CIC Approach to Federation

InCommon CAMP / Columbus, OH
June 2011
Matt Kolb <mk@msu.edu>
CIC IdM Co-chair

CIC Members (http://www.cic.net)

CIC Overview

- Provosts' Organization created to:
  - Advance Academic Mission
  - Generate Unique Opportunities for Students & Faculty
  - Share Expertise
  - Leverage Campus Resources
  - Collaborate on Innovative Programs

Does any of this sound familiar?

Smells like Federated Services sales pitch to me.

Approach

- Don't reinvent InCommon
- Identify projects
  - Everybody joins InCommon
  - Hook up with some SPs (TeraGrid, CILogon, HahtiTrust, MONK, etc, etc, etc)
  - Agree on Federated Security Incident Response
  - Figure out how to do Silver
  - Build relationships across schools in functional areas
- Iterate!

New Stuff

- Research CI Focus
  - Work with Research Virtual Organizations (VOs)
  - Lower the bar to SP onboarding
    - Attribute Bundles
    - User Consent (uApprove)

- # Mark Rank
  - UW-Milwaukee
  - Middleware Architect / IAM Program Manager
  - Email - rankm@uwm.edu

Consortium at UWM

- # University of Wisconsin System
  - o 2 Research, 11 Comprehensive, and 13 2-Year Institutions plus statewide Extension
- # LIGO Virtual Organization
- # SeWHiP
  - o Loose affiliation of research institutions in SE Wisconsin
- # State of Wisconsin

Enablers

- Have a pre-existing history
- Have an organizational mandate
- Have a "Killer Solution"
- Have a "Killer Problem"
- Have a disruptive opportunity
- Have an embedded team of motivated technologists

Challenges

- Finding champions and/or willing peer partners
- Achieving critical mass of consortium members at the same maturity level
- Navigating politics
- Building trust
- Stay ahead of the technology

North Carolina Identity Federations

Mark Scheible, IAM Consultant, MCNC

UNC Identity Federation

All constituent members of the University of North Carolina are full members of the Federation (including UNC Center for Public Television). MCNC, the non-profit entity that operations the North Carolina Research and Education Network (NCREN) is also a member.

Universities

Appalachian State University

East Carolina University

Elizabeth City State University

Fayetteville State University

North Carolina Agricultural and Technical State University

North Carolina Central University

North Carolina State University

University of North Carolina Asheville

University of North Carolina at Chapel Hill

University of North Carolina Charlotte

University of North Carolina Greensboro

University of North Carolina Pembroke

University of North Carolina School of the Arts

University of North Carolina Wilmington

Western Carolina University

Winston-Salem State University

High School

North Carolina School of Science and Math

Affiliates

UNC-TV

MCNC

Overview – Six Principles

1. Find the "Killer Application"

2. Minimize Costs

3. Stay Focused

4. Standardize Deployments

5. Herd the Cats

6. Grow – as needed/required

Summary

- UNC runs its own federation
  - Metadata file (XML)
  - WAYF (Where are you from?)

- No additional cost to interoperate between:
  - UNC schools
  - MCNC/NCREN services
  - Vendors (Google, SciQuest, PeopleAdmin*, ZimRide*, Qualtrics*, etc)

- Baseline for all new application development

- Could interfederate with another [state] federation (e.g. CC, K-12)
  - Technically simple
  - MOU to handle the "trust" aspect

MCNC – Federated Identity Management (FIM) Task Force

- First meeting in November, 2007

- Tasked with exploring FIM for North Carolina's K-20 community

- Evaluated two Federation Models
  - Build your own (e.g. UNC Identity Federation, UT)
  - Use an existing (InCommon) Federation (e.g. UC Trust)

- Benefits to InCommon Model
  - Already established Trust Federation
  - All the policy and governance work was done
  - We had limited experience at the time

The NCTrust Pilot

- The NC Trust Pilot began during 2008

- Goal: create a pilot identity federation to test web resource sharing among several K-20 organizations within NC

- Participants will gain access to online resources using their usernames and passwords as assigned by their home organizations

- Service providers will be able to make access decision to their resources by utilizing the identity management systems of the participants

NC Trust Pilot Participants

- Duke University

- NC State University

- UNC Chapel Hill

- MCNC

- NCDPI

- Rockingham County Schools

- Davie County Schools

- Wake Tech CC

- Virtual Computing Lab (VCL)

- NC Live

Key Milestones and Challenges

- Getting started was a huge learning curve

- Developed an NCTrust Memorandum of Understanding (MOU) for participation in the Pilot in August, 2008

- ShibFests were held at MCNC Oct, 2008 and Feb, 2009

- Getting participants to complete the "paperwork" (InCommon Participation Agreement and MOU) required some handholding

Key Milestones and Challenges (Cont.)

- Frequently, legal departments needed to be helped through the MOU and InCommon Agreement

- Building NCTrust on top of InCommon was not "straightforward" – there were no white papers or "cookbook" directions (learning curve)

- Determined that many participants lacked the skillsets required for standing up an IdP (particularly in K-12 and smaller HE institutions)

- Creation of NCTrust VM IdPs for K-12 and smaller institutions to help them get off the ground (with assistance from MCNC)

NCTrust Pilot Outcomes

- The pilot ran through December, 2009

- A report on the lessons learned during the pilot was presented in early 2010

- Recommendations and ideas on how a state-wide K-20 federation would be funded, operated and governed in the long-term were proposed

- The meeting notes and documentation on NCTrust are available on the FIM-TF Wiki at: https://edspace.mcnc.org/confluence/display/FIM/Home+-+Federated+Identity+Management+TF

Next Steps for FIM-TF/NCTrust

- Get more CC and K-12 participants and find "champions"

- By adding SPs that focus on Community Colleges and K-12, increase the value proposition for NCTrust membership

- Revisit some of the unique issues for K-12

  – Minors (< 18 years old) – legal "consent" issue

  – Parent involvement (How? Maintain accounts, use Social Identities?)

  – Attribute Release / New attributes? (e.g. eduPersonLegalAge, GradeLevel?)

  – IdP strategy (LEA, Regional, State?)

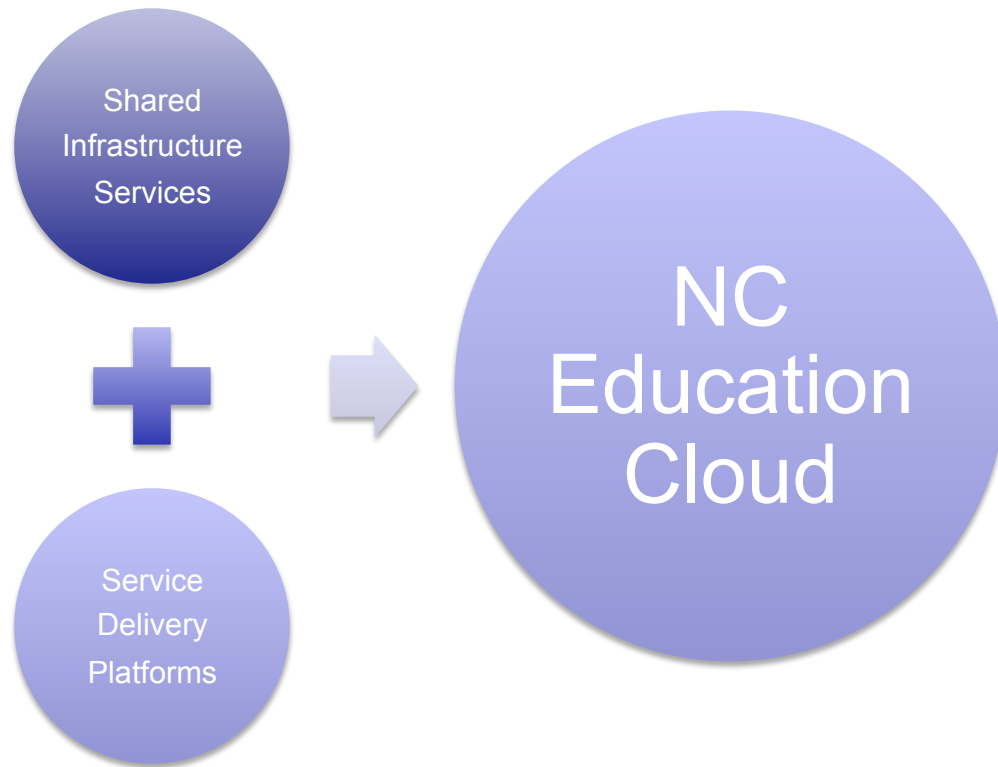- Explore funding options for future expansion of NCTrust
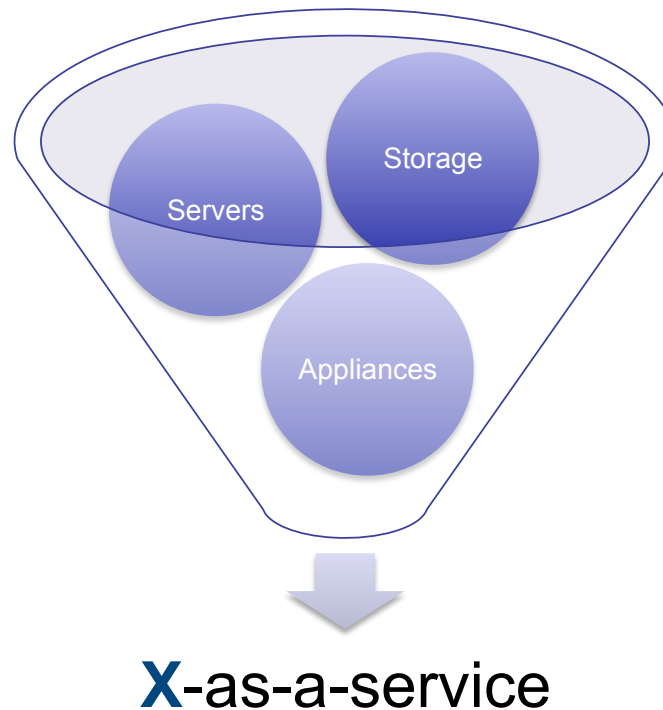
NC Education Cloud

Key Concerns

- Few LEAs have a solid, FT infrastructure

- Few have access to the data that they feed to DPI (NCWISE)

- Many don't carry common attributes in their directories

- To even consider K-12 federation these challenges need to be solved

Shared Infrastructure

X-as-a-service

Where "X" is Infrastructure or Software or Desktop or …

NC Education Cloud end game...

- LEAs pay substantially less as part of a buyers' consortium

- A shift in emphasis from technology support to instructional support

- Increased IT efficiency – fewer more highly utilized servers and other resources

- Increased service reliability – servers hosted in professional data centers with backup, DR, and service level guarantees

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*"

NC Education Cloud Services

Central Data Respository
Central Directory Service
Federation Software

IAM System

NCWISE Coordinator

HRMS Coordinator

Authoritative Data Sources

Local LEA Directory Service
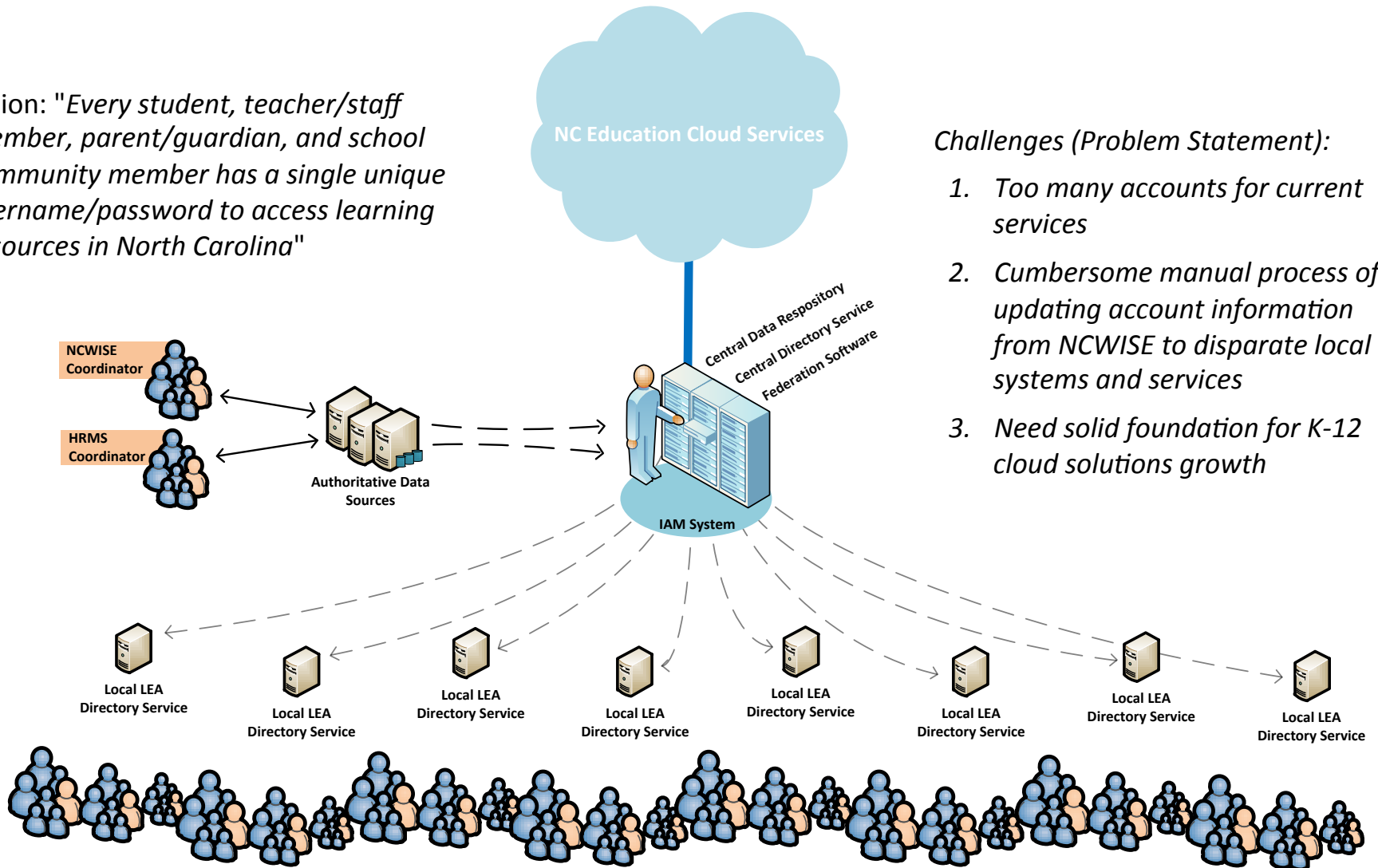
Challenges (Problem Statement):

1. Too many accounts for current services

2. Cumbersome manual process of updating account information from NCWISE to disparate local systems and services

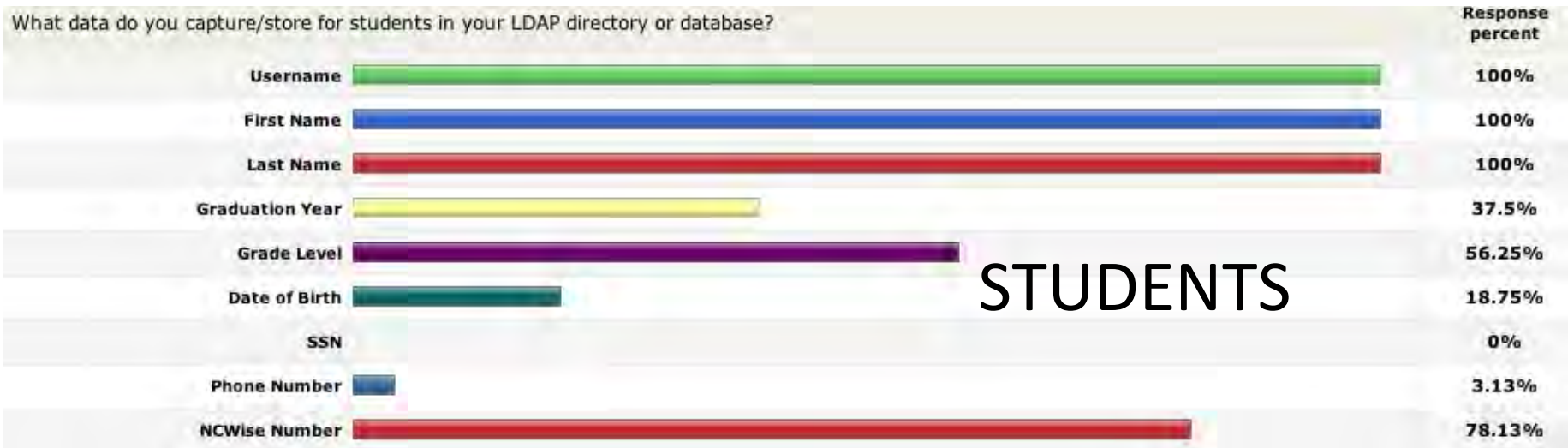3. Need solid foundation for K-12 cloud solutions growth

A few IAM-related data points gathered from 40 of the early LEA site interviews

- Directory Environments Deployed in your district:
  - Active Directory: 52.5%
  - eDirectory: 37.5%
  - OpenLDAP: 7.5%
  - Multiple: approximately 10-15%

- What username/password administration software do you use?
  - Active Directory: 62%
  - eDirectory: 43%
  - OpenLDAP: 13%
  - Other: 9 ManageEngine AD Self Service
              21 Workgroup Manager (WGM) on the Mac)
              35 AD Manager Plus

- <u>67.5% </u>of PreK-K5 Students have unique usernames in the system

Examples of data captured in Directory or Database

NOTE: These are preliminary and as yet incomplete sample numbers
that may not be representative of all the LEAs – there's more data to come!

What data do you capture/store for students in your LDAP directory or database?

	Response percent
Username	100%
First Name	100%
Last Name	100%
Graduation Year	37.5%
Grade Level	56.25%
Date of Birth	18.75%
SSN	0%
Phone Number	3.13%
NCWise Number	78.13%

STUDENTS

What data do you capture/store for staff in your LDAP directory or database?

	Response percent
Username	100%
First Name	100%
Last Name	100%
Graduation Year	0%
Grade Level	2.78%
SSN	2.78%
Phone Number	11.11%
HRMS Number	8.33%

STAFF

Tentative IAM Timeline

- Summer 2011: Build prototype/proof of concept(s) to show stakeholders and use as a tool to refine requirements and specifications for RFPs

- Fall 2011: RFPs awarded and then Build / Test / Setup Central IAM System and Engage in LEA Pilot interest

- Spring 2012: Formal Pilots of IAM System

- Summer 2012: Transition to Production

- Fall 2012: Deploy in Production Mode with Phased LEA adoption