# Private Cloud Identity Service: Conceptual Architecture

Prepared for Ohio | OARnet

**Dave Muehling**
Director
Security and Risk Practice
Gartner Consulting
Dave.Muehling@gartner.com

**GARTNER CONSULTING**
Engagement: 330011012 Version #1



Gartner

# Agenda


- Introductions
- Background and Objectives
- Federated Identity Model
- Private Cloud Identity Service Model
- Summary and Next Steps
- Q&A

# Background

- Background
  - In response to inquiries from member institution CIO's, OARnet is moving toward a goal of operationalizing Trusted Identity for its member institutions.
  - Under this initiative, OARnet has created a state-wide federated Identity program, "IAM Ohio", intended to develop strategy, partners, and capabilities necessary to insure success in federating identity within Ohio, across the US, and internationally, among public and private partners. Initiative is guided by a CIO Steering Committee.
  - IAM Ohio Steering Committee met in May and set the following goals
    - Business drivers identified by Steering Committee
      - Integrating Research at State and Federal level
      - Enabling Shared Services like OhioLINK, EduRoam, and the SSID
      - Improving Provisioning for automation and efficiency
      - Enhancing the Classroom and Online Teaching
    - Action plan recommended at May steering committee meeting
      - Compile current IDM practices information at member schools
      - Partner with campus IDM champions from outside IT
      - Design reference architecture for federation, including service catalog, federation scheme, and IDM architecture
    - Gartner was identified as a partner that could help with the portions of the Action Plan detailed above.

# Objectives

- Objectives of Today's Presentation
  - Review the standard federation model and discuss the pros and cons
  - Introduce the private cloud identity service model and discuss the pros and cons
  - Review the planned next phase for designing and implementation of the model
  - All participants gain a solid understanding of Gartner's recommended approach to identity services for Ohio

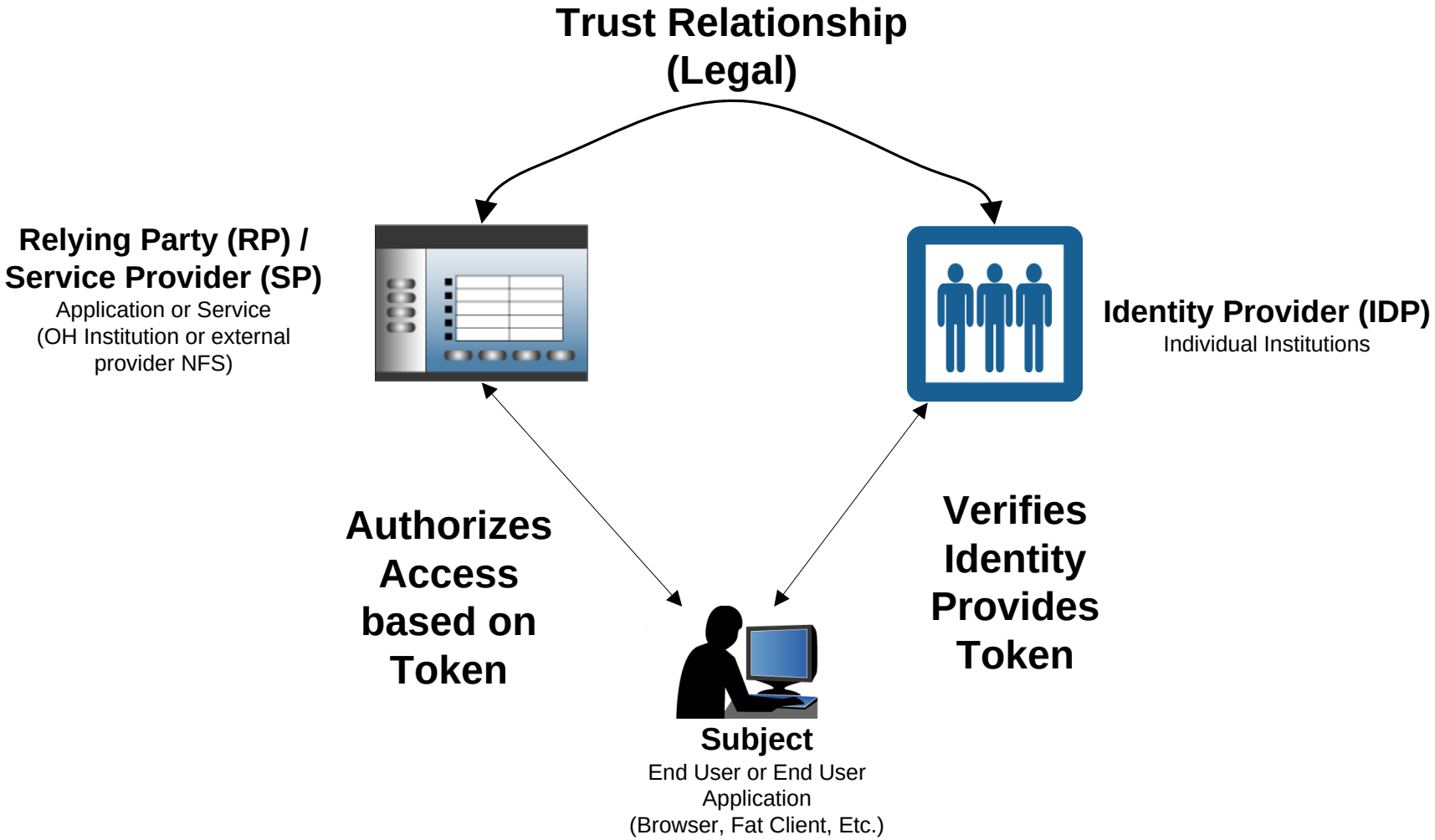
# Federated Identity Model

What is the Standard Federated Identity Model, in Context

Benefits of the Standard Model

Risks from Using Standard Model in Ohio's Context

# Standard Federated Identity Model



# Risks from Using Standard Model in Ohio's Context

- Provisioning and De-Provisioning of Attributes
  - Works great for simple web apps like an information site where information is read-only with no interaction
  - Becomes less clean when some information is needed to provide the user individualized content or allows for data interaction (e.g., portal, forums, interactive applications, etc.)
    - Federation is an Authenticator of the identity and relies on a simple trust model
    - Some organizations are overloading the SAML token with attributes to provide poor-mans provisioning
      - Results in out-of-date or orphaned identity information at the service provider, which requires cleaning to "de-provision" stale accounts
    - SAML was not meant to provide authorization style attributes, Service Provisioning Markup Language (SPML) is the mechanism for this functionality
- Federation is a Point-to-Point model, there is no required Hub
  - Institutions and organizations connect to each other, not a central authority
  - Example: In-Common provides a shared identity model and trust level but is not required for federation, they are not a middle-man brokering connections
- Trust cannot always be trusted or achieved
  - Each SP/RP must have a trust relationship with each IDP
  - Simple math: 20 institutions providing Identity info (IDP) also acting as service providers (SP) means 400 trust relationships
  - Legal trust is not easy to agree to, which is what In-Common is trying to provide a framework to achieve but…
  - What if a change occurs at a trusted partner over time? Stringent policies and audits must be implemented or trust erodes and eventually cannot be trusted.

# Benefits of the Standard Model

- Flexibility
  - Using a standard Federation model provides a high level of flexibility for each institution
  - Can decide who to trust or not
  - Controls identities they own, no middle-man
- Independence
  - Institutions can use any technology they choose as long as SAML is support
  - Not tied to any group so connections and trust is wholly determined by each institution and service provider
- Since only authentication is required...
  - Institutions do not have to worry about “their” identities proliferating into external service providers (as long as they don’t overload the SAML token with attributes to achieve poor-man’s provisioning)
  - Connections and access to a wide number of supporting service providers becomes technically feasible with a low entry cost (trust relationship and configuration)
  - Institutions can provide access to services that require SAML (e.g., NSF)

# Private Cloud Identity Service Model

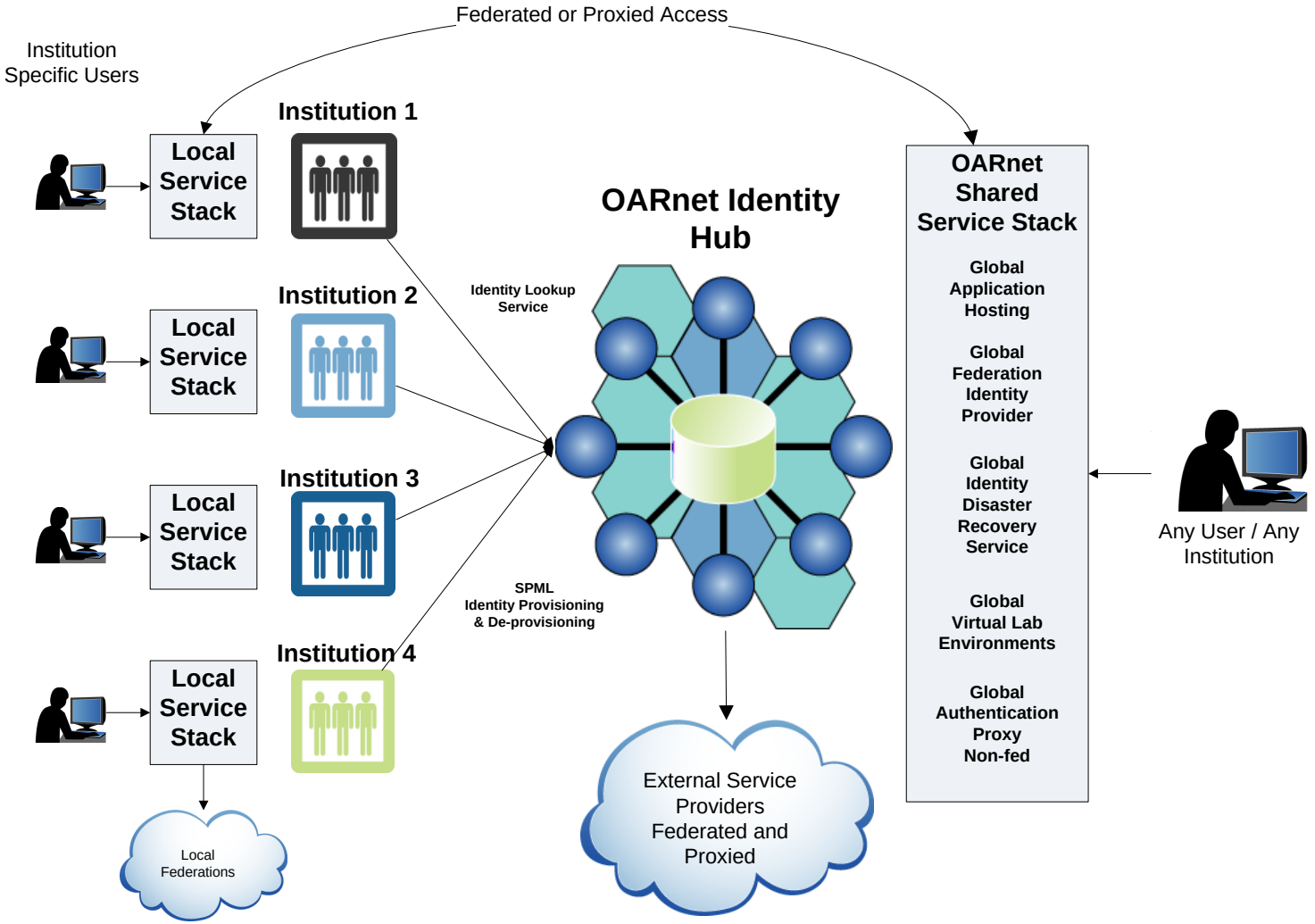
What is the Private Cloud Identity Service Model, in Context

Why Should Ohio use the Private Cloud Identity Service Model

Are Other Organizations using this Model

Risks Associated with the Private Cloud Identity Service Model

# Private Cloud Identity Service Model (Simplified View)



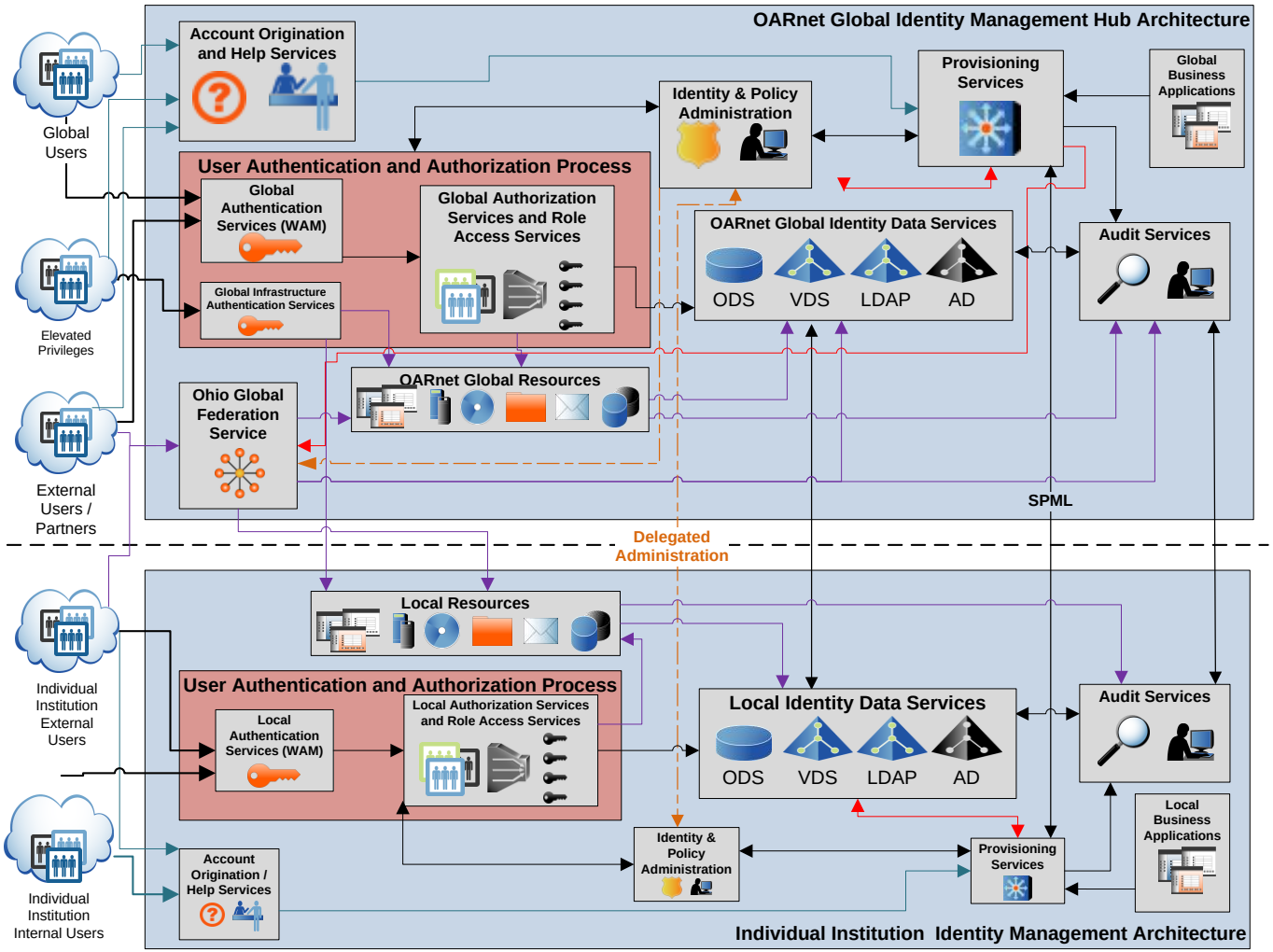
# Private Cloud Identity Service Model (Detailed View)

OARnet provides a global identity management service Hub

Individual institutions run independently and own all local identities and lifecycles

Identities of individual institutions are provisioned and de-provisioned to/from OARnet 's global directory

Only a skeleton of identity information is stored based on a common, state-wide schema



# Why should Ohio use the Private Cloud Identity Service Model

- OARnet would maintain a global record of all participating identities
  - Storage of a sub-set of identity information globally would provide:
    - A replica of identities for participating institutions for disaster recovery purposes
    - Ability for OARnet to provide global federation services including centralized trust relationships
      - OARnet maintains all external trust contracts/relationships for all members
      - OARnet can provide not only authentication tokens but also provide identity attribute info (XACML) based on identity services, including de-provisioning notifications (SPML)
      - Simple math: 20 institutions participating in the global hub, all identities can access all providers, only one trust with OARnet per institution
    - Each member institution could verify any identity through OARnet's identity service
    - Individual identities could be transferred or replicated between member institutions through OARnet and a change of attribute info (student transfers, faculty sharing/transfer, staff sharing/transfer)
    - Global services provided by OARnet can be accessed securely by anyone with a valid identity in a member institution (as long as authorization checks pass of course!)
- Security is enhanced
  - Global patterns of abuse identifiable (student logging into two campuses on opposite sides of the state at the same time)
  - Cross check of identity with owner is an instant reality
  - Guest users can have one global account and do not need to be retained locally
  - Authorization and de-provisioning across institutions are a reality
- Every institution is different
  - By using SPML (a standard provisioning language), institutions can leverage any identity technology that meets their local needs and can participate through the standard
  - Institutions can use any custom schema they want, locally, as long as it supports the OARnet schema definition

## Are Other Organizations using this Model?

- Short answer, **yes**.
- Gartner has provided similar architectures for multiple systems, states, and very large institutions.
- The model has been tested and is in use today.
- The model is in sync with what Gartner sees as trends in education and state government.
- Once in operation, return on investment through speed to connectivity and reduced resources required for audit come quick.
- Model has flexibility to support all major IDM product stacks and open source products that support LDAP, SPML, SAML and XACML, all industry mature standards.

# Risks Associated with the Private Cloud Identity Service Model

- Ability to provision identities either automatically (preferred) or manually (through a provided service) is required.
  - Some smaller institutions may not have this capability
    - In those cases an out-sourced IDM provider may provide the solution, Fischer is currently being POCed
  - Staff may not have the skills to implement local IDM systems
- Maturity is paramount
  - Similar to in-common's trust levels, OARnet members will need to maintain a specified level of maturity to ensure that the system as a whole is not compromised through poor identity management
- If the cloud service goes down, global services will be out of sync (authentication and authorization) with local identity providers until the service can re-sync and update.
- Local institutions may rely on OARnet to provide central trusts for federation services with external service providers, including new federation partner requests, which may cause delay in connectivity due to process.

# Summary

Main Theme Review

What are the Next Steps for Ohio

## Main Theme Review

- Federation is not a silver bullet – it's only one method for authentication.
- De-Provisioning and orphaned identities can cause significant security issues if not given full attention in a federated environment.
- Private Cloud Identity Services provide the highest level of flexibility and independence to the member institutions.
- Security is improved through the use of an identity hub.
- OARnet is currently providing advanced services to Ohio institutions and will be able to expand with the addition of an identity hub model.

- To sum it up: Gartner recommends that Ohio adopt a Private Cloud Identity Service Model.

# What are the Next Steps for Ohio

- Gartner will be developing a second Phase with OARnet that includes the following deliverables:
  - Gartner will create a communication email for the requesting of an identity schema (LDIF or Data model) from up to 20 institutions. These will serve as the sample for the creation of a Private Cloud Identity Service Model based on the EDUPerson LDIF.
  - Gartner will be onsite for one full day to gather information required to complete the project from the OARnet staff. This will be a full eight-hour day of discussions.
  - Gartner will create a standards based, central identity model based on the EDUPerson schema (may contain extensions to that schema to support specific requirement for Ohio, in particular the applications EduRoam and OhioLINK).
  - Gartner will create a mid-level architecture for the central identity hub service (implementation to be at OARnet).
  - Gartner will create a set of initiatives in a timeline format for the implementation of the central identity hub service at OARNet.
  - Gartner will present a final briefing of all deliverables onsite.
- Items not in scope for Phase 2
  - Gartner will not be providing specific vendor or cost information.  Recommended products will be relegated to types of technologies (e.g., a provisioning service, an ldap directory, etc.). Gartner will provide top three vendors we believe OARNet should short list.
  - Gartner will not provide RFP style, detailed product requirements.
  - Gartner will not be designing the implementation architecture for the individual institutions. This will require an additional engagements.
  - Gartner will not be providing institution specific schema designs.

# Q&A