

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

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 private 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 budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.
A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology PSPs 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 State agencies. Without authentication, State 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 the user/customer community 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.

- 4.1. *Directory Services* - Lightweight Directory Access Protocol (LDAP) shall be used to provide access to directory and application services.
- As a widely accepted, industry standard for access to directory information, LDAP supports multi-vendor interoperability by providing an open, extensible, vendor-independent, platform-independent, protocol standard.
 - LDAP directories provide repositories for security-related data (e.g., userIDs, passwords, URLs, pointers, binary data, Public Key Certificates, etc.).
 - LDAP protocol directly supports various forms of strong security technology used to perform authentication, privacy, and data integrity services.
 - The LDAP Version 3 proposal for Transport Layer Security (TLS) includes data encryption methods.
 - 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.
- 4.2. *Authentication by Knowledge* - User authentication shall be based on the presence of a userID associated with something only the user/customer knows and may include the following:
- 4.2.1. 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 and implement criteria governing the following:
- Number of unsuccessful login attempts allowed,
 - Procedures for revoking and resetting passwords,
 - Minimum password length and format,
 - Maximum validity periods for passwords, and
 - Password re-use limitations.
- Use of passwords shall conform to the following requirements:
- a. Passwords shall be for individual users/customers in order to maintain accountability. Generic, multi-user IDs should be eliminated;
 - b. Passwords shall be kept confidential;
 - c. Passwords shall not be kept on paper or stored in plain text format;
 - d. Passwords shall be changed whenever there is a chance that the password or the system has been compromised;
 - e. Passwords shall be changed periodically and not recycled;
 - f. Passwords shall not be included in a macro or function key to automate log-in processes;

- d. A Bluetooth-enabled token with CPU and memory. Bluetooth is a shortrange, 2.45GHz wireless connection protocol;
- 4.3.2 Symmetric-Key Cryptography - A cryptographic system in which the sender and receiver of a message share a single, common key used to encrypt and decrypt the message. (Please refer to S850 – Encryption Technologies.)
- 4.3.3 Asymmetric-Key Cryptography - A cryptographic system that uses two keys, a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message. (Please refer to S850 – Encryption Technologies.)
- 4.4 ***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 must 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:
 - 4.4.1 Physiological Characteristic such as:
 - a. Fingerprint – any fingerprint imaging used shall conform to current Department of Public Safety (DPS) Fingerprint Imaging Bureau standards.
 - b. Iris patterns
 - c. Retina patterns
 - d. Hand geometry
 - e. Face geometry
 - f. Palm print
 - 4.4.2 Behavioral Characteristics such as:
 - a. Voiceprint (speech patterns)
 - b. Signature
 - c. Keystroke dynamics

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms for definitions and abbreviations.

6. REFERENCES

6.1. Developmental

- 6.1.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 6.1.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 6.1.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 6.1.4. A. R. S. § 41-1461, “Definitions.”
- 6.1.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 6.1.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 6.1.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 6.1.8. A. R. S. § 41-3501, “Definitions.”
- 6.1.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 6.1.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 6.1.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 6.1.12. Arizona Administrative Code, Title 2, Chapter 7.
- 6.1.13. Arizona Administrative Code, Title 2, Chapter 10.
- 6.1.14. Arizona Administrative Code, Title 2, Chapter 18.
- 6.1.15. Statewide Information Technology Policy P100.
- 6.1.16. Statewide IT Security Policy P800
- 6.1.17. Encryption Technologies Standard P800-S850
- 6.1.18. State of Arizona Target Security Architecture,
http://gita.state.az.us/enterprise_architecture.

7. ATTACHMENTS

None