Enterprise Technology Strategy and Services Policy 10-20
Identification and Authentication (IA)  
Brian Tardiff, CISO
Last Revision: 8/31/2020
doa.entsec@doit.ri.gov

1. Purpose

Establish policy for identifying and authenticating user access to information systems and network resources that ensures user access is authorized, confidential and sensitive data is protected, and accountability is maintained.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments1 (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

**Authentication**
Establishing the validity of the user’s claimed identity using one of the following techniques: something the user knows (e.g. password), something the user has (e.g. key card), or something the user is (e.g. biometric fingerprint). Authenticators include, for example, passwords, key cards, PKI certificates, and biometric fingerprints.

**Federal Identity, Credential, and Access Management (FICAM)**
A common set of identity, credential, and access management standards, best practices, and implementation guidance for federal agencies. State of Rhode Island information systems are required to adhere to the FICAM architecture.

**Identification**
Providing the users claimed identity to the information system, most commonly via a user ID. System processes and devices may also have an identity. An identifier is required to assign responsibility and accountability for user actions on the system.

---

1 State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
Multifactor Authentication (MFA)
Establishing the validity of the user’s claimed identity using at least two of the following techniques: something the user knows (e.g. password), something the user has (e.g. key card), or something the user is (e.g. biometric fingerprint).

Personal Identity Verification (PIV)
Credentials which conform to FIPS Publication 201 and supporting documentation that are used to access controlled facilities and information systems at the appropriate security level.

4. Procedures for Compliance

<table>
<thead>
<tr>
<th>Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Risk Systems (IAL1)</strong> Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.</td>
</tr>
<tr>
<td><strong>Moderate Risk Systems (IAL2)</strong> Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.</td>
</tr>
</tbody>
</table>

4.1. [IAL1, IAL2] Identification and Authentication Policy and Procedures (IA-1). The agency will develop, document, disseminate, review, and annually update an identification and authentication policy and procedures.

4.2. [IAL1, IAL2] Identification and Authentication – Agency Users (IA-2). The information system will uniquely identify and authenticate system users or processes acting on behalf of system users. Agency system users will reauthenticate to the information system to release a session lock, when the role or the authenticator changes, or when system or data security requirements require it (e.g. change in data classification, execution of privileged functions).

4.2.1. [IAL1, IAL2] Network Access to Privileged Accounts (IA-2.1). The information system will implement MFA for network access to privileged accounts.
4.2.2. [IAL2] Network Access to Non-Privileged Accounts (IA-2.2). The information system will implement MFA for network access to non-privileged accounts.

4.2.3. [IAL2] Local Access to Privileged Accounts (IA-2.3). The information system will implement MFA for local access to privileged accounts.

4.2.4. [IAL2] Network Access to Privileged Accounts – Replay Resistant (IA-2.8). The information system will implement replay-resistant authentication mechanisms for privileged account access to the network. A replay attack is a type of man-in-the-middle attack that allows an attacker to duplicate a previous valid data transmission and allow unauthorized access to the information system. Information systems should validate user credentials between authenticating clients and application servers for each session to reduce the risk of replay attacks. Replay-resistant techniques include nonce’s (one-time use numbers), challenges (e.g. TLS, Web Services Security), PKI certificates, and other one-time authenticators (e.g. time-synchronous, challenge-response).

4.2.5. [IAL2] Remote Access – Separate Device (IA-2.11). The information system will implement MFA for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device that is separate from the system gaining access to reduce the likelihood of compromising authentication credentials stored on the system.

4.2.6. [IAL1, IAL2] Acceptance of PIV Credentials (IA-2.12). The information system will accept and electronically verify PIV credentials.

4.3. [IAL1, IAL2] Device Identification and Authentication – Agency Users (IA-3). The information system will uniquely identify and authenticate device-to-device connections via a method (e.g. MAC address, TCP/IP address, Radius, Kerberos, TLS, EAP) that is appropriate for the connected devices and required authentication mechanism strength for the security category of the information system.

4.4. [IAL1, IAL2] Identifier Management (IA-4). The agency will receive authorization from designated personnel prior to assigning an identifier to an individual, group, role, or device and will not reuse or reassign the identifier to another individual, group, role, or device. The information system will automatically disable identifiers after no more than 90 days of inactivity.

4.5. [IAL1, IAL2] Authenticator Management (IA-5). The agency will manage information system authenticators in accordance with the following:
• Verify the identity of the individual, group, role, or device receiving the authenticator.
• Establish initial authenticator content for authenticators defined by the agency.
• Ensure authenticators have sufficient strength of mechanism for their intended use.
• Establish procedures for (i) initial authenticator distribution, (ii) lost, compromised, or damaged authenticators, and (iii) revoking authenticators.
• Change default content of authenticators prior to information system installation.
• Establish authenticator lifetime restrictions and reuse conditions.
• Periodically change or refresh authenticators.
• Protect authenticators from unauthorized disclosure and modification.
• Require individuals take specific security safeguards to protect authenticators.
• Change authenticators for group/role accounts upon a change in membership.

4.5.1. [IAL1, IAL2] Password-Based Authentication (IA-5.1). See ETSS Enterprise Password Security Policy 10-01 for information regarding password length, complexity, strength, security, and change, re-use, and enforcement requirements.

4.5.2. [IAL2] PKI-Party-Based Authentication (IA-5.2). For PKI-based authentication, the information system will (i) validate certifications by constructing and verifying the certification path to an accepted trust anchor, including verifying certificate status information (e.g., certificate revocation list, certificate status protocol response), (ii) enforce authorized access to the corresponding private key, (iii) map the authenticated identity to the account of the individual or group, and (iv) implement a local cache of revocation data to support path discovery and validation (to reduce risk in the event the information system is not able to access revocation data via the network).

4.5.3. [IAL2] In-Person/Trusted Third-Party Registration (IA-5.3). The agency will require that the registration process to receive employee ID badges that grant physical access to state facilities and physical authentication tokens that grant access to enterprise information systems be conducted in person with DCAMM or Enterprise Security Team, as appropriate, with authorization from the agency technical support manager (TSM).

4.5.4. [IAL1, IAL2] Hardware Token-Party-Based Authentication (IA-5.11). For hardware token-based authentication, the information system will employ encryption mechanisms that comply with ETSS Data Encryption Policy 05-03.

4.6. [IAL1, IAL2] Authenticator Feedback (IA-6). The information system will obscure authenticator information during the authentication process and does not provide information that would allow the authentication mechanism to be compromised. The information system will obscure passwords with symbols, such as asterisks, when entered on screen. To reduce the risk of passwords being compromised from shoulder surfing, system users should ensure there is no individual behind them prior to entering their password.

4.7. [IAL1, IAL2] Cryptographic Module Authentication (IA-7). The information system will implement a mechanism for authentication to a cryptographic module that meets the requirements of applicable mandates and guidance for such authentication. Sensitive information will only be protected by modules tested and validated by NIST to meet FIPS 140-2 standards (see list of validated cryptographic modules at http://csrc.nist.gov/).
4.8. [IAL1, IAL2] Identification and Authentication – Non-Agency Users (IA-8). The information system will uniquely identify and authenticate non-agency system users or processes acting on behalf of non-agency system users. Non-agency system users will reauthenticate to the information system to release a session lock, when the role or the authenticator changes, or when system or data security requirements require it.

4.8.1. [IAL1, IAL2] Acceptance of PIV Credentials from Other Agencies (IA-8.1). The information system will accept and electronically verify PIV credentials from other agencies.

4.8.2. [IAL1, IAL2] Acceptance of Third-Party Credentials (IA-8.2). For information systems that are accessible by the public (e.g. public-facing websites), the information system will only accept FICAM-approved third-party credentials.

4.8.3. [IAL1, IAL2] Use of FICAM-Approved Products (IA-8.3). For information systems that are accessible by the public (e.g. public-facing websites), the agency will employ only FICAM-approved information system components within mission critical information systems.

4.8.4. [IAL1, IAL2] Use of FICAM-Issued Profiles (IA-8.4). The information system will conform to FICAM-issued profiles of approved protocols (e.g. SAML, OpenID).

5. Approval / Review Signature:

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2020.09.14 12:11:20 -04'00'

Chief Information Security Officer