The Path to Cloud Federation via Standards

Dr. Robert Bohn, *CTL/NIST*
Dr. Craig A. Lee, *Federation Partners*
Dr. Martial Michel, *Data Machines*

April 6, 2022
MAGIC/NITRD

NIST Cloud Computing Program

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

In the Beginning

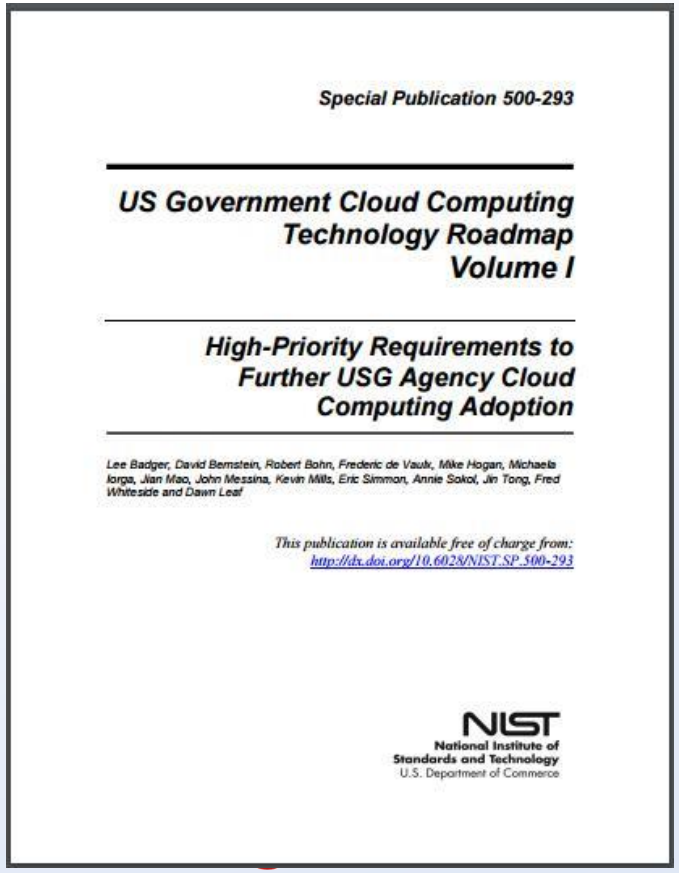
- Cost & Efficiency drivers - US IT Budget ~ $80B/year:
- Federal Cloud Computing Strategy (*Cloud First – Feb 2011*)
- NIST's Goal – To accelerate the federal government's adoption of cloud computing
  - *Build a USG Cloud Computing Technology Roadmap*
  - *Lead efforts to develop standards and guidelines*
- Starting Material – *NIST Definition of Cloud Computing (SP 800-145)*
- Develop a Reference Architecture for Cloud Computing
  - *Determine the "What" of Cloud Computing, not the "How"*

NIST Cloud Computing Program

A USG Cloud Computing Technology Roadmap

Public Working Groups

Reference Architecture | Standards | Security | Technical Use Cases | Business Use Cases



Special Publication 500-293

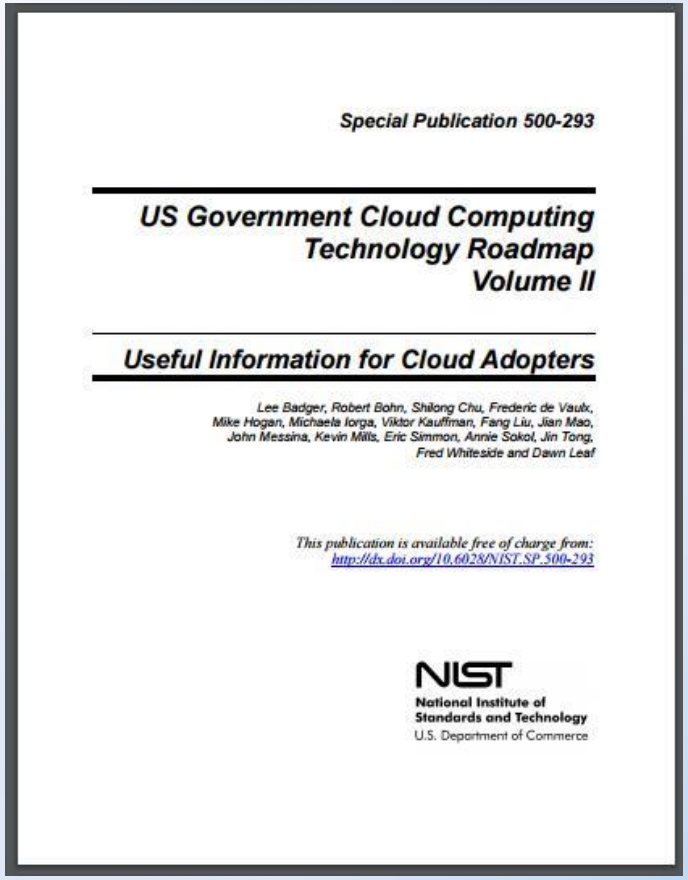
US Government Cloud Computing Technology Roadmap Volume I

High-Priority Requirements to Further USG Agency Cloud Computing Adoption

Lee Badger, David Bernstein, Robert Bohn, Frederic de Vaulx, Mike Hogan, Michaela Iorga, Jian Mao, John Messina, Kevin Mills, Eric Simmon, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.500-293

NIST National Institute of Standards and Technology U.S. Department of Commerce



Special Publication 500-293

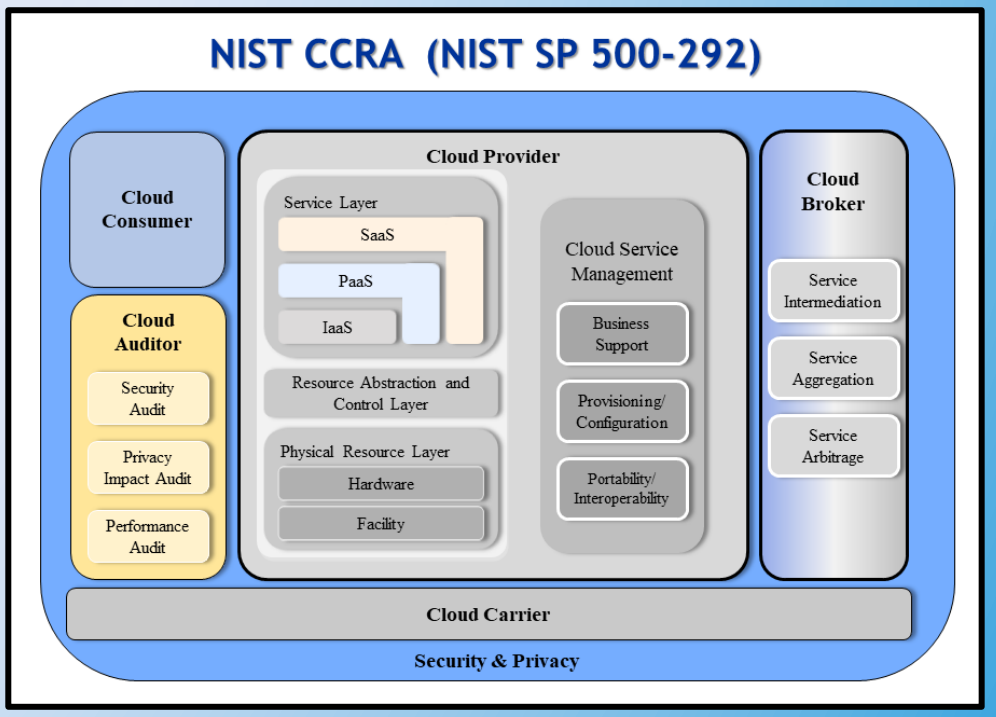
US Government Cloud Computing Technology Roadmap Volume II

Useful Information for Cloud Adopters

Lee Badger, Robert Bohn, Shilong Chu, Frederic de Vaulx, Mike Hogan, Michaela Iorga, Viktor Kauffman, Fang Liu, Jian Mao, John Messina, Kevin Mills, Eric Simmon, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.500-293

NIST National Institute of Standards and Technology U.S. Department of Commerce



5 Actors – Consumer, Provider, Broker Auditor, Carrier

USG Cloud Computing Technology Roadmap Requirements (NIST SP 500-293)

1. International voluntary consensus-based standards
2. Solutions for High-priority Security Requirements, technically de-coupled from organizational policy decisions
3. Technical specifications to enable development of consistent, high-quality Service-Level Agreements
4. Clearly and consistently categorized cloud services
5. **Frameworks to support seamless implementation of federated community cloud environments**
6. Updated Organization Policy that reflects the Cloud Computing Business and Technology model
7. Defined unique government regulatory requirements and solutions
8. Collaborative parallel strategic “future cloud” development initiatives
9. Defined and implemented reliability design goals
10. Defined and implemented cloud service metrics

NIST Cloud Computing Program

NIST/IEEE Collaboration

- NIST recognized the importance of “Frameworks to support seamless implementation of federated community cloud environments” in USG Cloud Computing Roadmap (NIST SP 500-293).
- Collaboration between NIST and IEEE P2302 will help build consensus on creating an Intercloud - an open, transparent infrastructure amongst cloud providers to support evolving technological and business models and the growing demand for standards that address Intercloud interoperability.

NIST Cloud Computing Program

IEEE SIIF Objectives

- **Purpose:** *This standard creates an economy amongst cloud providers that is transparent to users and applications, which provides for a dynamic infrastructure that can support evolving business models.*
- **Scope:** *To define topology, functions, and governance for cloud-to-cloud interoperability and federation.*

- **Support Transparent Infrastructure**
  - Like the Internet
  - Like the Phone Network
- **Cloud Implementation Independent**
  - Like the Internet Router
  - Like the Phone Network CO Switch
  - Based on Standards
- **Simple Protocol Set, Easy to Join**
  - Like an ISP, simple IP based protocols enough to get started
  - Supports Regional Governance
- **Support for Generalized Resource Federation**
  - Not Just VM's – IaaS, PaaS, *aaS
  - Extensibility to Any Describable Resource Type
  - Communities can Add Resource Types
- **Support for Multiple (Open or Proprietary) Federation Topologies**
  - Network Abstraction
- **Global Scale Capable**

NIST Cloud Computing Program

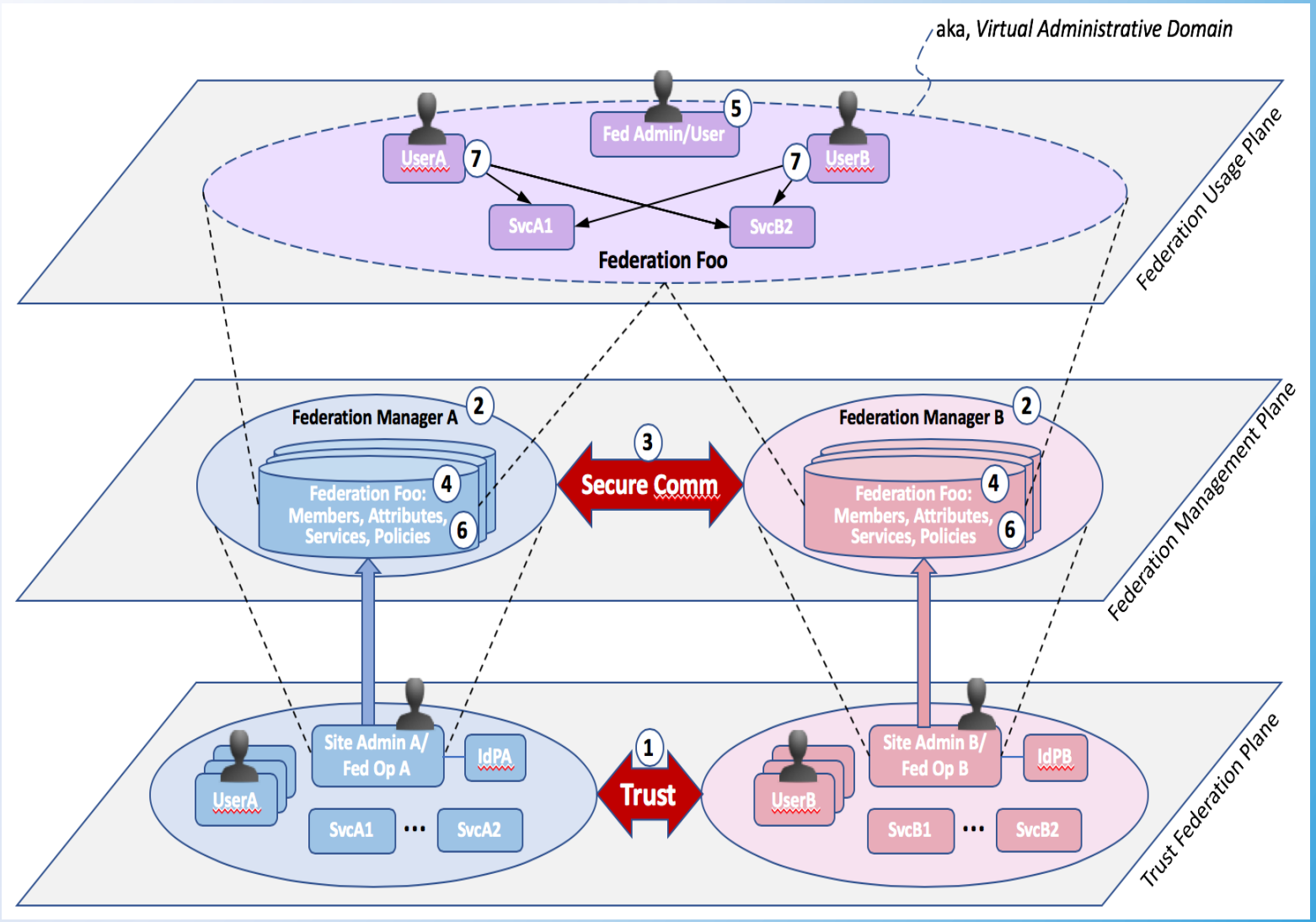
NIST PWGFC/IEEE P2302 Goals & Outputs

- The NIST PWGFC will develop a **cloud federation vocabulary and conceptual model** based on the Scope and Purpose.
  - The PWGFC interim outputs will be contributed to the IEEE P2302 Working Group in real-time.
  - The PWGFC output will be a NIST Special Publication.
- The IEEE P2302 Intercloud Working Group will develop a **cloud federation standard** based on the Scope and Purpose.
  - The PWGFC interim contributions will serve as input.
  - Feedback on PWGFC vocabulary and conceptual architecture contributions will be provided to the PWGFC in real-time.
  - The P2302 initial output will be an IEEE Standard.
  - Plan to contribute the P2302 Standard to ISO/JTC1 to create an International Standard.

NIST Cloud Computing Program

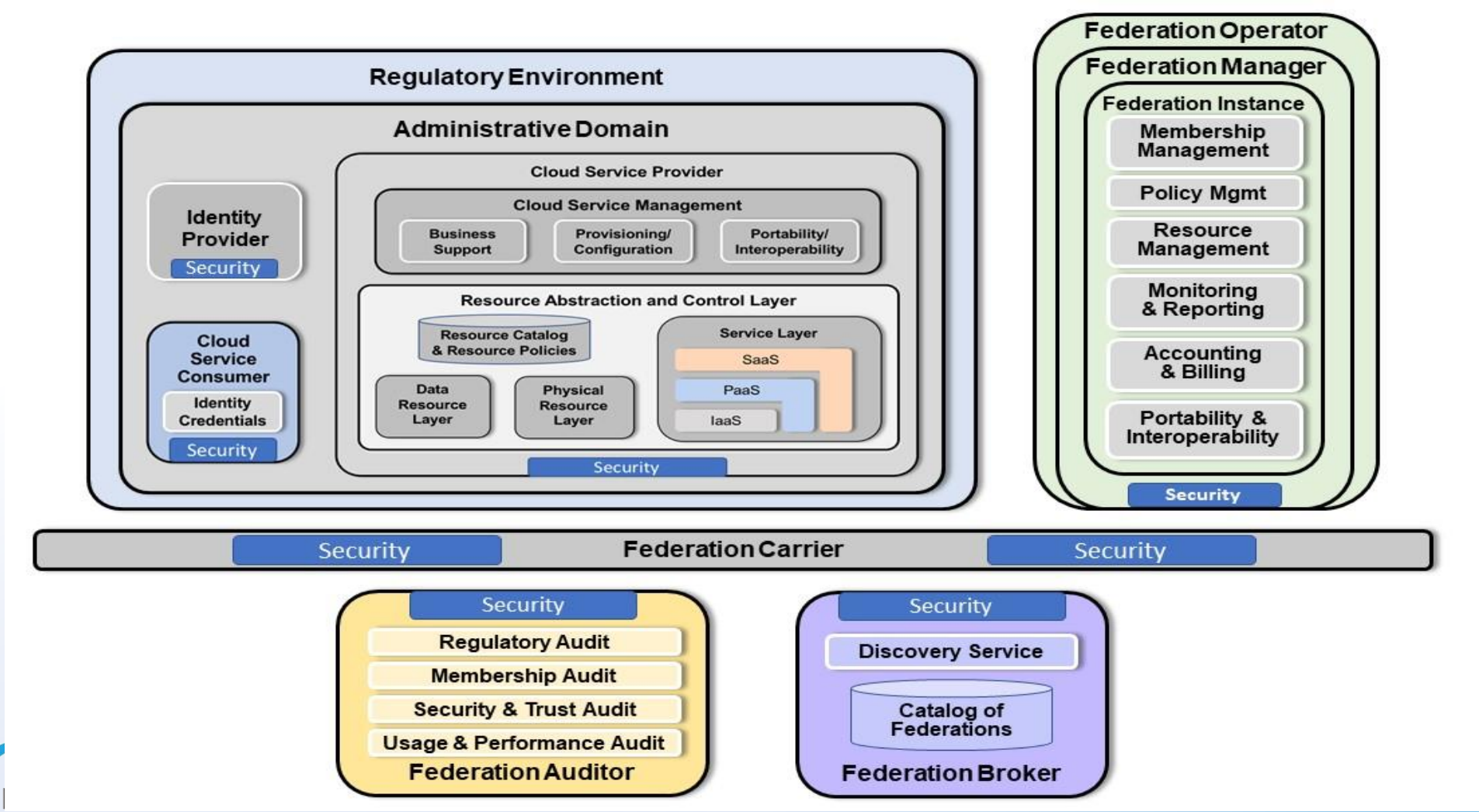
NIST Cloud Federation Reference Architecture

1) Sites decide to collaborate and establish trust
2) *Federation Managers (FMs)* are deployed
3) FMs configured to communicate based on trust relationship
4) *FedAdmin(s)* create one or more federation instances
5) A federation is a *Virtual Administrative Domain*
6) *Resource Owner* register services for a specific federation
7) Federation members can invoke federation services



NIST Cloud Computing Program

NIST Cloud Federation Reference Architecture
NIST SP 500-332



Computing Program

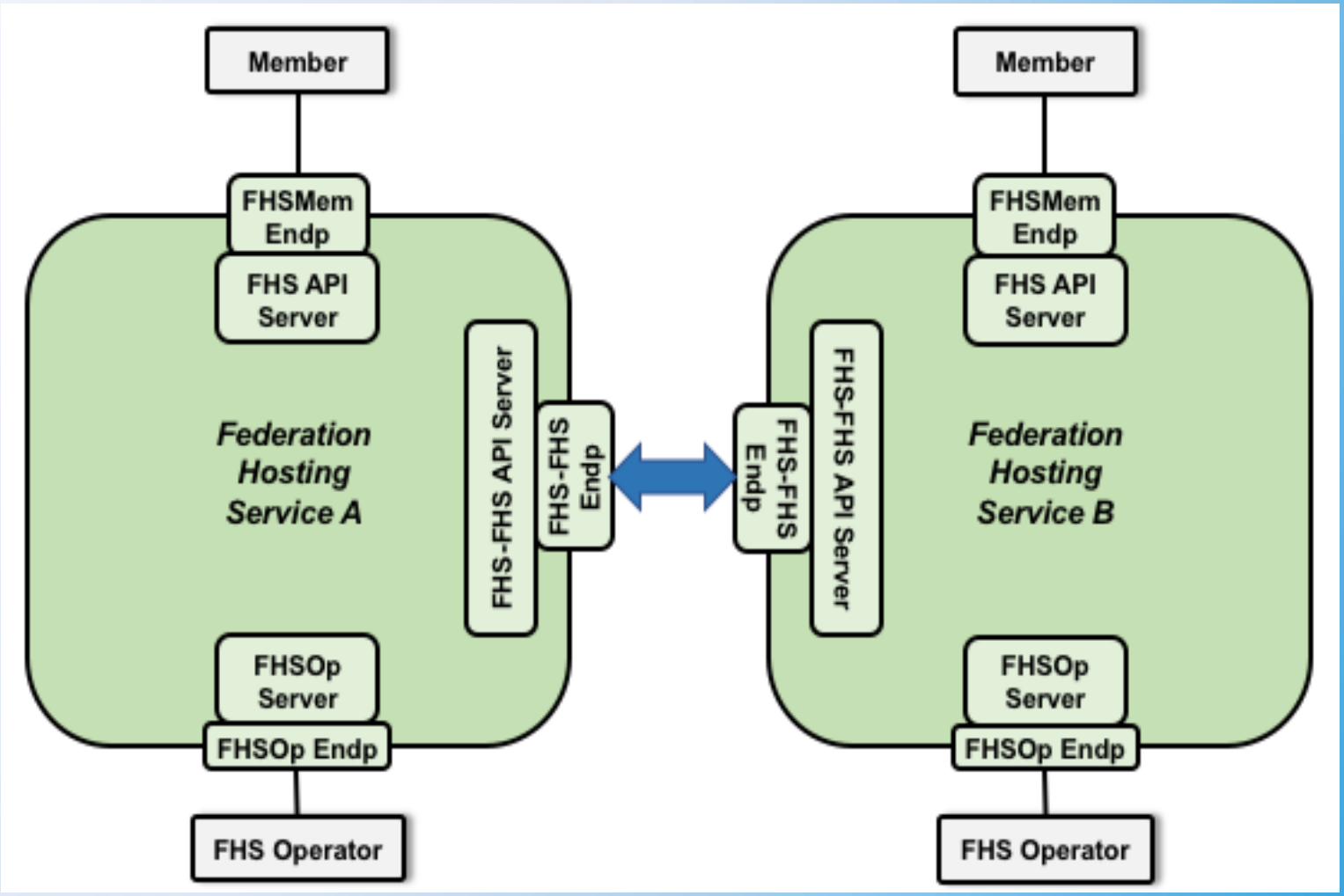
https://doi.org/10.6028/NIST.SP.500-332

IEEE 2302-2021 is a Collaborative NIST / IEEE Effort

- IEEE 2302-2021 formalizes the CFRA model as a *Federation Hosting Service (FHS)*
  - Codifies an Architectural Approach and API for *Federation Instances*
- A federation instance has:
  - Members, including *Service Owners* and at least one *Fed Admin*
  - Federation-specific roles and attributes
  - Federation members can discover and use *registered services* regardless of location
- Fed instances are hosted on one or more FHSs
  - A set of FHSs constitute a *distributed API Gateway*
  - As with ordinary API Gateways, an FHS can "back-end" an external IdP
  - IEEE 2302 does not mandate a specific type of Identity Provider or identity credential
- A set of FHSs are the “railroad” on which many federation instances can run
  - FHSs operators establish trust and secure communication among themselves
  - Federation members establish trust among themselves

The IEEE 2302-2021 Federation Hosting Service (FHS) Model

- Three APIs in OpenAPI 3.0:
  - FHSOp API
  - FHSMember API
  - FHS-FHS API, and
- Four *Federation Capability Levels*
  - L1: Core
  - L2: Accounting, Billing, Auditing
  - L3: Legal/Compliance Agreements
  - L4: Automation
- IEEE 2302-2021 defines L1 Core API
- There are three pre-defined roles:
  - FedAdmin
  - ServiceOwner
  - Member
- FHS configurable to use various IdPs
  - OIDC, PKI, Verifiable Credentials, etc.



The FHS model is essentially a set of communicating API Gateways

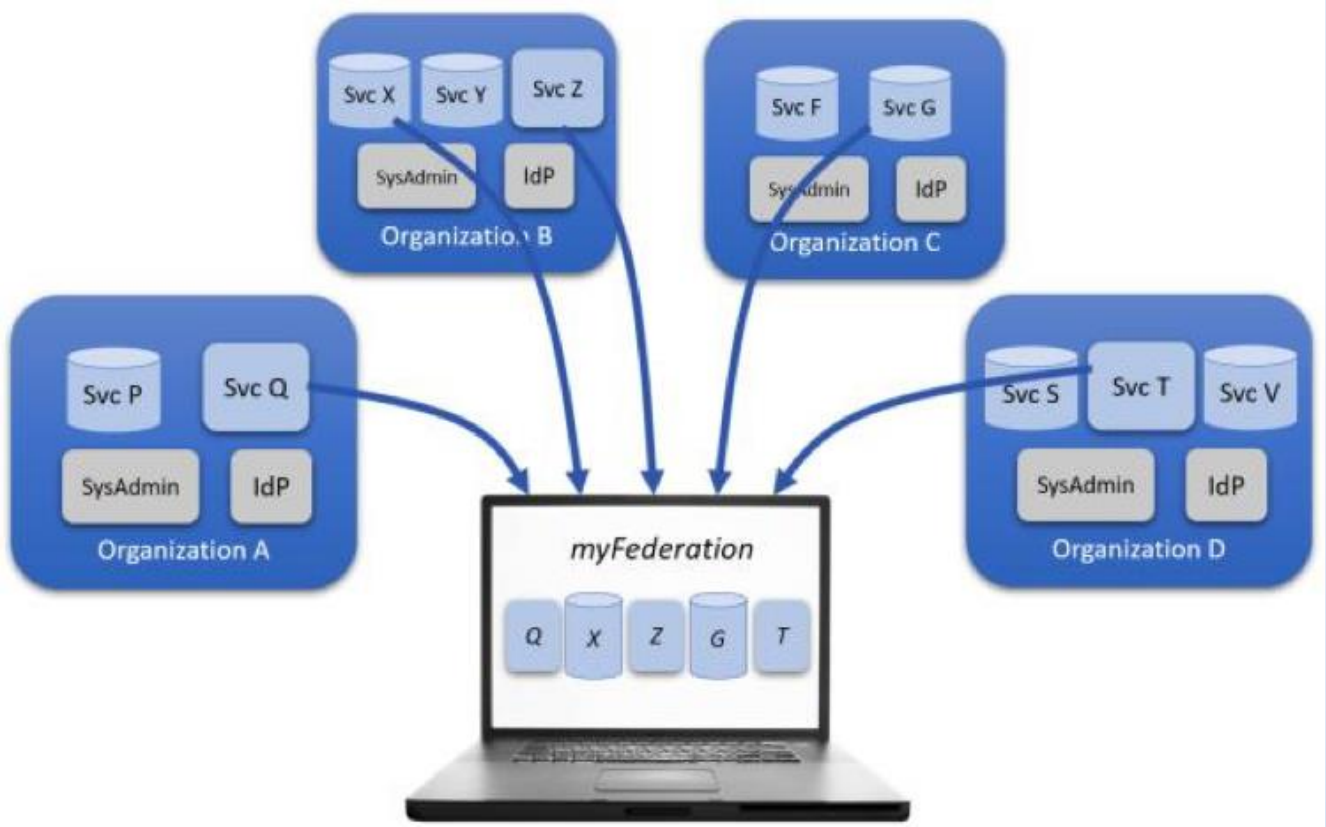
NIST Cloud Computing Program

Range of Deployment and Governance Configurations

- Centralized (and by definition, Homogeneous)
  - Single FHS operated by a trusted operator
- Decentralized and Homogeneous
  - Set of communicating FHSs with the same type of IdP
  - FHSs could be operated by different organizations
- Decentralized and Heterogeneous
  - Set of communicating FHSs with different IdPs
  - Differences in credential formats could be address using token translation
    - Similar to universal token translation approach of the *Authentication and Authorisation for Research Collaborations (AARC) project*
  - To reiterate: attribute semantics and release are not issues since attributes are federation-specific

NIST Cloud Computing Program

The User's Perspective



- After authentication, a federation member has a consistent view and ability to interact with federated resources
- Member can use services and access data based on their authorizations, regardless of who owns the resource
- Resource owners retain unilateral control over the discovery and access policies of their resources
- Different user-friendly front-end interfaces possible. For example:
  - Web portals
  - Virtual desktops
  - Jupyter notebooks

Building Out the Capability Levels

- Accounting & Billing
  - Resource usage cost structure applied to monitored usage data
- Regulatory Compliance
  - Federation credentials have sufficient identity and authorization information to properly enforce well-defined policies
- Trust Domain Management
  - Simple federations can manually manage trust “out-of-band”
  - *OIDC Federation Specification* could be used to establish trusted communication between (OIDC-based) FHSs that have a *common trust anchor*
  - *Trustmark Frameworks* could be used where users build a *Trustmark Interop Profile*
- Automation
  - Commercial federation providers could operate fleets of on-demand FHSs
  - Operation similar to current cloud-based Content Distribution Networks

NIST Cloud Computing Program

Comparison with Existing Approaches and Systems

- IEEE 2302-2021 architectural approach is similar to:
  - Dataverse (similar proxy approach)
  - OpenStack Keystone service ("Federate In, Federate Out")
  - DARPA Security Enclaves (research work published in 2000)
- InCommon, in contrast, provides a single, monolithic, trust environment
  - Defined by the *metadata* file of trusted IdPs and SPs
  - Has created a "trust ecosystem" wherein additional services have been developed to provide enhanced capabilities and flexibility, e.g., CILogon, Grouper, COmanage
- Open Science Pool: OSG Data Federation and OSG Compute Federation
  - Access Points (APoints) provide workflow management, including input/output data staging
  - Execution Points (XPoints) enable sites to contribute server capacity to an OSPool
- NIH Cloud Interoperability approaches
  - "Find data", "Authorization to use data", "Set up place to do analysis"
  - GA4GH *Passports* and *Data Repository Services*
  - *Researcher Auth Service (RAS)* utilizes OAuth/OIDC
- REFEDS Federation 2.0 WG chartered to make recommendations for future academic interfederations
  - "Drive innovative technical architectures, standards and policies"
  - *Evolve* academic interfederations by leveraging technologies and standards from across the federation landscape

NIST Cloud Computing Program

Summary

- The need for collaboration that is inherently distributed is fundamental
  - Application domains exist across academia, industry and government
  - Widely adopted common practices and standardized tooling are needed
- The 2302-2021 model and API is a "Ford Model T" with lots of development needed.
- Supports range of deployment and governance
  - Small-scale deployments
    - Individual projects and organizations can own and operate their own FHSs
  - Large-scale, commercial, deployments
    - Commercial federation providers could operate a fleet of FHSs across their data centers to provide on-demand federations with a potentially global footprint
    - Similar to provisioning of Content Distribution Networks
- Provides a possible evolutionary path for current federation environments
  - Architectural approach provides flexibility that *ad hoc* federation approaches can't
- Economic market development is the future challenge

NIST Cloud Computing Program

Additional Material

Additional Compatible Data Security Mechanisms

- Open Geospatial Consortium (OGC) Data-Centric Security
  - Only encrypted data is circulated
  - Recipients must retrieve decryption keys from *Key Management Server*
- Trusted Data Format
  - Policy Enforcement Point (PEP) is “packaged with” the data
  - PEP knows how to contact remote Policy Decision Point to get access decision
- Attribute-Based Encryption
  - Access policy is encrypted with the data
  - Recipients must have proper attributes (not just keys) to access data
- Remote Access to Trusted Execution Environments (TEEs)
  - Remote data is encrypted until loaded into hardware-protected TEE memory
  - *Federated Analytics* use case identified by the Confidential Computing Consortium

NIST Cloud Computing Program

Federation Hosting Service Operator (FHSOperator) API

1. FHSOPERATOR CORE

```
1.1 POST /FHSOperator/NewFedAdmin
1.2 GET /FHSOperator/FedAdmins
1.3 PUT /FHSOperator/FedAdmin/{member_id}
1.4 DELETE /FHSOperator/FedAdmin/{member_id}
1.5 GET /FHSOperator/FedInstances
1.6 PUT /FHSOperator/FedInstance/{fed_id}
1.7 DELETE /FHSOperator/FedInstance/{fed_id}
```

2. FHSOPERATOR FHS-FHS

```
2.1 POST /FHSOperator/AllowConnection
2.2 POST /FHSOperator/Connect
2.3 GET /FHSOperator/Connections
2.4 DELETE /FHSOperator/Connection/{conn_id}
```

FHSOp API

Grants membership to FedAdmins

- Special users with federation admin privileges

Initiates establishment of secure communication with other FHSs

IEEE P2302 Program

Member - Federation Hosting Service (MemFHS) API

1. ATTRIBUTES

1.1 GET /Attribute/{fed_id}
1.2 POST /Attribute/{fed_id}
1.3 DELETE /Attribute/{fed_id}/{attr_id}

2. AUTHORIZATION

2.1 PUT /Authorization/{fed_id}/{member_id}/{attr_id}
2.2 DELETE /Authorization/{fed_id}/{member_id}/{attr_id}

3. DISCOVERY

3.1 POST /Discovery/{fed_id}/{member_id}

4. FEDERATION

4.1 POST /Federation
4.2 GET /Federation/{member_id}
4.3 GET /Federation/{member_id}/{fed_id}
4.4 DELETE /Federation/{member_id}/{fed_id}

5. FEDERATION FHS-FHS

5.1 GET /Federation/Query
5.2 POST /Federation/Join/{fed_id}
5.3 GET /Federation/JoinRequests
5.4 POST /Federation/JoinGrant/{request_id}
5.5 POST /Federation/JoinDeny/{request_id}
5.6 DELETE /Federation/Leave/{fed_id}

6. FEDERATION MONITORING

6.1 GET /MonitoringParams/{fed_id}
6.2 PUT /MonitoringParams/{fed_id}
6.3 PUT /MonitoringProxy/{fed_id}

7. LOG IN/OUT

7.1 POST /MemberLogin
7.2 DELETE /MemberLogout/{login_session_id}

8. MEMBERSHIP

8.1 GET /Membership/{fed_id}
8.2 POST /Membership/{fed_id}
8.3 GET /Membership/{fed_id}/{member_id}
8.4 DELETE /Membership/{fed_id}/{member_id}

9. SERVICES

9.1 POST /Services/{fed_id}
9.2 GET /Services/{fed_id}/{svc_owner_id}
9.3 GET /Services/{fed_id}/{svc_owner_id}/{svc_id}
9.4 PUT /Services/{fed_id}/{svc_owner_id}/{svc_id}
9.5 DELETE /Services/{fed_id}/{svc_owner_id}/{svc_id}

FHSMember API

- Members log in/out of specific federations
- FedAdmins can:
  - Create federation instances
  - Grant/revoke federation membership
  - Define federation roles
  - Grant/revoke roles
  - Join existing federations
  - Manage per federation monitoring and “back-end” monitoring systems
- ServiceOwners can:
  - Register services
  - Define discovery and access policies
- Members can:
  - Discover and invoke services

Program

Federation Hosting Service - FHS API

1. CONNECTION

1.1 POST /Connect

1.2 DELETE /Connect/{connection_id}

2. FEDERATION

2.1 POST /JoinFederation

2.2 PUT /UpdateFederation

2.3 POST /ValidateMember

2.4 DELETE /LeaveFederation/{fed_id}

3. FEDERATION MONITORING

3.1 POST /MonitoringData/{fed_id}

FHS-FHS API

Establishes secure communication with other FHSs

Exchanges information on specific federation instances

Exchanges monitoring data when collocation desired

IEEE P2302 Program

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov