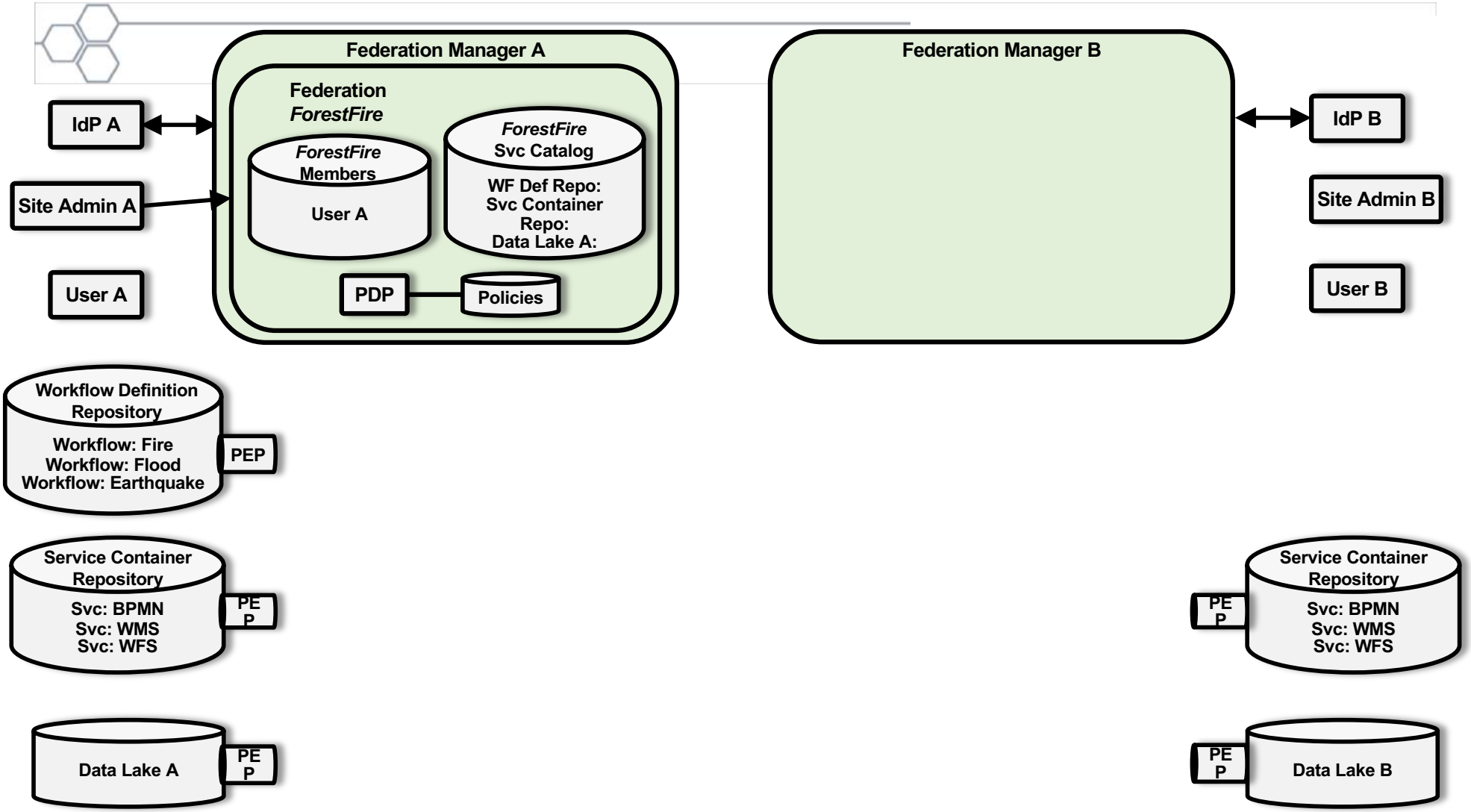
- The NIST Fed Cloud Ref Arch is by nature conceptual
  - Takes a step back to understand the entire federation *design space*
  - Identifies a spectrum of *deployment* and *governance models*
- It is critical that we show how these concepts can be mapped to concrete implementations!
  - This is the purpose of Appendix B in the NIST Ref Arch doc
- *The Forest Fire Workflow Use Case*
  - A workflow needs to access different data repositories with different data owners
    - This use case has been mentioned by several different stakeholders
  - Two organizations that run their own internal, pairwise, P2P Federation Managers, along with other services
  - (This is work-in-progress in the NIST Public WG on Federated Cloud)

The System Components



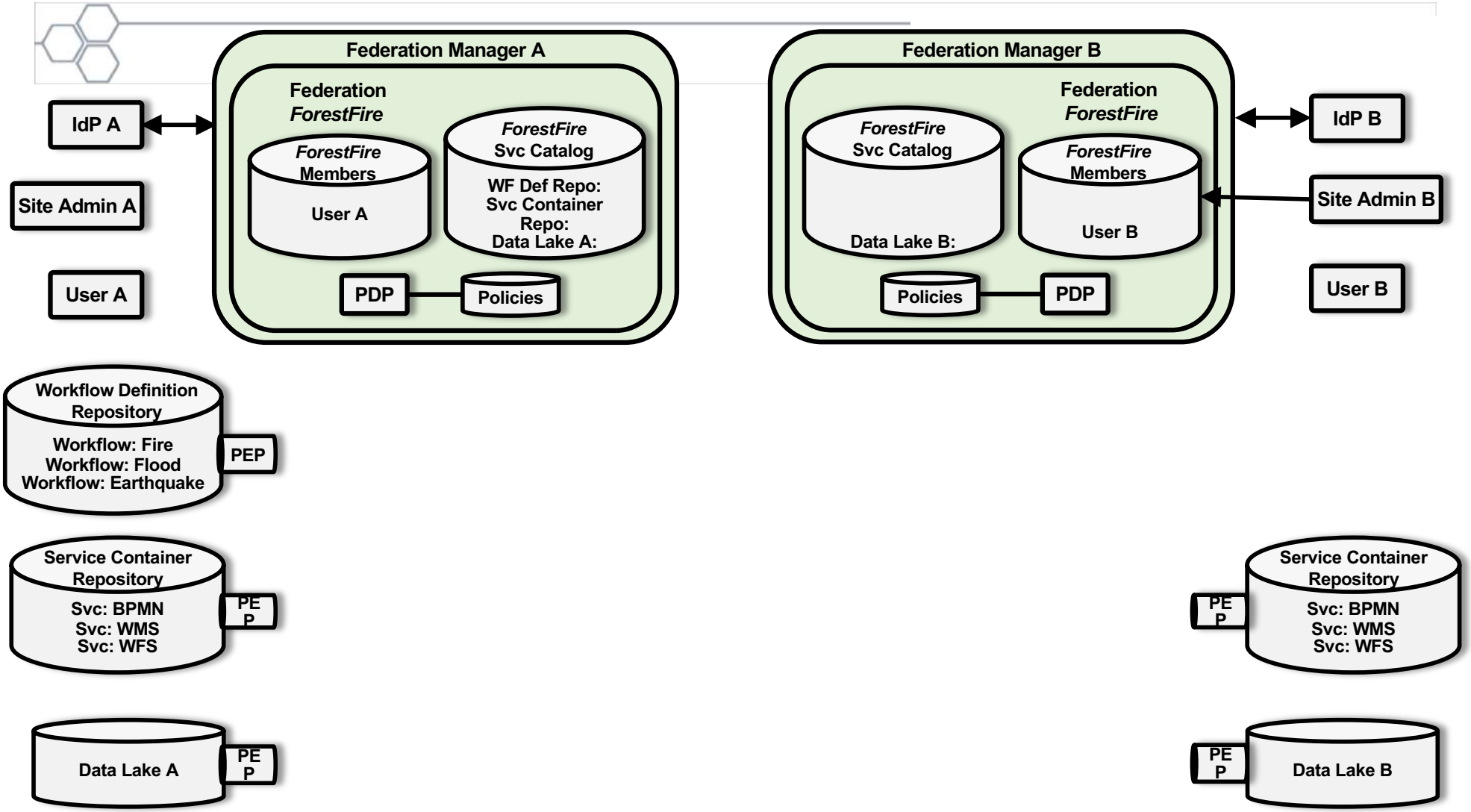
OGC®

Site Admin A Instantiates Federation *ForestFire*



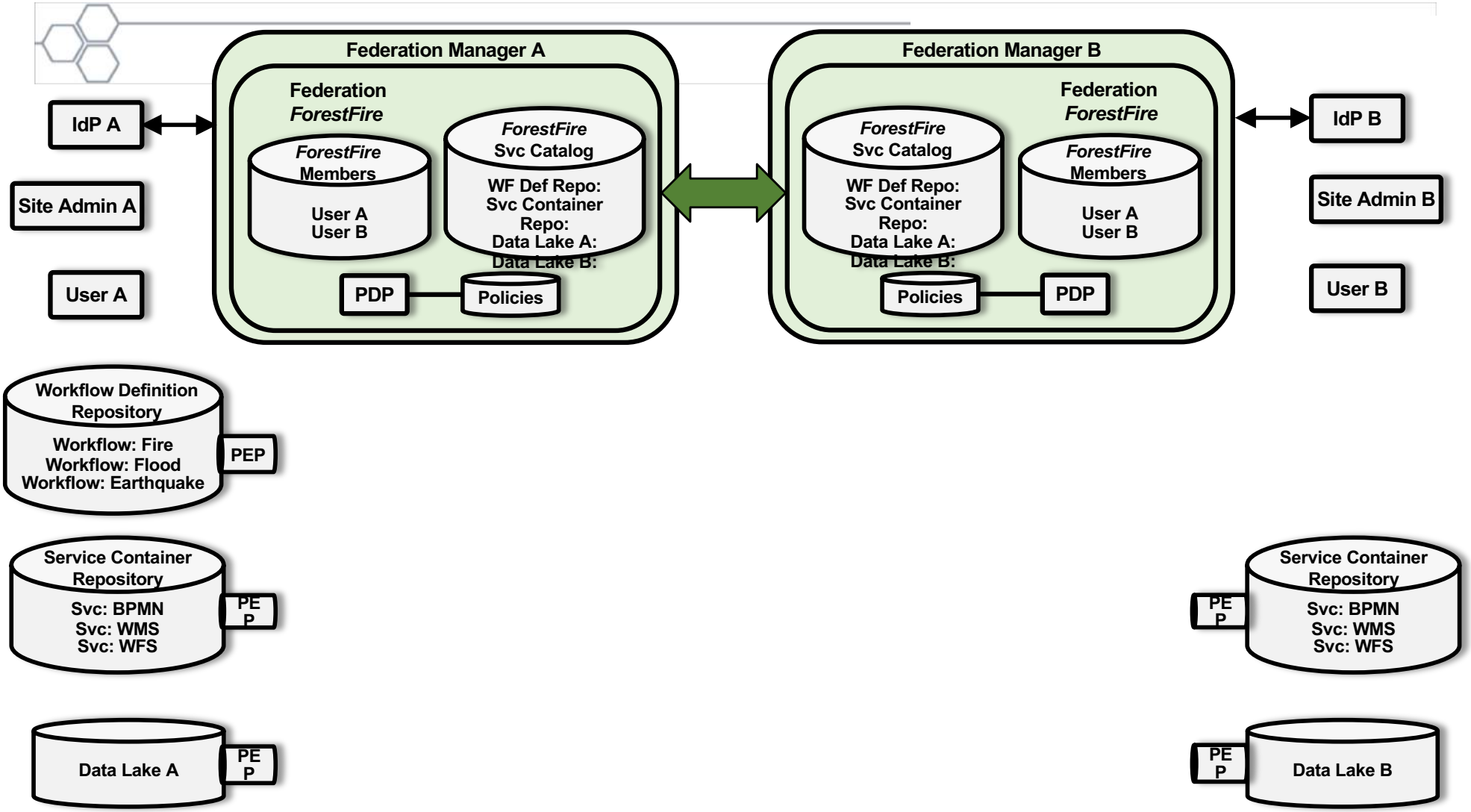
OGC®

Site Admin B Decides to Join *ForestFire*



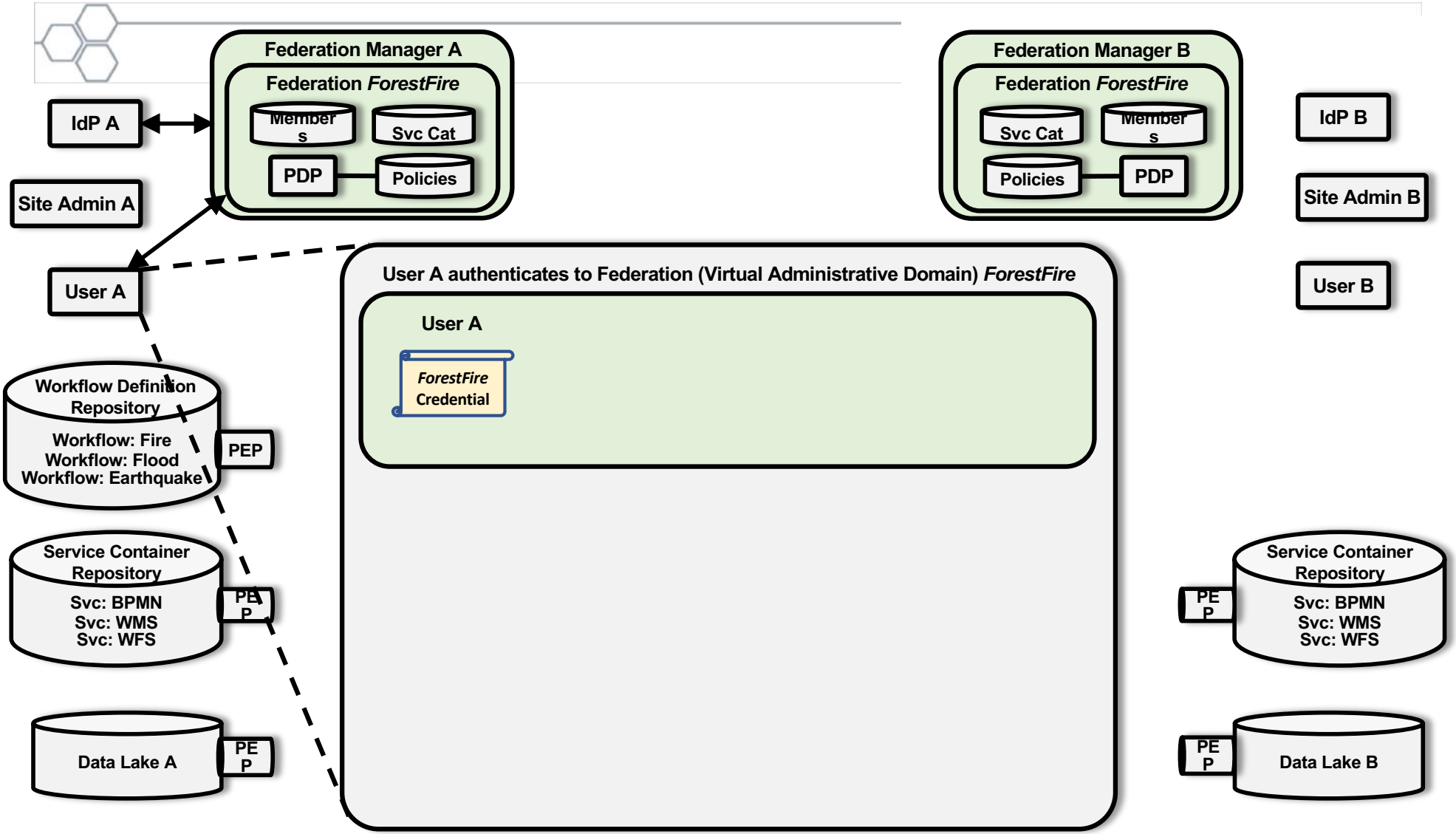
OGC®

The Federation Managers Eventually Synchronize



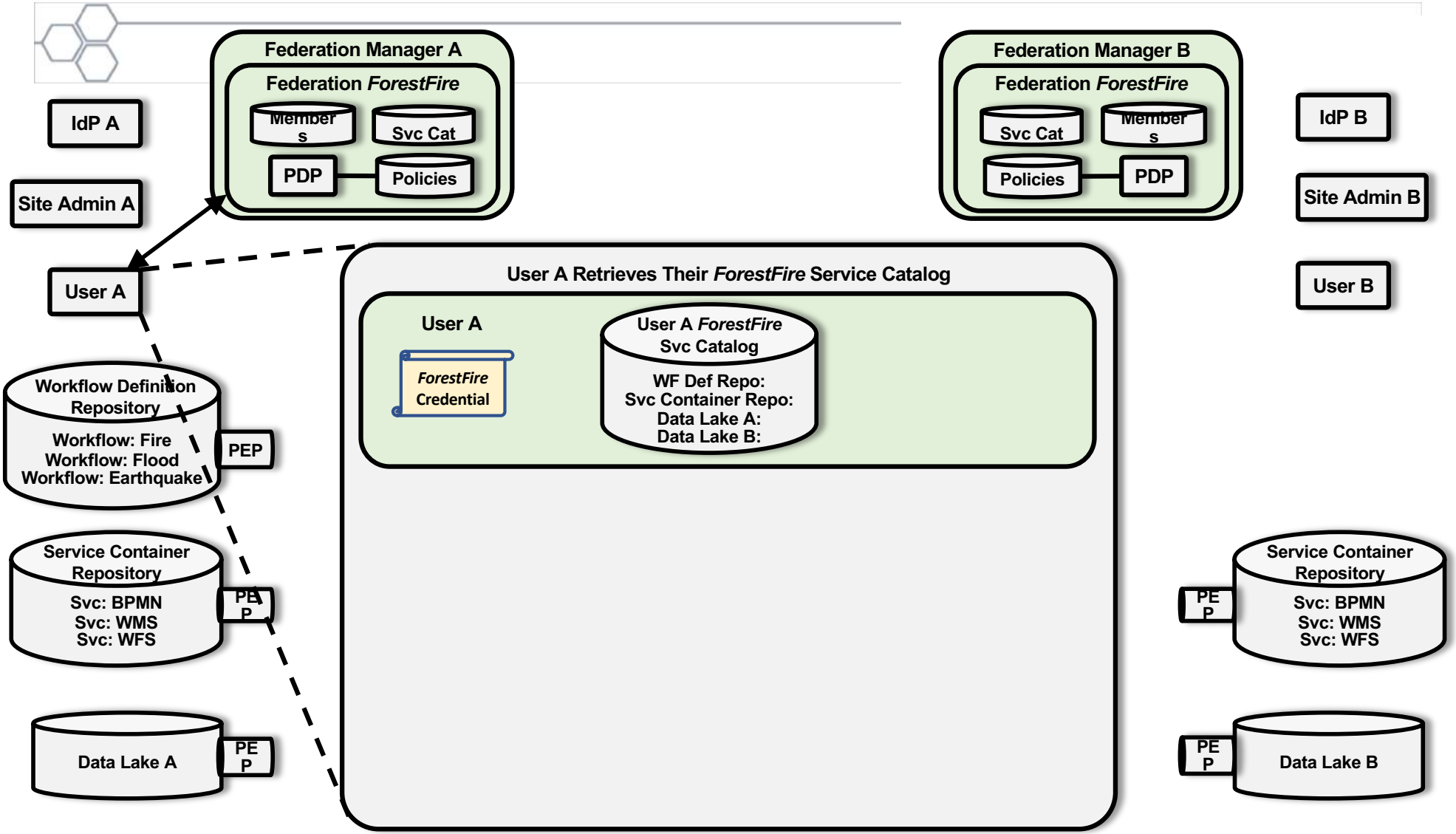
OGC®

User A Authenticates to *ForestFire*



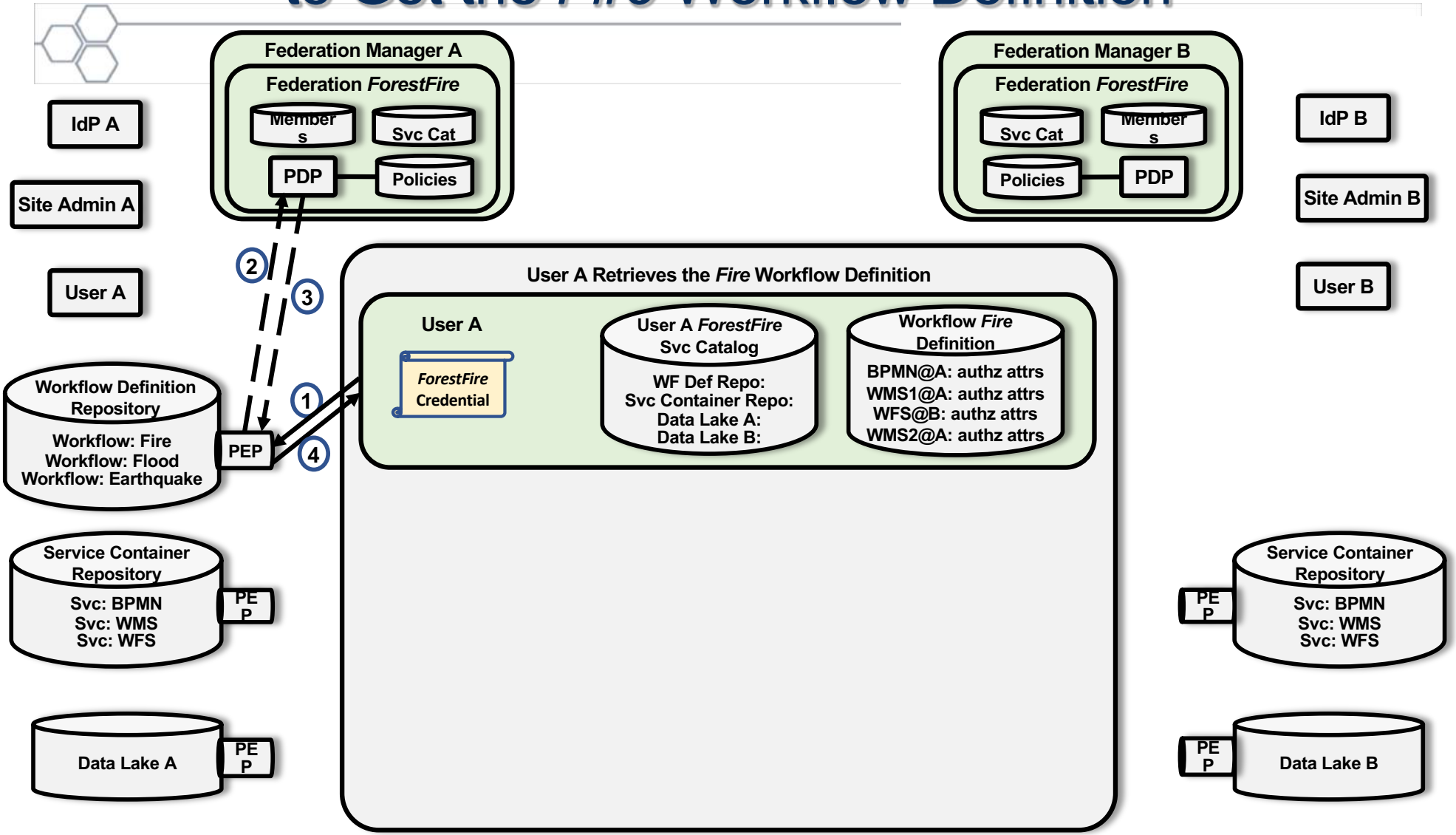
OGC®

User A Retrieves their Service Catalog



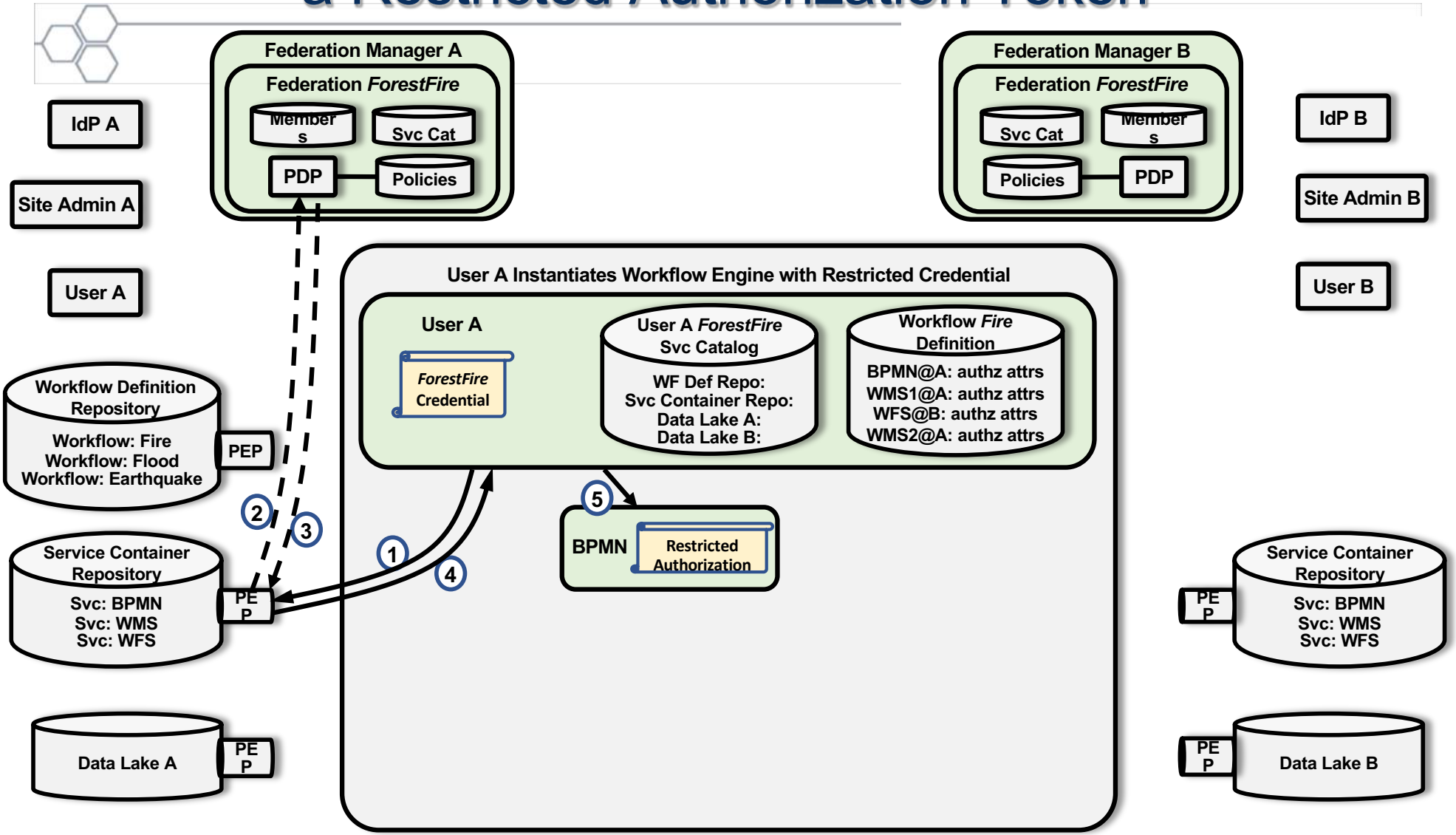
OGC®

User A Uses Their *ForestFire* Credential to Get the *Fire* Workflow Definition



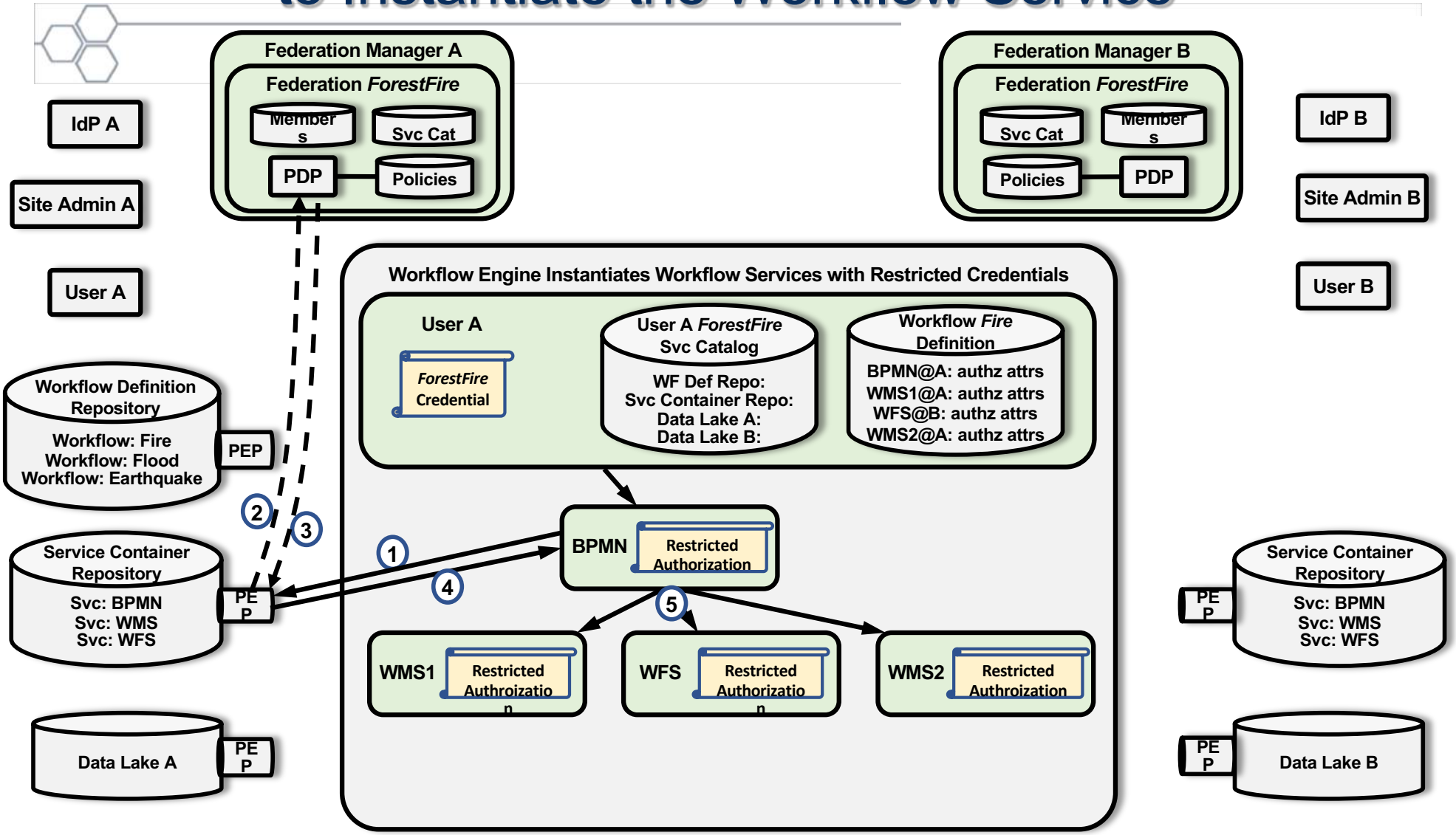
OGC®

User A Spins-up a BPMN Container with a Restricted Authorization Token



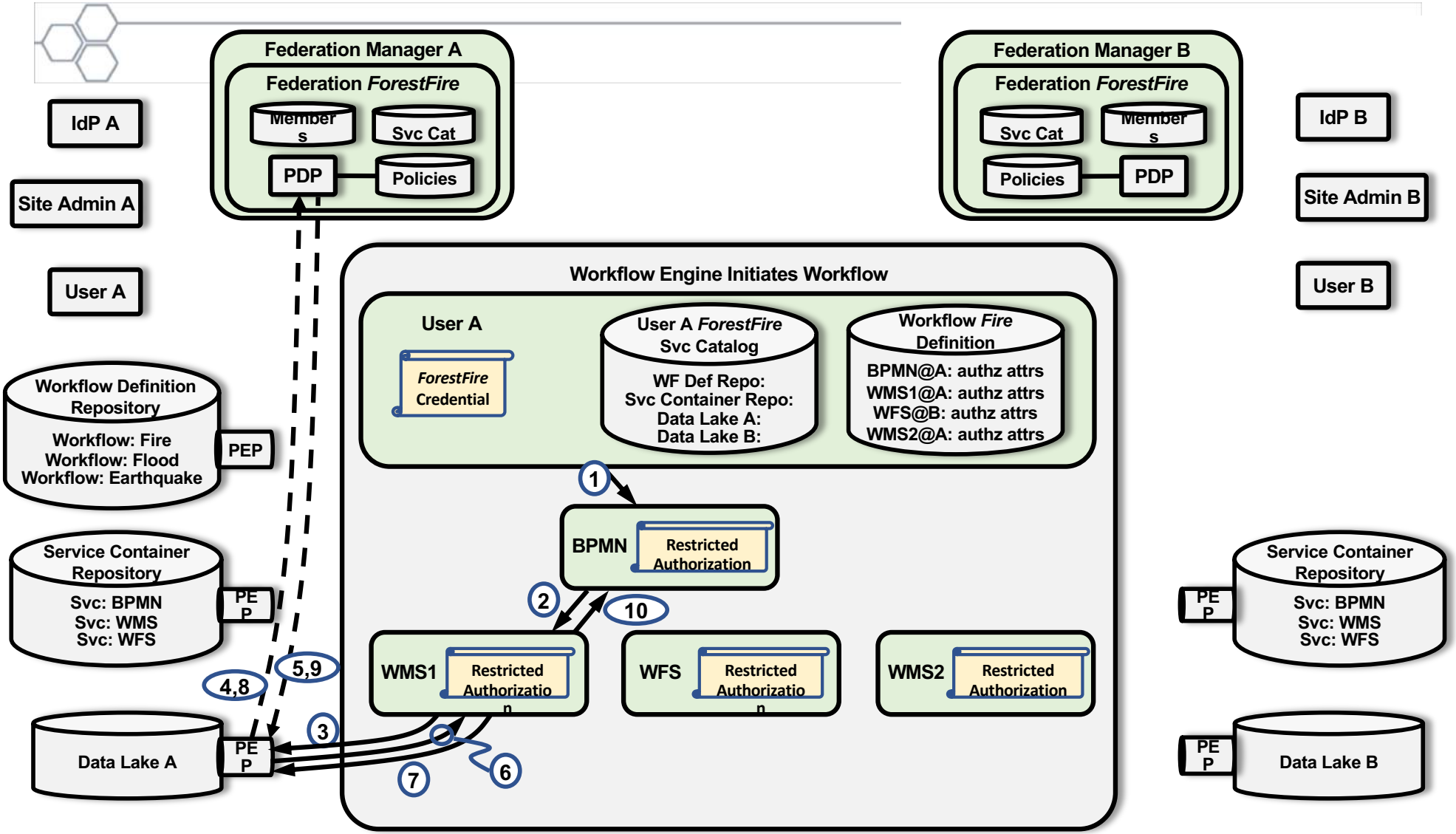
OGC®

The BPMN Accesses the Service Container Repo to Instantiate the Workflow Service



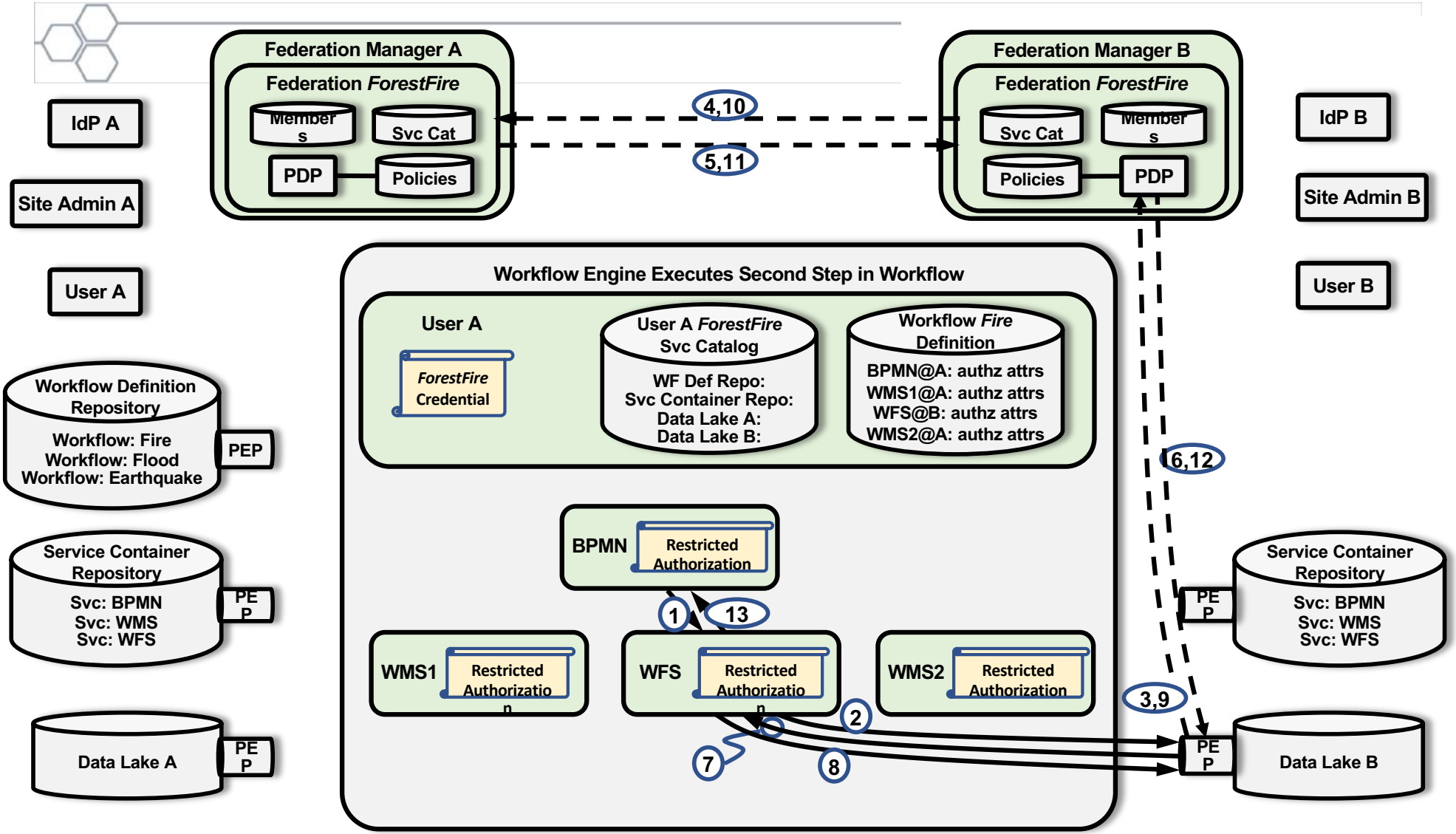
OGC®

The First Workflow Step Accesses Data Lake A



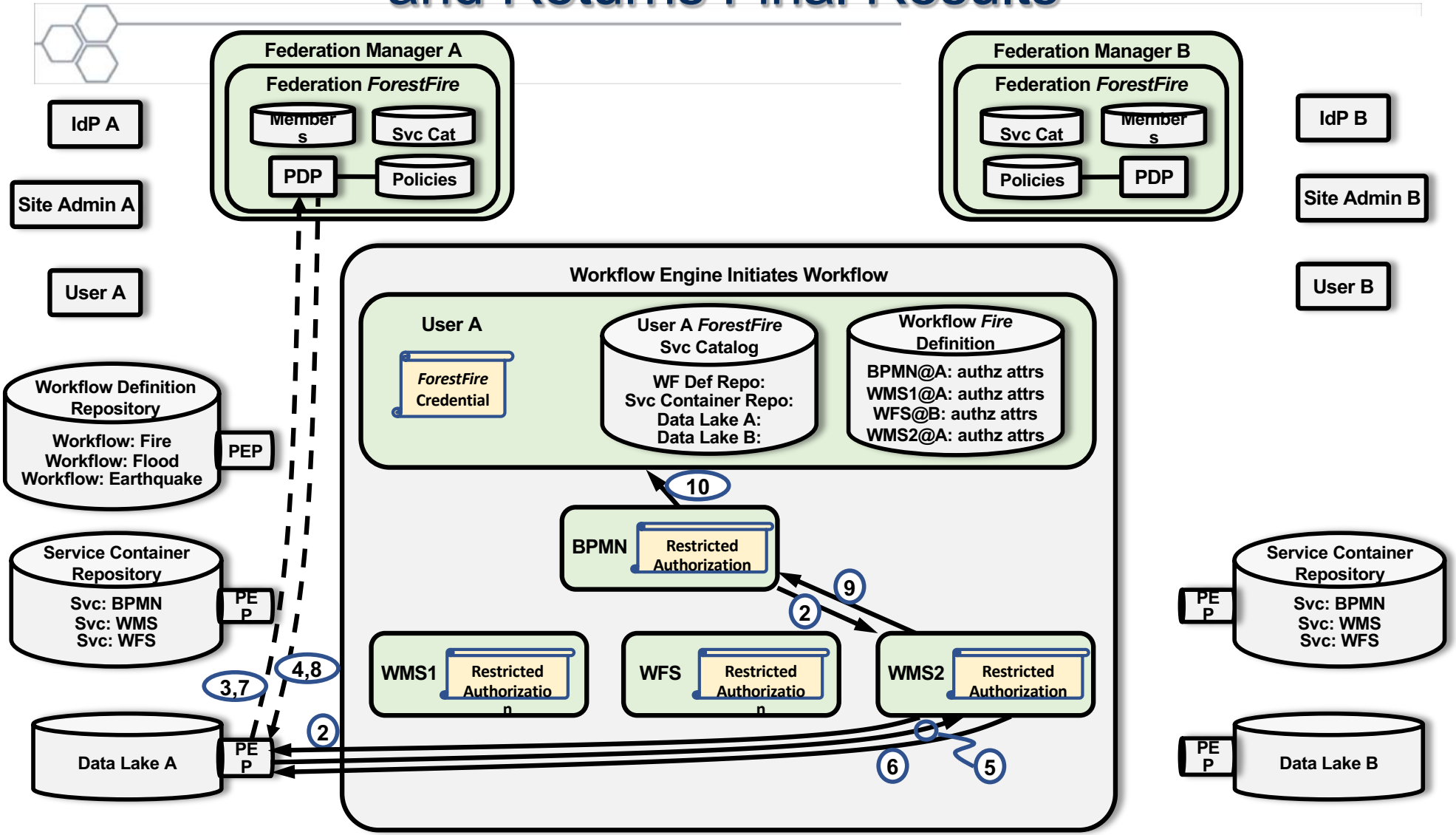
OGC®

The Second Workflow Step Accesses Data Lake B



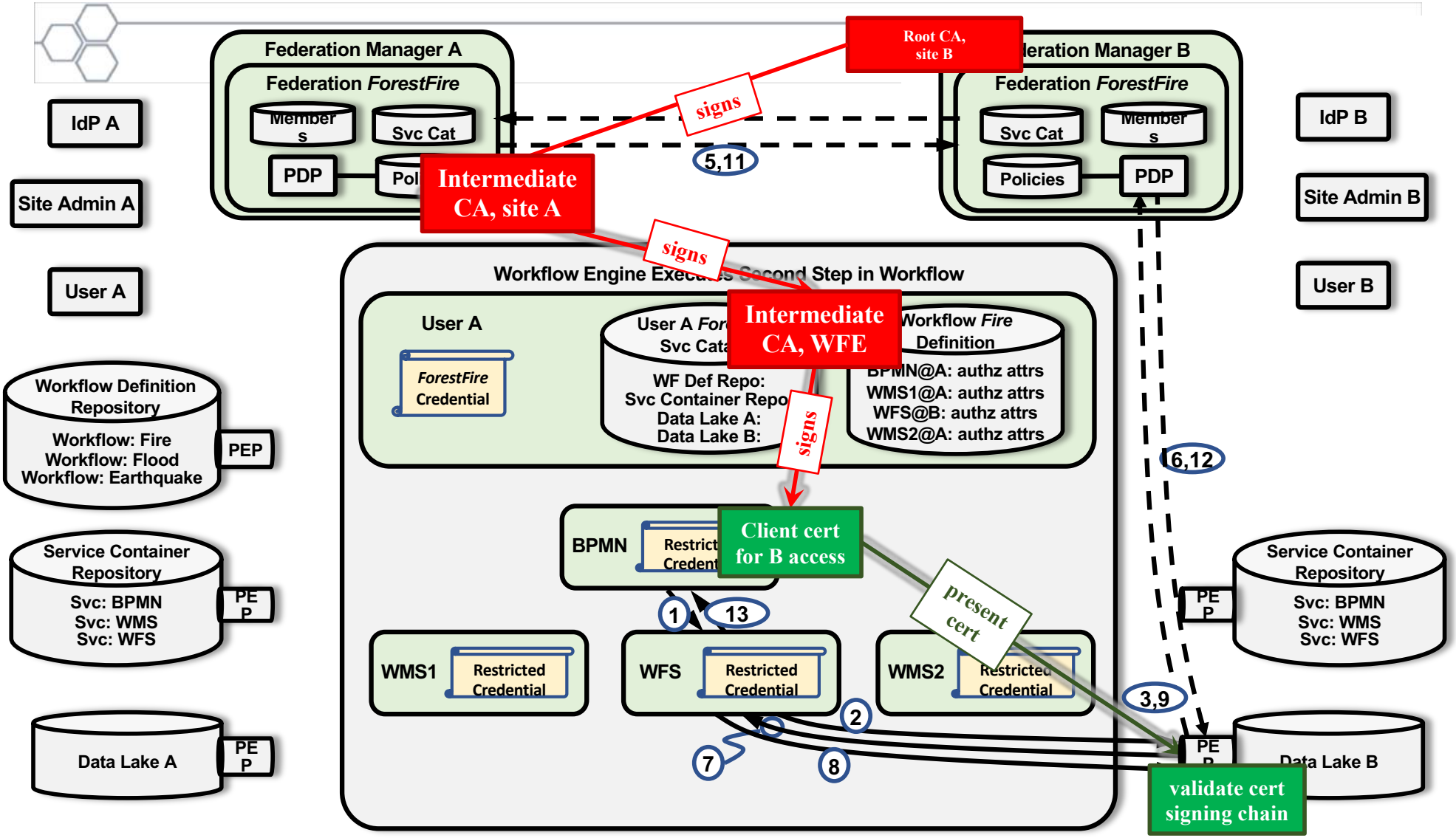
OGC®

The Last Step Accesses Data Lake A and Returns Final Results



OGC®

DRAFT Modifications Using PKI



(From Victor Danilchenko, Schneider Electrics)

OGC®

What Are the Next Steps?

- What can different stakeholders do that builds on their current investments?
- What incremental steps can be taken that moves current systems/tools in the direction of interoperable standards?
- Some suggestions:
  - Integration of existing identity federation mechanisms
  - Investigating the use of existing standards and tools, such as OpenID, OAuth and Web Service API Gateways
  - A method for defining federations
  - User-to-FM communication APIs and protocols
  - FM-to-FM communication APIs and protocols
  - Raising awareness using FM-based trust federations

OGC®

Thank You

Questions?