InCommon

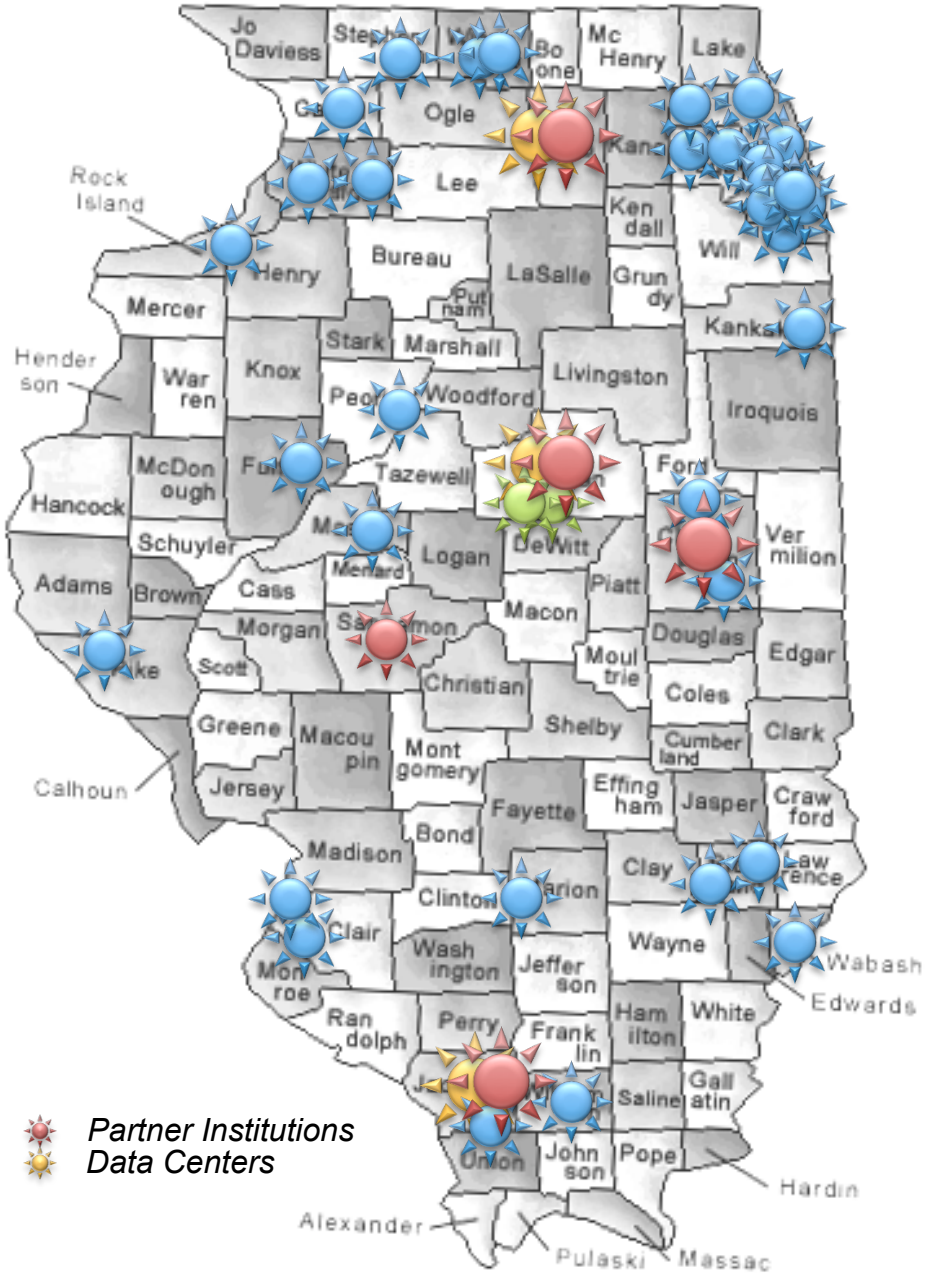
The Illinois K12 Pilot

Quilt/InCommon Workshop
Winter 2014
La Jolla

Bernie A'cs, NCSA at the University of Illinois
Jim Peterson, IlliniCloud and School District 87
Bob Lamvik, Aegis Identity
Micheal Grady, Unicon

Pilot Overview

NCSA and IlliniCloud are participants in the Illinois Shared Learning Environment (ISLE) project with the shared objective to develop an identity management solution that can be easily adopted by K12 school districts, and to implement procedures and processes required for school districts to manage their relationships with service providers and vendors.



Partners:

NCSA

Illini Cloud

SIU Southern Illinois University Carbondale

irc Illinois Interactive Report Card

Pilot Description – more details

IlliniCloud is a non-profit organization providing services for primarily for K12 school district all over the state of Illinois. Acting as a K12 federation operator and service provider, the IlliniCloud is establishing three foundational service dimensions for the K12 community:

- Data Services
- Identity Services
- Presentation Services

Minimal threshold of Adoption: The implementation is focused on mitigating integration requirements for K12 school districts adoption of services with little to no modification of existing practices and procedures.

Backend Interfaces & Services
Tenants (School Districts)

aegisIDENTITY
the identity software company

End-User Facing Interfaces
Tenants (School Districts)

UNICON

Initial Goals

The collaboration will undertake an implementation effort to establish an identity management infrastructure for K12 school districts that will satisfy functional requirements necessary for them to manage relationships with external service providers.

The implementation planned is conceptually a “hub and spoke” model that builds upon a philosophy that recognizes and supports local school district autonomy and decision making authority. The approach promotes use of lightweight “mediation service” that connects local school districts existing “directory services” with the central service hub

The central hub implementation will act as an Identity provider for the external “service providers” on behalf the school districts. The model will logically function like a “ProxyIdp/SP”; described as an identity provider that is back-ended by a service logic that discovers a given user’s true identity authority and delegates an authentication request

Challenges/Successes and Lessons Learned

Challenges encountered and how they were addressed

Unanticipated Issues

Successes and Lessons Learned

Successes

Unanticipated Benefits

Status and Path Forward

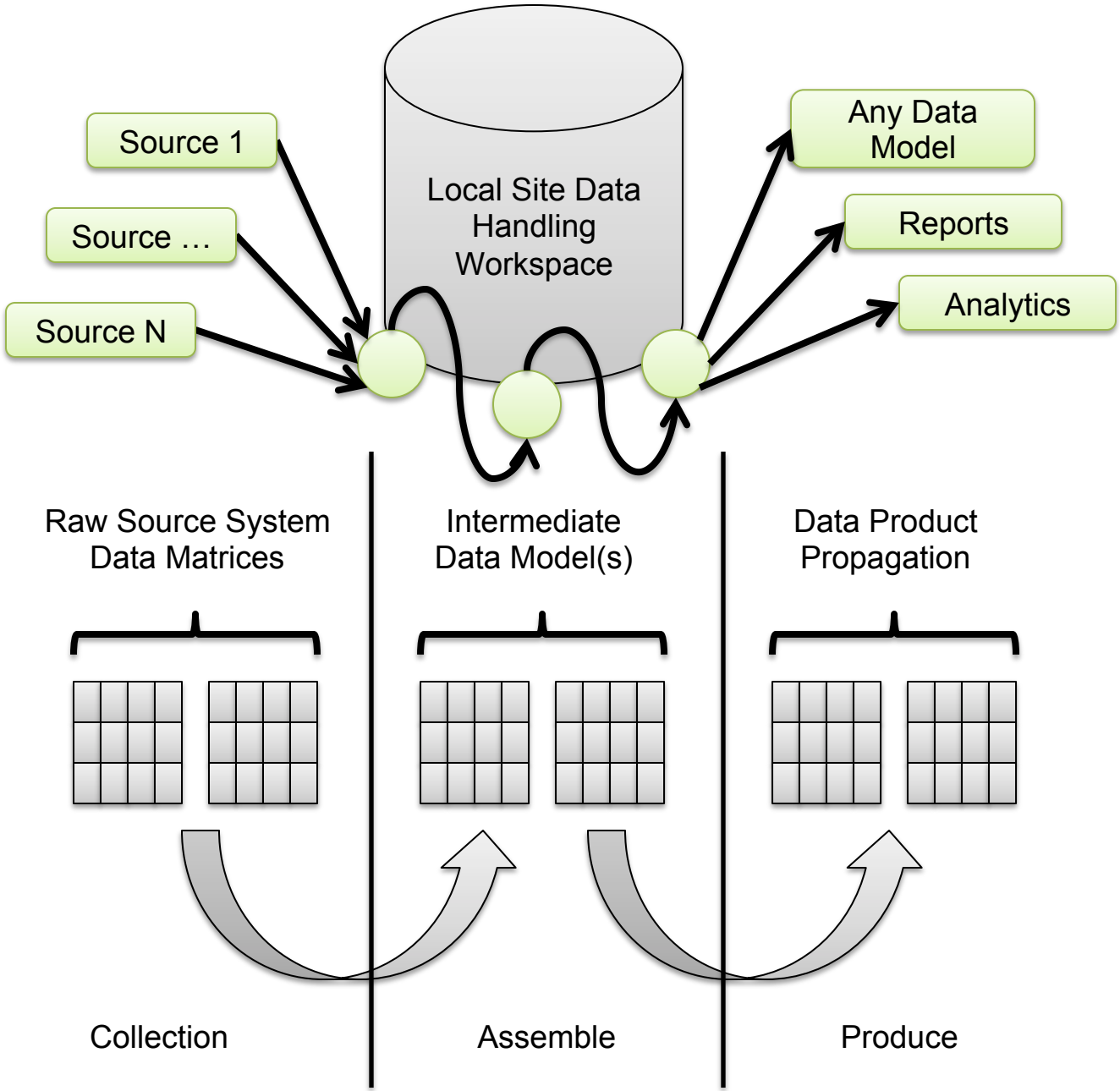
Where things are now

Plans for scaling beyond current scope (Post-Pilot Goals)

Next Steps

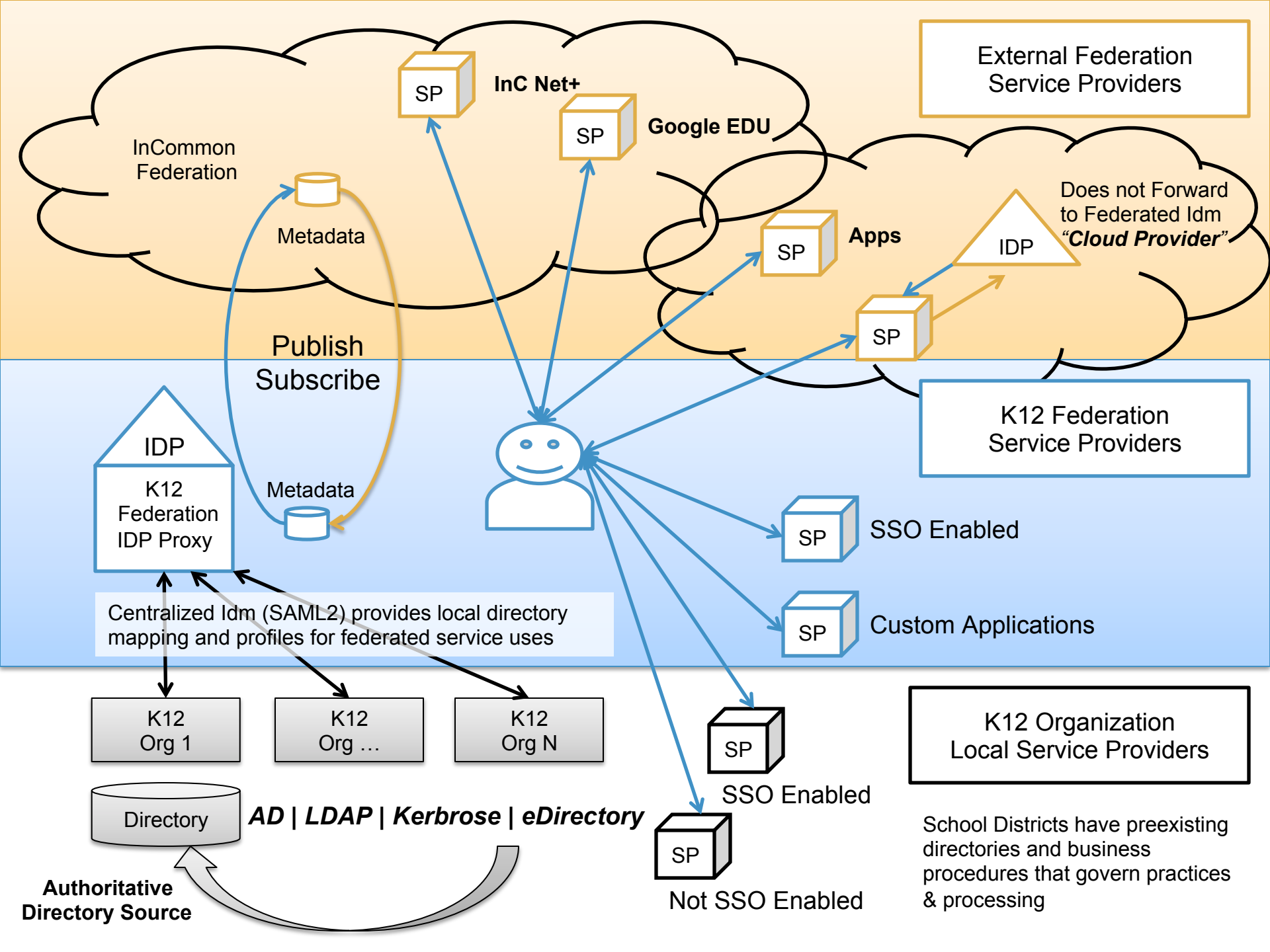
Data Service

- Data Asset Management
  - Managed Services and Local District Integration
    - Operational Data Store (Centralized ETL Platform)
      - SIF Integration
      - Utility Applications for non-Agent based integration
      - Authoritative Source System Integration
    - Operational Services (Value-adds)
      - Data Model assembly (SIF v2.5)(*verify ba)
      - Value validation processor
      - Extended ETL operations SIF->CED->inBloom (Ed-Fi 1.1.1)
      - Extended ETL operations SIF->CED->Ed-Fi Solution (Ed-Fi 1.2)
      - Extended ETL operations SIF<->ISBE)
    - Operational Integrity & Ownership (IT Operations)


Source 1
Source …
Source N
Local Site Data Handling Workspace
Any Data Model
Reports
Analytics
Raw Source System Data Matrices
Intermediate Data Model(s)
Data Product Propagation
Collection
Assemble
Produce

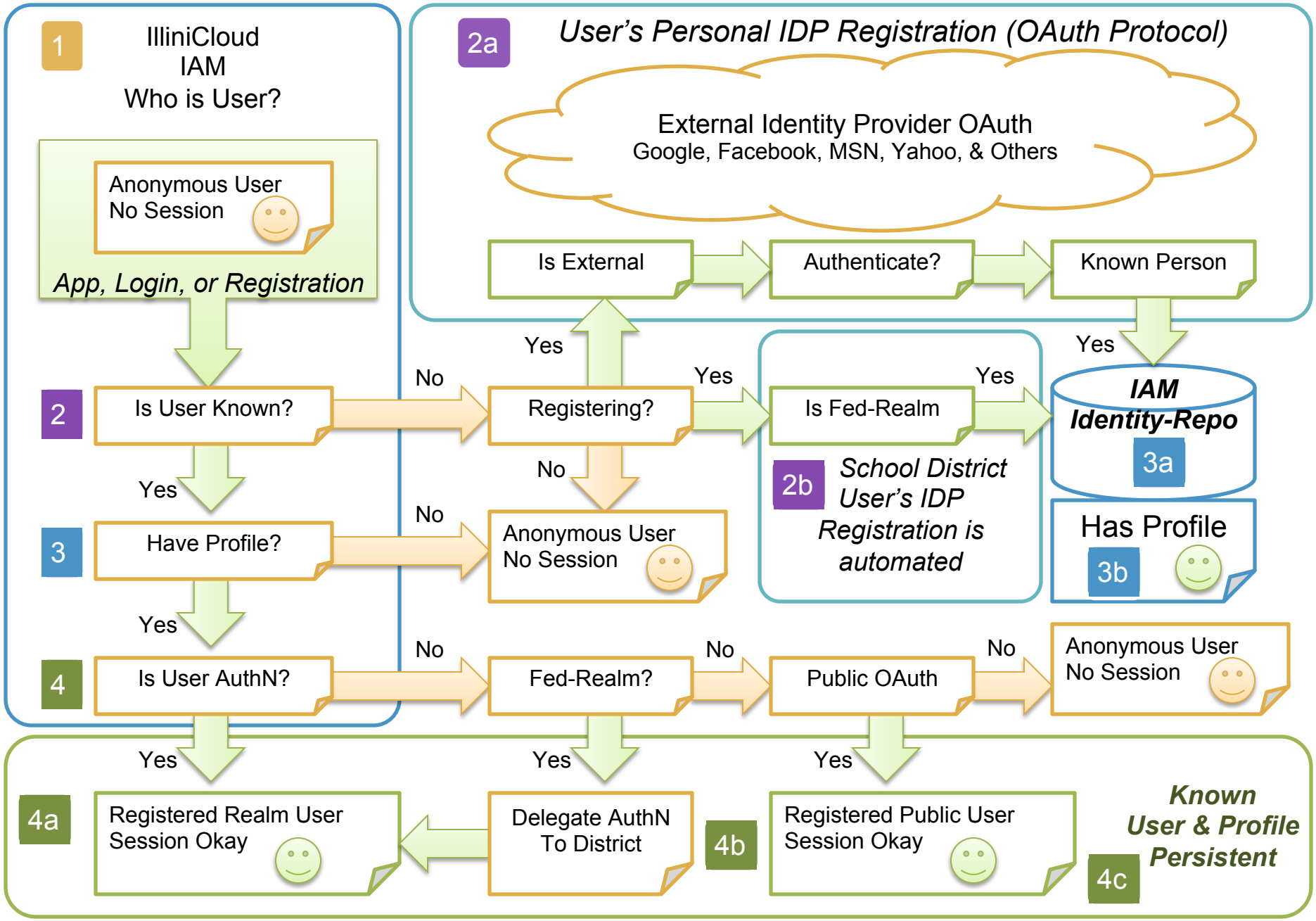
IlliniCloud IAM
Value Proposition

- Identity Access Management (IAM)
  - Facilitate local school district integration (IAM)
    - Existing Operational Environments at each site
      - Low threshold of change /modification to existing ops
        - Establishing Mechanical Connectivity and Operational Agreements
        - Facilitate transparent profile management for SD Identities
      - Integration of “roles” and “service providers” administration
        - Supply job role descriptor to enable services to map roles
        - SD must be able to manage SP relationships and “Attribute Release”
    - Data Sharing/Propagation is intimately related to IAM
      - Identity relations expressed in context of data model
        - Logical Entity Mappings for Staff, Teachers and more
        - Logical Access Controls based upon predefined API constraints
      - Critical Crosswalk Mapping required for IAM
        - Authentication management
        - Access control management (including audit ability)
    - Ownership, Operations, & Sustainability


External Federation Service Providers
SP
InC Net+
SP
Google EDU
InCommon Federation
Metadata
SP
Apps
IDP
Does not Forward to Federated Idm
"Cloud Provider"
SP
Publish
Subscribe
K12 Federation Service Providers
IDP
K12 Federation IDP Proxy
Metadata
SP
SSO Enabled
SP
Custom Applications
Centralized Idm (SAML2) provides local directory mapping and profiles for federated service uses
K12 Org 1
K12 Org …
K12 Org N
SP
SSO Enabled
K12 Organization Local Service Providers
Directory
AD | LDAP | Kerbrose | eDirectory
SP
Not SSO Enabled
School Districts have preexisting directories and business procedures that govern practices & processing
Authoritative Directory Source

IlliniCloud IAM Operational Requirements

- Identity Access Management (IAM)
  - IAM integration Services
    - Manage human user Identity (Known and Authorized)
      - Central Identity Service Platform
        - Minimal Identity Profile Management (Organization/Individual)
        - Self-Service (Individual) Service Provider Relationships
      - Local School District Identity Integration
        - Organizational Autonomy (Users, Roles and Vendors)
        - Facilitate Local Single Sign On (SSO)
    - Facilitate exchange of IAM values for logical user sessions
      - Centralize integration services for third party service providers
        - Federation Registry (Federated SSO-SAML)
        - Support SAML,Oauth, and OpenID
      - Facilitate Single Sign On (SSO)
        - With third party service providers (vendors and federation services)
        - Application registry and identity management
    - Business process integrity and management


1
IlliniCloud
IAM
Who is User?
Anonymous User
No Session
App, Login, or Registration
2
Is User Known?
Yes
3
Have Profile?
Yes
4
Is User AuthN?
No
Registering?
No
Anonymous User
No Session
No
Fed-Realm?
No
Public OAuth
No
Anonymous User
No Session
Yes
Yes
Yes
Yes
2a
User's Personal IDP Registration (OAuth Protocol)
External Identity Provider OAuth
Google, Facebook, MSN, Yahoo, & Others
Is External
Authenticate?
Known Person
Yes
Is Fed-Realm
Yes
2b
School District
User's IDP
Registration is
automated
Yes
IAM
Identity-Repo
3a
Has Profile
3b
4a
Registered Realm User
Session Okay
Delegate AuthN
To District
4b
Registered Public User
Session Okay
4c
Known
User & Profile
Persistent

IlliniCloud IAM
K12 Consortium: Federated Services

- Identity Access Management (IAM)
  - Federated Service Platform
    - K12 Identity Federation Service Provider
      - Logical Portal Tenant “Organization Entity” (school district)
        - Authoritative controls for query/AuthN (local directory)
        - Administrative interfaces to manage SP relations
    - Central Applications Service Support
      - Federation Services:
        - Certificate Management Services
        - SP Registration Interfaces (federation registry)
        - Web Portal Services (Primary User Management SP)
          - ISLE Applications
          - Organization Applications
          - User Pages

IlliniCloud Portal

Drew Wills/Unicon

One thing that makes this portal special is its requirements for Multi-Tenancy. Individual school districts are the “tenants” in this portal – and there are over 800 of them in Illinois!

Each tenant must be able to customize the appearance & content of the portal for its own needs. Users who log into the portal get the appropriate experience for the tenant (district) to which they are connected.

Tenant customization examples include logo, colors, header/footer text, navigation (tabs), and content (portlets). Tenants, moreover, not only need to manage these items, they also need to “manage the managers” – they must be able to grant or deny access to these management functions with regard to their own staff.

IlliniCloud Portal, Identity, & Data

- Central Portal Integration
  - User Profile & Application Launch Panel
    - Primitive Requirements
      - Human User Profile
      - Application Panel Preferences
    - Federated Applications
      - ISLE Applications (Phase 2 out comes)
      - InCommon (Applications & Services)
    - Continued Evolution, Operation, and Sustainability
      - Development, Quality Assurance, and Production
      - Application Integration Services

Successes and Lessons Learned

Successes

Unanticipated Benefits

Status and Path Forward

- Where things are now
- Plans for scaling beyond current scope
  - (Post-Pilot Goals)
- Next Steps

Questions?