NC Education Cloud
Identity and Access Management Webinar
10 AM Wednesday, April 18, 2012
Agenda

• Recap from last webinar

• General IAM updates

• Current Project Status

• Next Steps

• Q&A / Open Discussion
Recap: Recall the “Big Picture”

Vision: "Every student, teacher/staff member, parent/guardian, and school community member has a single unique username/password to access learning resources in North Carolina"

Challenges (Problem Statement):
1. Too many accounts for current services
2. Cumbersome manual process of updating account information from NCWISE to disparate local systems and services
3. Need solid foundation for K-12 cloud solutions growth
Tentative Schedule – Still on Track

Phase I – Research and Planning
Tentative Schedule: October 2010 – October 2011 (12 Months)

Phase II – Establish Service Model
Tentative Schedule: November 2011 – June 2012 (8 Months)

Phase III – Build and Implementation
Tentative Schedule: July 2012 – June 2013 (12 Months)

Phase IV – Full Production and Operation
Tentative Schedule: July 2013 – Ongoing
IAM Plan v5

- Version 4 of the IAM paper was completed December 2, 2011

- Version 5 of the IAM paper was completed February 29, 2012
  - Provides a snapshot of the proposed IAM system
  - Modified the IAM Service Model to purchase the IAM system “as a Service” (see next slides)
  - Facilitates IAM related communications within and among NC Education Cloud Team, LEAs, vendors, similar state or regional projects, and other interested parties.

- The Vision: “Every student, teacher/staff member, parent/guardian, and school community member has a single unique username/password to access learning resources in North Carolina”

Updated Service Model

Policy and Governance
- Requirements & Policies
  - State Board of Education
  - IAM Working Group
  - DPI/ITS
  - Friday Institute / NC Cloud Team
  - Educational Service Agency
  - Others?

Service Manager
- Collaborations between Roles
- Management of the Service Provider
- Coordination of Dependencies
- Service Manager Tech Support

Service Consumers
- Cloud Services (Vendors)
  - Applications
  - Services
  - Resources
- DPI
  - Applications
  - NCWISE
  - CECAS
  - UID
  - Others
- LEAs, Charters, NCVPS, NCSSM (Users)
  - End users
    - Self Service
    - Reduced/Single Sign-On
  - Delegated Admins
    - Pwd Resets
    - Sponsored Guests
    - Workflow Requests & Approvals
  - Ensure Accuracy of user data in Source Systems
  - Local Tech Support

Data Sources
- Systems of Record
  - NCWISE
  - HRMS
  - UID
  - Wake (HR)
  - CMS(HR)
  - NCSSM
  - NCVPS

Data Integration
- SW Vendor
  - IAM SW Stack
  - Recommends HW/OS
  - Technical Support
- Systems Integrator
  - Technical Architect
  - Design
  - Implementation
  - Technical Support

HW - Infrastructure Hosting
- Cloud Service
  - IaaS, SaaS
  - Technical Support
- Locally Hosted
  - HW/OS Platform Vendor
  - Technical Support

Authority

Requirements & Policies

Data Match & Merge
- Person Registry
- Provisioning of Accounts
- Authentication/SSO
- Authorization
- User Directory (LDAP)
- Directory data -> LEAs
- Access Management
- Provisioning of Access
- Federation
- User Self-Service
- Guest System

Delegated Administration
- Audit Logging, Reports
- Ongoing Support and Administration
  - Provisioning Rules
  - Request Workflows
- Application Onboarding & Integration with Service
  - All HW & SW support
  - Systems Integration
  - Vendor Technical Support

Data Match & Merge
- Person Registry
- Provisioning of Accounts
- Authentication/SSO
- Authorization
- User Directory (LDAP)
- Directory data -> LEAs
- Access Management
- Provisioning of Access
- Federation
- User Self-Service
- Guest System

Delegated Administration
- Audit Logging, Reports
- Ongoing Support and Administration
  - Provisioning Rules
  - Request Workflows
- Application Onboarding & Integration with Service
  - All HW & SW support
  - Systems Integration
  - Vendor Technical Support

Data Match & Merge
- Person Registry
- Provisioning of Accounts
- Authentication/SSO
- Authorization
- User Directory (LDAP)
- Directory data -> LEAs
- Access Management
- Provisioning of Access
- Federation
- User Self-Service
- Guest System

Delegated Administration
- Audit Logging, Reports
- Ongoing Support and Administration
  - Provisioning Rules
  - Request Workflows
- Application Onboarding & Integration with Service
  - All HW & SW support
  - Systems Integration
  - Vendor Technical Support
IAM Managed Service Provider

This figure shows what the NC Education Cloud project is looking to purchase (everything in the Yellow block). A complete “IAM as a Managed Service” offering.

Inputs to the Managed Service would be data either from a Data Integration service, or from the Source Systems, possibly in the form of a tab-delimited file(s). If the Data Integration service exists, the first two items (in blue) would likely be supported there. Otherwise, they would need to be part of the IAM Managed Service.

Additionally, policy and business practices would be provided - to be implemented through provisioning and workflow functions.

Target Systems would access the IAM Managed Service for a variety of reasons from authentication and user attributes to federation and data and audit reporting.

Managed Service

- Data Match & Merge
- Person Registry
- Provisioning of Accounts
- Authentication/SSO
- Authorization
- User Directory (LDAP)
- Directory data -> LEAs
- Access Management
- Provisioning of Access
- Federation
- User Self-Service
- Guest System
- Delegated Administration
- Audit Logging, Reports
- Ongoing Support and Administration
- Provisioning Rules
- Request Workflows
- Application Onboarding & Integration with Service
  - All HW & SW support
  - Systems Integration
  - Vendor Technical Support

SW Vendor
- IAM SW Stack
- Recommends HW/OS
- Technical Support

Systems Integrator
- Technical Architect
- Service Design
- Implementation
- Technical Support

HW Infrastructure
- Cloud Service
  - IaaS, SaaS
  - Technical Support
- Locally Hosted
  - HW/OS Vendor
  - Technical Support

or

Locally Hosted
- HW/OS Vendor
- Technical Support

SW Vendor
- IAM SW Stack
- Recommends HW/OS
- Technical Support
IAM Managed Service – Required Functionality

**Managed Service**
- Data Match & Merge
- Person Registry
- Provisioning of Accounts
- Authentication/SSO
- Authorization
- User Directory (LDAP)
- Directory data -> LEAs
- Access Management
- Provisioning of Access
- Federation
- User Self-Service
- Guest System
- Delegated Administration
- Audit Logging, Reports
- Ongoing Support and Administration
- Provisioning Rules
- Request Workflows
- Application Onboarding & Integration with Service
  - All HW & SW support
  - Systems Integration
  - Vendor Technical Support

**SW Vendor**
- IAM SW Stack
- Recommends HW/OS
- Technical Support

**Systems Integrator**
- Technical Architect
- Service Design
- Implementation
- Technical Support

**HW Infrastructure**
- Cloud Service
  - IaaS, SaaS
  - Technical Support
- Locally Hosted
  - HW/OS Vendor
  - Technical Support

**Account Provisioning & Directory Services**
- Data Integration Service
- Group, Role, & Entitlement Management
- Guest System (Accounts?)

**Authentication, User Attributes, SSO/Federation, Non-web Apps? & Service Account Provisioning**
IAM Managed Service – Sources & Targets

**Managed Service**
- Data Match & Merge
- Person Registry
- Provisioning of Accounts
- Authentication/SSO
- Authorization
- User Directory (LDAP)
- Directory data -> LEAs
- Access Management
- Provisioning of Access
- Federation
- User Self-Service
- Guest System
- Delegated Administration
- Audit Logging, Reports
- Ongoing Support and Administration
  - Provisioning Rules
  - Request Workflows
- Application Onboarding & Integration with Service
  - All HW & SW support
  - Systems Integration
  - Vendor Technical Support

**Sources**
- Systems of Record
  - HRMS
  - Wake-HR
  - CMS-HR
  - NCWISE
  - Others...

**Managed Service**
- SW Vendor
  - IAM SW Stack
  - Recommends HW/OS
  - Technical Support
- Systems Integrator
  - Technical Architect
  - Service Design
  - Implementation
  - Technical Support

**HW Infrastructure**
- Cloud Service
  - IaaS, SaaS
  - Technical Support
- Locally Hosted
  - HW/OS Vendor
  - Technical Support

**Shared Infrastructure & Cloud Services**
- IIS
- NCLOR
- Blackboard
- Moodle
- Google Apps
- Blackboard
- Live@EDU
- Follett
- Destiny
- ClassScape
- MCNC Web Security
- DiscoveryEd
- Others... TBD

**Targets**
IAM Service Manager Role

**Managing a statewide IAM Service** for the IAM Service Consumers as specified by the NC Education Cloud and other advisory bodies
   Phased approach / Pilot then Production

Responsible for management of the IAM Managed Service provider relationship

Establishing relationships and coordinate as needed with owners of authoritative source data systems

**Providing level 2-3 technical support services and a help desk (may be part of a larger NC Education Cloud Help Desk),** to the IAM Service Consumers for matters related to the IAM Service

**Ensuring implementation and support of policies** defined by IAM Policy and Governance bodies

**Providing technical and strategic guidance to the IAM Policy and Governance bodies** about any necessary policies that are needed to help the IAM Service Provider deliver and support a better IAM Service for the IAM Service Consumers

**Coordinating with IAM Managed Service provider to translate IAM Service Consumer and/or IAM Policy and Governance requirements** into enhancements or corrections for the IAM Service

**Coordinating with IAM Managed Service provider and IAM Service Consumers to onboard/integrate new Cloud Applications, Resources, and Services**

**Providing to IAM Service Consumers and IAM Policy and Governance bodies any reporting and audit information as needed** (may be provided by a Cloud Security and Compliance group)

**Providing training and documentation to IAM Service Consumers** as they onboard and use the resources/services provided by the IAM Service

**Tracking user suggestions** for improvements, features, and developing the methodology for IAM system enhancements

**Developing metrics and report on the impact of IAM** on the Service Consumers to IAM Policy and Governance where appropriate

**Communicating new IAM Service features** to appropriate IAM Service Consumer participants

**Managing vendor churn** for IAM System components

**Managing vendor contracts** and developing acceptance criteria for each checkpoint of a contract
Support Model / Help Desk Escalation Process

- **Support – Cloud**
  (NC Education Cloud Help Desk)
  *Triaged to appropriate Cloud Service*

- **Support – District**
  (Technology Director)

- **Support – School**
  (Teacher/Technology Facilitator)

- **Support - Service Manager**
  (Managed Service Provider)

- **Support - Vendor**
  (Managed Service Provider)

---

*** It’s unclear at this time where a response would go, but likely to the school or district level (not the user)
New Data Integration Project

• Data Integration Update
  • Sammie is leading separate Data Integration effort
  • DI can become authoritative source for IAM, once it’s available
IAM Managed Service RFP Process

• IAM Managed Service Provider RFP will come through ITS, on behalf of DPI
  – IAM Service RFP via DPI/ITS
  – Service Manager role will not be part of that RFP

• RFP draft is currently working its way through DPI and ITS

• Goal: announce award by summer, 2012
Key RFP Steps: Past, Current, Soon

1. Drafting
2. Review of Draft
3. RFP draft goes to DPI
4. DPI reviews / updates
5. RFP draft goes to ITS
6. ITS reviews / updates
7. RFP “hits the streets”
8. Question submission period
9. Final responses to questions published 1 week later
10. Vendor RFP response submissions due ~2 weeks later
11. Response evaluation, includes meetings/PoCs with lead candidates
12. Recommended selection made to administrative team
13. Award announced
Key Next Steps

• Top priority: Complete the RFP process
  • Award vendor Summer 2012

• Source Data Integration, IAM Managed Service Technical Implementation Plan (vendor), Installation and Configuration of the IAM-MS, Target Services Integration, Pilots
  • During first year

• Service Manager will serve as intermediary between Managed Service Provider, LEAs/Charters, DPI, Policy and Governance

• Sammie will facilitate the Data Integration project in parallel

• Production IAM system 12 months after award
Open Q&A + Contact Info

• Web site—place for FAQ, Guidelines, Presentations, Organization, Team members, news, links to DPI & others: [http://cloud.fi.ncsu.edu](http://cloud.fi.ncsu.edu)

• IAM Email List is [cloud-iam@lists.ncsu.edu](mailto:cloud-iam@lists.ncsu.edu)

• Sammie Carter, [swcarter@ncsu.edu](mailto:swcarter@ncsu.edu), 919-513-8513

• Mark Scheible, [mscheible@mcnc.org](mailto:mscheible@mcnc.org), 919-248-1997

• Steve Thorpe, [thorpe@mcnc.org](mailto:thorpe@mcnc.org), 919-248-1161