SLDS Topical Webinar Summary

Identity Management Approaches: Protecting Access while Serving Multiple Stakeholders

This webinar featured Neal Gibson, Director of the Arkansas Department of Education's Arkansas Research Center, and Robert Swiggum, Chief Information Officer for the Georgia Department of Education, who presented on their states' unique approaches to identity management. Presenters discussed the types of stakeholders served, authentication approaches used, user roles and access rights, district involvement, and privacy and security issues.

The Intricacies of Identity Management

With the convenience of online education data comes a slew of issues: How do we protect the data? Who is allowed to access what data? And how can the process of accessing data be made secure without being cumbersome for the user?

Understandably, identity management is a complex issue. Some issues state education agencies (SEAs) must consider include the following:

- *Establishing identity*: the process of associating a physical person with verified identity information prior to the issuance of digital identifiers and the creation of a user account.
- *Authentication*: the process of gaining confidence that the person using a digital identity is the person who is qualified to use it.
- *Authorization*: the process of determining a specific person's eligibility to gain access to an application or function or to use a resource.
- *Enterprise directory*: a central institutional lookup repository that holds data regarding the institution's people and services, informing authentication and authorization processes.
- *Reduced or single sign-on (RSSO)*: a method of authentication that lets a user log into a network and, for a period of time, have his or her credentials passed to the requested applications, enabling use of the resource without requiring separate authentication for each one.
- *Federated identity*: the means of linking a person's electronic identity and attributes across multiple distinct identity management systems.[1]

States may manage any number of operating systems—systems that often require users to create and remember separate login credentials. Additionally, much staff time may be devoted to adding/removing the same user to/from multiple systems, or changing a user's permissions in multiple systems. A coherent approach to identity management can increase user satisfaction and overall security, and decrease time and resources spent managing user accounts across multiple systems.

[1]Ronald Yanosky with Gail Salaway. Identity Management in Higher Education: A Baseline Study. Available at *http://net.educause.edu/ir/library/pdf/ERS0602/ekf0602.pdf*

This product of the Institute of Education Sciences (IES) was developed with the help of knowledgeable staff from state education agencies and partner organizations. The content of this publication was derived from a Statewide Longitudinal Data Systems (SLDS) Grant Program monthly topical webinar that took place on May 29, 2012. The views expressed do not necessarily represent those of the IES SLDS Grant Program. We thank the following people for their valuable contributions:

Webinar Presenters:
Neal Gibson
Arkansas Department of Education's Arkansas Research Center

Robert Swiggum
Georgia Department of Education

Moderator:
Baron Rodriguez
SLDS Program, State Support Team

For more information on the IES SLDS Grant Program or for support with system development, please visit http://nces.ed.gov/programs/SLDS.

ies NATIONAL CENTER FOR EDUCATION STATISTICS
Institute of Education Sciences

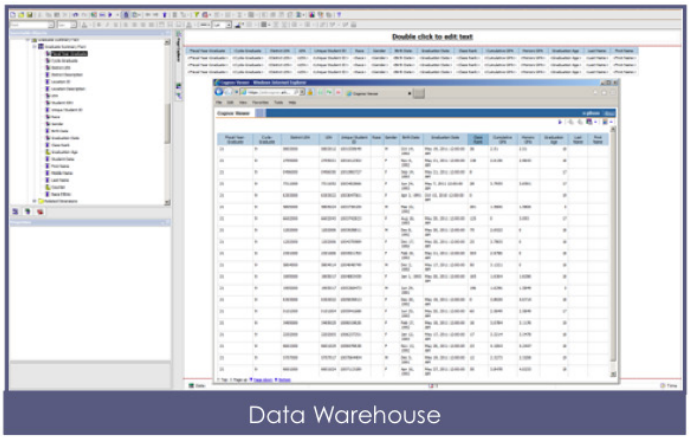
Multiple Systems in Arkansas

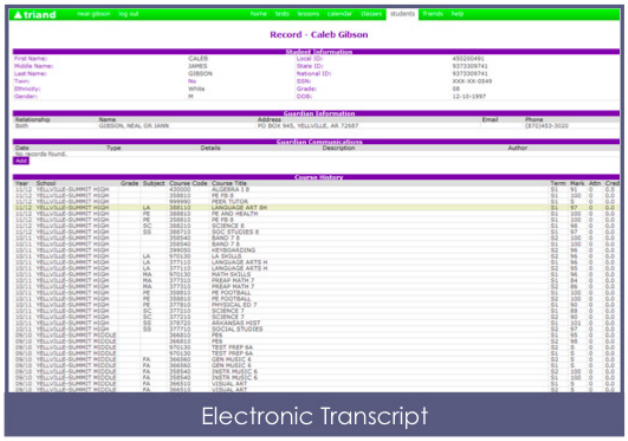
Arkansas has a problem that is common among SEAs: too many systems, and no single sign-on solution. As depicted in Figure 1, these systems are

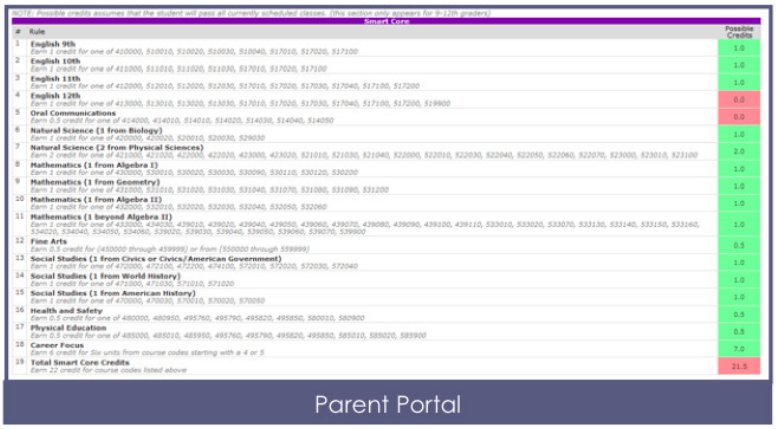
- data warehouse – a real-time tool for the student information system (SIS), used to query data and produce reports. Access is directly determined by SIS access.
- electronic transcript – the data belongs to the district, so levels of access are decided at the district level. A "super user" is named for each district. The super user is the system administrator who handles access, passwords, etc.
- parent portal – allows parents to view how their child is progressing in completing the "Smart Core" set of classes, which are required for the state's lottery scholarship.
- Academic Challenge Scholarship application – students can apply online and allow access to their transcript for determination of scholarship eligibility.

Users with multiple roles, which is common in states with small, rural districts, is another issue. In smaller districts, especially, local education agency (LEA) staff may hold more than one position, and therefore have multiple levels of access. As of right now, such staff have multiple log-ins, which is not ideal.

Figure 1. Screen shots of Arkansas's multiple data systems


Data Warehouse


Electronic Transcript

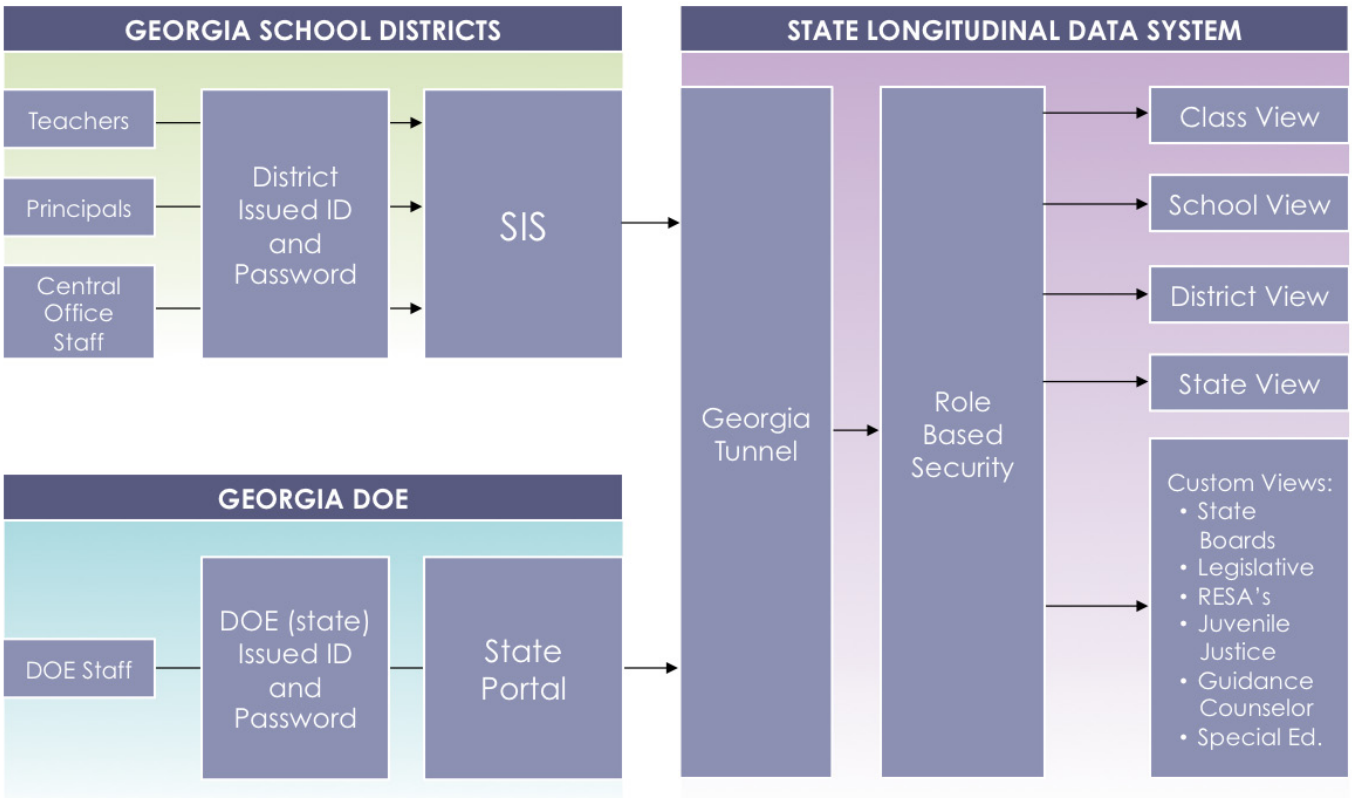

Parent Portal

Scholarship Application

The Georgia Identity Management System

The Georgia model bypasses the need for a single sign-on system, because all state systems can be accessed through the LEA's SIS. Once a user has signed on to the LEA's SIS, they can be transferred through the click of a button to the statewide longitudinal data system. This connection, called the Georgia Tunnel[2], passes the user seamlessly to the portal hosted at the Georgia Department of Education. The user's role at the LEA level is transferred to the state level and determines the user's access and view. Figure 2 illustrates how users at both the local and state level can gain access to the SLDS through a seamless link from either their SIS or state portal, respectively.

Figure 2. Users statewide can access Georgia's SLDS through the Georgia Tunnel



To initiate this system, the SEA had to approach the SIS vendors at the LEA level, who charged roughly $1,000 per school to add a button to the Georgia Tunnel. Additionally, all passwords and roles are maintained at the district level. If an LEA needs to add a new role, they must go back to their original SIS vendor. However, because the statewide portal is really an extension of the LEA's portal, users are in familiar territory, and thus the Georgia Tunnel had a very high adoption rate.

Security/Data Use Processes

Neither Arkansas nor Georgia monitor identity management nor passwords at the local level. However, both states provide security training, and both have signed statements from superintendents confirming that they understand how to manage data. Additionally, statewide policies, such as the complexity of passwords and how often they need to be changed, ensure that security issues are handled efficiently and uniformly across LEAs.

[2]The Georgia Tunnel is available for free download via the Public Domain Clearinghouse in GRADS360° at *https://nces.grads360.org*. To request access to GRADS360 °, please send your name, title, agency, and state to *accounts@grads360.org*.