NC Education Cloud
Identity and Access Management Working Group
10 AM Wednesday, October 26, 2011
• General Updates

• Question of the Day Feedback

• IAM Plan v3.0

• Next Steps

• Q&A / Open Discussion
• Roll Call

• Recent Site Visits
  ➢ Winston-Salem/Forsyth County Schools
    ➢ Included CSI Outfitters
  ➢ Wake County Public School System
    ➢ Met with around a dozen tech staff
    ➢ Also had teleconference with data manager Harriet Dunston
  ➢ Many thanks to Betty Weycker, Walter White, and all meeting participants. These discussions were very helpful!

• Last Call for Vendors
  ➢ We’re now finishing up communications with vendors in preparation to move to the next phase – the RFP process
General Updates (2)

• **Internet2 Member Meeting / NCREN Community Day Presentation**
  - NC Education Cloud project, including IAM, was presented
  - Search for “North Carolina Education Cloud” link here: [http://events.internet2.edu/2011/fall-mm/agenda.cfm](http://events.internet2.edu/2011/fall-mm/agenda.cfm)
  - Slides are available from the site
  - Many other sessions from the I2MM were archived in video format for later viewing at your convenience

• **Staff Data Sets**
  - Starting in early October, Sammie obtained access to some staff (UID) data via MFTS
• **Initial Apps**
  - Google Apps and Office 365 are likely high on the list
  - Data from all 115 site surveys will help prioritize
  - Interactions with other parts of the Cloud project will help too
  - As the policy and governance structure is solidified, input from the governing bodies will be sought

• **Authentication Methods**
  - Several models are described, including the Local Authentication method for disaster recovery
  - See “Appendix D – Requirements for Integrating Cloud Applications, Resources, and Services with the NC Education Cloud Identity and Access Management System”
• **Agency Involvement**
  • In addition to the LEAs, we are indeed seeking active communication/involvement with DPI and ITS
  • Want to avoid the silos if at all possible

• **RFP Process**
  • It is definitely possible there might be a contingency included to have periodic reviews for continuance. Though the terms are still TBD.
IAM Plan V3

• Version 3 of the IAM paper was completed October 2
  • “DRAFT” was removed
  • Provides a snapshot of the proposed IAM system
  • New contributions from Mark Scheible on Service Model and other sections
  • Facilitates IAM related communications within and among NC Education Cloud Team, LEAs, vendors, similar state or regional projects, and other interested parties.
  • Feedback is welcomed from all potential stakeholders, as it will enhance project success

• 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”

Valuable Input Has Been Received From Many Sources

- Alamance-Burlington School System
- Catawba County Schools
- Durham Public Schools
- Granville County Schools
- Mooresville City Schools
- LEA Site Surveys
  - DPI
  - ITS
- LEA Tech Directors
- This IAM Working Group (20+ Educational Organizations)
- AegisUSA
- CA Technologies
- CampusEAI
- CSI Outfitters
- Data Networks
- IBM
- Identity Automation
- Microsoft
- Mycroft
- Oracle
- Pearson
- Radiant Logic
- Zscaler
- etc.....
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>10</td>
</tr>
<tr>
<td>PROJECT BACKGROUND</td>
<td>11</td>
</tr>
<tr>
<td>IDENTITY MANAGEMENT OVERVIEW</td>
<td>14</td>
</tr>
<tr>
<td>PART I POLICY AND GOVERNANCE</td>
<td>16</td>
</tr>
<tr>
<td>PART II REQUIREMENTS AND SPECIFICATIONS</td>
<td>29</td>
</tr>
<tr>
<td>PART III SERVICE MODEL</td>
<td>71</td>
</tr>
<tr>
<td>IAM Service Roles</td>
<td>74</td>
</tr>
<tr>
<td>Step 1: Building the IAM System</td>
<td>83</td>
</tr>
<tr>
<td>Step 2: Deployment and Migration Model</td>
<td>88</td>
</tr>
<tr>
<td>Step 3: Production and Operating Model</td>
<td>89</td>
</tr>
<tr>
<td>APPENDICIES</td>
<td>90</td>
</tr>
<tr>
<td>APPENDIX B – REGULATORY AND COMPLIANCE</td>
<td>95</td>
</tr>
<tr>
<td>APPENDIX C – IAM RESEARCH</td>
<td>97</td>
</tr>
<tr>
<td>APPENDIX D – REQUIREMENTS FOR INTEGRATING CLOUD APPLICATIONS, RESOURCES,Services with the NC Education Cloud Identity and Access Management System</td>
<td>98</td>
</tr>
<tr>
<td>APPENDIX E – IAM PROJECT RISKS</td>
<td>106</td>
</tr>
<tr>
<td>APPENDIX F - FREQUENTLY ASKED QUESTIONS</td>
<td>107</td>
</tr>
<tr>
<td>GLOSSARY</td>
<td>110</td>
</tr>
</tbody>
</table>
• **We seek your approval of the final IAM plan** before we start Phase 2 of the project, RFP(s). We want to make sure you feel we have done sufficient research/planning and adequately captured your challenges around identity management.

• **RFP(s)** - We will be forming teams soon that will be participating in the RFP(s) process. The LEA community will have a large representation in this process. We will touch base with you to solicit participation when we are ready to start that process. We first would like any of your final input to and your approval of the plan.
IAM Project Outline and (Tentative) Schedule

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
Tentative RFP Steps

Step 1: RFP Preparation (November through January)
Step 2: RFP Release (Mid-February 2012)
Step 3: RFP Team Review Responses (April 2012)
Step 4: RFP Awarded (Late May/Early June 2012)
Step 5: Develop detailed technical implementation plan with platform provider(s)
Step 6: Initial piloting / implementation (Fall 2012)
Open Q&A + Contact Info

- 10 AM Nov. 2: informational webinar for Tech Directors

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

- IAM Email List is cloud-iam@lists.ncsu.edu

- Sammie Carter, swcarter@ncsu.edu, 919-513-8513

- Steve Thorpe, thorpe@mcnc.org, 919-248-1161
REST OF SLIDES ARE ON THE BACK BURNER
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
Identity and Access Management (IAM) System has 3 Major Components

1. Central Data Repository
   The central repository will be comprised of relevant user data from various authoritative data sources

2. Central Directory Service
   The central directory will contain all user IDs, passwords, and other identity information. It will serve as master authentication and authorization point for all cloud-based services and allow syncing to LEAs

3. Federation Software
   The federation software security extends identity information to cloud-based services providing end users with single sign on experience
User Account Provisioning

Step 1
NCWISE and HRMS Coordinators manage users information as normal

Step 2
Student and HR data is propagated to IAM system

Step 3
User accounts are provisioned in IAM System and granted access to new Cloud Services and current LEA services
Local LEA and IAM Directory Integration

Local users log into devices and authenticate against Local LEA Directory Service as normal.

Local LEA Directory Service can sync to Central Directory Service for global user accounts.

Central Directory Service gets provisioned from Authoritative Data Sources.

Local LEA and IAM Directory Integration
Local LEA and IAM Directory Integration

Local LEA Directory Service could be Open Directory, Active Directory, or eDirectory

Synced Global Users from Central Directory Service
- Local Users
- Local Applications
- Local Printers
- Local Workstations
- Local Servers
- Other local stuff

Local Users log into devices and authenticate against Local LEA Directory Service as normal.