Nebraska Directory Services

Web Based Authentication Standard for State Government Agencies.

Monday, September 27, 2004
Nebraska State Office Building Room LLD
10 AM - Noon

You are invited to attend this important informational meeting where a new web based application security standard will be introduced. In addition, there will be an overview of NDS and what capabilities can come from using an enterprise directory service. Following that will be an opportunity for feedback comments and Q&A. The information presented and discussed will be of vital interest to any agency developing web based applications.

Agenda:

1. Proposed Web Based Authentication Standard (10 mins.)
2. Overview of the Nebraska Directory Services project (15 mins.)
3. Discussion of the processes.
    a. Detailed discussion of the Authentication and Authorization process (15 mins.)
    b. Demonstration of the Enterprise Directory (20 mins.)
4. Questions and answers (60 mins.)

Benefits to using the Enterprise Nebraska Directory Services

1. **Streamlined Administration**
    a. Central repository – A single, redundant repository for managing all users.
    b. Delegated / centralized administration – Administration can be carried out either centrally or it can be delegated out to the agency or their designated resource.

2. **Single User repository**

    When John Smith changes his email address today, he must contact each individual application, not even agency… to request a change to his profile, or risk losing access to some of all functions within that application. By employing a single user repository, when John Smith's email is changed, all agencies and applications can have that change 'pushed' to them programmatically, instantly.

3. **Secure API for Development**
    a. No duplication of effort
    b. Savings – IMServices has seen an approximately 25-30% saving in development, because the security has already been built.
    c. Enhanced Security – The API is a proven, secure, standards based LDAP authentication and authorization mechanism that can now be leveraged by any developer, regardless of their experience or skill level.

4. **Opportunities for enhanced auditing**
    a. Better auditing capabilities.
    b. Easier compliance with State and Federal regulations. (i.e. HIPAA, IRS, Gramm-Leach-Bliley, Sarbanes Oxley, etc…)

5. **Enhanced Security**
    a. Single gateway to the State network – eliminate the multiple ingress points to the state network that are currently required.
    b. Ability to apply policies to all users.

6. **Role-Based Authorization.**

    Users are only allowed to see the information they are cleared to access. Restrictions with regards to read, write, and delete capabilities are also granted based upon their role. This greatly reduces the amount of administration while at the same time increasing the level of security.

Nebraska Information
Technology Commission

STANDARDS AND GUIDELINES

Web Based Authentication Standard for State Government Agencies

Category	**Security Architecture**
Title	**Web Based Authentication Standard for State Government Agencies.**
Number	

Applicability	☑ State Government Agencies, **excluding** Higher Education; and agencies receiving an exemption pursuant to Section 4.2……........... **Standard** ☐ **State Government Agencies,** all ....**Not Applicable** ☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.................**Not Applicable** ☐ **Other:** _____________ ....**Not Applicable** **Definitions:** **Standard** - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of the Nebraska Information Technology Commission after review by the Technical Panel (see Section 4.2). **Guideline** - Adherence is voluntary.

Status	☐ Adopted	☑ Draft	☐ Other:________
Dates	Date: September 27, 2004 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard:

The state will standardize on a secure methodology in which individual users will be required to authenticate against the state enterprise LDAP directory, known as Nebraska Directory Services to access all state web applications requiring authentication and authorization.

2.0 Purpose and Objectives:

Implement (reduced) single sign on using role based authentication and authorization for electronic government (e-Government) to provide for a cost effective, efficient delivery of services, while maintaining necessary security and confidentiality of non-public information through an industry standard enterprise directory.

3.0 Definitions:

3.1 Authentication – The process of identifying an individual. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

3.2 Authorization – The process of giving individuals access to system objects based on their identity which allows them to add, update, delete or view information for a web application.

3.3 Web Applications – Applications that are accessed using a web browser. This definition includes custom developed systems and third party software systems.

4.0 Applicability

4.1 State Government Agencies

This standard applies to all state government agencies, commissions and boards, except Higher Education and those agencies receiving an exemption under Section 4.2.

4.1.1 State Agencies, Commissions, and Boards

All new web applications requiring authentication and authorization receiving state appropriations must comply with the standard listed in Section 1.0. All existing web applications requiring authentication and authorization must convert to the standard listed in Section 1.0 as soon as fiscally prudent or upon an upgrade to the web application, whichever comes first.

4.2 Exemption

Exemptions may be granted by the NITC upon request by an agency.

4.2.1 Exemption Process

Any agency may request an exemption from this standard by submitting a “Request for Exemption” to the NITC. Requests should state the reason for the exemption. Reasons for an exemption include, but are not limited to: statutory exclusion; federal government requirements; or financial hardship. Requests may be submitted to the Office of the CIO via e-mail (info@cio.state.ne.us) or letter (Office of the CIO, 521 S 14th Street, Suite 301, Lincoln, NE 68508). Requests will be considered by the NITC after review by the Technical Panel.

5.0 Responsibility

5.1 IMServices

IMServices will incorporate the needed hardware and software into their infrastructure to provide the following:

- LDAP directory for user /entity objects.
- Role-based authentication and authorization to the MyNebraska Portal and applicable applications for registered users.
- Business/disaster recovery.
- Authentication methods available:
    - User ID and password
    - Two-factor authentication
    - X.509 certificates

5.2 State Agencies, Boards and Commissions

Agencies, Commissions, and Boards will carry out the following responsibilities:

- Web applications requiring authentication and authorization must comply with the standard listed in Section 1.0.
- Require this standard be referenced in all RFPs (Requests for Purchase) for web applications covered by this standard.
- Require that commercial off-the-shelf software requiring authentication and authorization utilize the Nebraska Directory Services Web-based authentication standard.

5.3 State Government Council Directory Services Workgroup

The State Government Council's Directory Services Workgroup will provide ongoing advice and direction.

6.0 Related Policies, Standards and Guidelines

- NITC Information Security Management Policy – January 23, 2001
- NITC Access Control Policy – January 23, 2001
- NITC Network Security Policy – January 23, 2001
- State Government Council's Directory Services Workgroup Phase I recommendation – July 30, 2003