Division of Information Technology Services
Department of Administrative Services
State of Utah

June 20, 2002

State User Authentication Policy

Introduction: The State of Utah authentication policy provides guidelines and standards for any and all authentication into any network/system resource provided by the state.

Policy Objectives and Scope: The objective of this policy is to cover the standards by which the state can offer secure and individually unique user identification for access into state information resources. This policy is intended to cover standards of implementation and not specific implementation procedures or process.

Definitions:

Access
Opportunity to make use of an automated information system resource; The ability to have contact with a terminal from which a transaction may be initiated.

Authentication
Verifying the identity of a user who is logging onto a computer system or verifying the integrity of a transmitted message.

Authorization
The processes of determining what types of activities are permitted to a user. Usually, authorization is in the context of authentication. Once you have authenticated a user, they may be authorized different types of access or activity.

Logging
As with all network services the authentication service must be capable of logging a minimum of user identity, time and date of access (or attempt), logoff, and activities attempting to bypass authentication.

Replication of Data
It is important that the UMD provide for replication of data, redundancy, and/or replication of data to prevent any denial of service based on downtime.

Utah Master Directory (UMD)
The UMD will be the authoritative source of unique identifiers for all employees. There may be replicas of information throughout the State of Utah networks, but the UMD will encompass all information found on a given replica.

Security Requirements: ***Authentication Server Access***
Access to authentication servers should be limited to state managed resources, and the users of those resources.

Access mechanisms (such as SiteMinder and/or NDS) must access the authentication repository over a trusted network. If access must be provided in an un-trusted environment, the data must be encrypted with 128 bit encryption or better.

Authentication services must be capable of enhanced authentication methods including (but not limited to) biometrics, smart cards, tokens, digital signatures, etc.

Abstract Programming Interfaces (API's) and Plug-ins: Some applications will need authentication mechanisms to control access. For this purpose the state will provide access to the

authentication server via abstract programming interfaces and or application plug-ins. When implementing either of these with the intention of accessing the data repository, the data must either pass over a trusted state network, or and encryption tunnel using 128 bit or better encryption.

Contingency Planning: Technical staff working on UMD servers must prepare and obtain ITS concurrence for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, and power outage. These contingency plans must be kept up-to-date to reflect changes in the State of Utah computing environment. These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable computing environment.

Change Control: All changes to State of Utah authentication servers, including configuration changes as well as software upgrades and patches, must have an ITS approved implementation plan.

Physical Security: All State of Utah authentication servers must be physically secured from unauthorized individuals. This security should include verification of any physical access by individually unique authorization mechanisms (such as id cards, magnetic card key entry, etc.).

References:

Interim Date: Pending
Organization Sponsoring the Standard: ITS**,** State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: 6/27/02 for comment
Author(s): John Malouf, Rick Gee (ITS)
Related Documents: State Firewall Standard, State Information Security Policy, State Network Access Policy, HIPAA and Related Security Requirements Summary (Working Draft), UMD Design Document.