State of New Mexico Statewide
Architectural Configuration Requirement
Title: Authentication and Directory Services Standard
S-STD001.002
Effective Date: October 18, 2005

1. Authority

The Department of Information Technology (DoIT) in coordination with the Information Technology Commission, shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act, NMSA, 9-27-1 et. seq. (1978).

2. Purpose

The purpose of this standard is to coordinate Agency and State implementations associated with the identification and verification of information systems users who access resources or services through agency and State systems. Identification and verification provide the foundation for many other information security systems and services in the State.

3. Scope

This applies to all Executive Agencies and to any other Agency or Entity utilizing Executive Agency infrastructure.

The Department Secretary or Agency Director, working in conjunction with the Department or Agency Chief Information Officer or IT Lead, shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures within each agency.

4. Standard

Identification, authentication, and directory services are crucial for proper authorization to applications and systems, non-repudiation, and auditing capabilities for agencies. Without authentication, agencies have no assurance that access to resources and services is properly controlled and monitored.

To safeguard critical systems, applications, information and networks from unauthorized access or intrusion, agencies shall ensure identity and authentication of a user/customer before granting access to resources and services by implementing one or more of the following authentication methods:

- ***Authentication by Knowledge*** – Based on information only the user knows;
- ***Authentication by Ownership*** – Based on something only the user possesses;
- ***Authentication by Characteristic*** – Based on a user's physical characteristic.

External connections to networks, in accordance with existing rules, guidelines, and architectural configuration requirements, shall be routed through secure gateways, encrypted, and require strong authentication, such as challenge/response devices, one- time passwords, tokens, Kerberos, and smart cards, as well as the standard method of authentication required by the agency for internal connectivity (commonly referred to as multifactor authentication.)

Agency authentication methods shall be documented and maintained as part of, and in accordance with, existing rules, guidelines, and architectural configuration requirements.

4.1. ACCESS TO RESOURCES AND SERVICES – shall be in accordance with existing rules, guidelines, and architectural configuration requirements including Physical Security, Personnel Security, and Account Management requirements. Internal and external connectivity to networks to provide access to resources and services shall be in accordance with existing rules, guidelines, and architectural configuration requirements including Network Security requirements.

4.2. DIRECTORY SERVICES – The preferred method is Lightweight Directory Access Protocol (LDAP) to provide access to directory and new application services.

Future meta-directory services should be established with individual LDAP directory repositories and be accessible via standard LDAP protocols. Meta-directory service design should include obtaining an Object Identifier (OID) tree for the State from the Internet Assigned Numbers Authority (IANA) that can be used to uniquely identify attributes and object classes to facilitate the matching and coordination of information among individual LDAP implementations.

4.3. AUTHENTICATION BY KNOWLEDGE - User authentication shall be based on the presence of a userID associated with something only the user/customer knows and shall include the following:

4.3.1. Password – A secret series of characters that, by association with a userID, enables a user to access information, systems, applications, or networks. Agencies shall establish, implement, document, and communicate (in accordance with existing rules, guidelines, and architectural configuration requirements including Security Training and Awareness requirements and criteria with Password Policy requirements.)

4.3.2. Personal Identification Number (PIN) - A character string used as a password to gain access to a system resource. PINs shall only be entered using a keypad and usually not sent across the network, to prevent interception. PINs may be used in conjunction with other types of authentication devices (i.e., a smart card).

4.4 AUTHENTICATION BY OWNERSHIP – User authentication shall be based on something only the user possesses, making it more secure than a knowledge-based system, and may include the following:

4.4.1 Hardware Based Challenge-Response – The server challenges the user to demonstrate that he/she possesses a specific token and knows the PIN or pass phrase by combining them to generate a response that is valid, but only once. Some examples may be:

- A small, handheld device, with or without a key pad, containing an LCD window or display interface – the device acts as the user's token.
- A smart card. An ISO 7816-compliant chip card with CPU and memory. Contact smart cards require PC/SC standard readers, based on ISO 7816, and supporting workstation software. Contactless smart cards require a Mifare architecture card reader based on ISO Standard 14443A.
- A Universal Serial Bus (USB) key. A device with CPU memory that plugs into a universal serial bus port on a workstation.
- A Bluetooth-enabled token with CPU and memory. Bluetooth is a short-range, 2.45GHz wireless connection protocol.

4.4.2 Third party authentication such as *Verisign* certificates.

4.5 AUTHENTICATION BY CHARACTERISTIC – User authentication based on information about a person gathered by digitizing measurements of a physiological or behavioral characteristic has been categorized as an emerging technology. When used, implementations shall be based on open, industry standards, if available. Requirements may be issued for the following areas once the technology matures to the point of becoming strategic for the State:

4.5.1 Physiological characteristic such as:

- Fingerprint – any fingerprint imaging used shall conform to current
- NIST Fingerprint Imaging Bureau standards.
- Iris patterns.
- Retina patterns.
- Hand geometry.
- Face geometry.
- Palm print.

4.5.2 Behavioral characteristics such as:

- Voiceprint (speech patterns).
- Signature.
- Keystroke dynamics.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

6. References

NIST National Institute of Standards and Technology

7. Attachments

None

8. Version Control

S-TD-001.002

9. Revision History

Original 10/18/05
Format Updated 09/18/13