

Public Key Infrastructure (PKI) Standard



STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup – Public Key Infrastructure Standard

1. Purpose

To further increase the overall security posture of the State of Montana, several agencies agreed to collaborate on a strategic goal of increasing security through efforts associated with data encryption. A subgroup of the MT-ISAC Best Practices and Tools workgroups met during 2017 to review relevant policies and guidance associated with encryption and develop a standard technique on how to best meet those policies. The technique chosen is a technology currently implemented by the State of Montana known as Public Key Infrastructure (PKI) certificates.

The use of PKI certificates provides the capability to enable services such as: encrypting email, encrypting web connections, and encrypting individual files.

In addition to encryption, PKI certificates may also be used in identification and authentication services such as: digitally signing email, digitally signing documents, device to device login, and human to device login.

The current standard for handling State employee accounts is Microsoft Active Directory which also provides for a Certificate Authority capable of issuing PKI certificates to every employee and device listed in the State's Active Directory.

The goal for State of Montana Certificate Authority is to issue PKI certificates to every employee listed in the State Active Directory to an Assurance Level capable of positively identifying employees and securely handling data up to State of Montana Level 3 classification.

The vision for State of Montana PKI Certificate Authority is to reach an Assurance Level capable of being ~~for~~ cross-certified with the Federal Bridge Certificate Authority (FBCA). Cross certification with the FBCA will provide the ability for the State of Montana to positively identify employees and securely exchange information with federal agency counterparts using an established PKI certificate standard (X.509).

2. Policy

Encryption strategy applies to the following policies found within the Montana Operations Manual.

a. Internet Privacy and Security Policy

- Transaction Information

- The state uses secured servers for conducting online transactions. All credit card and other payment information that is transmitted is protected by

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup – Public Key Infrastructure Standard

encryption technology, provided the website user's browser is properly configured and the user's computer is operating properly.

b. Enterprise Mobile Device Management Policy

- All Fully Managed (Fully Enrolled) mobile devices that access State of Montana data protected by federal or state regulation must enable encryption on all storage directly associated with the mobile device including Secure Digital (SD) cards and flash drives. Because encryption enforcement is limited with BYOD enrolled services, agencies will be responsible for configuring the MDM solution to limit BYOD devices from storing data on unencrypted storage.

c. Information Security Policy

- 2. Protect
 - 2.1 Manage identities and credentials for authorized devices and users that
 - 2.1.5 Requires the following of identifiers:
 - 2.1.5.4 Password encryption during both storage and transmission;
 - 2.1.6 Requires that certificates are validated and map the identity;
 - 2.1.7 Requires that hardware token-based authentication employs mechanisms that satisfy Public Key Infrastructure (PKI) requirements;
 - 2.5 Manage Remote Access that
 - 2.5.5 Utilizes encryption
 - 2.20 Protect communication and control networks by:
 - 2.20.2 Maintaining usage restrictions, configuration requirements, and implementation guidance for wireless access that:
 - 2.20.3 Encrypts wireless access

d. Information Security Policy – Appendix A

- AC-17 Remote Access
 - Remote access is monitored and uses encryption for all access sessions. All remote access is routed through state designated control points (e.g., Helena & Billings). Privileged commands are authorized only for system administrators.
- AC-18 Wireless Access
 - Wireless access is protected by authentication of users and devices and uses NIST standard encryption for authentication and communication.
- IA-5 Authenticator Management
 - Encryption of passwords in storage and transmission
- IA-7 Cryptographic Module Authentication
 - The standard for data encryption is the Advanced Encryption Standard 256bit or higher (AES 256-bit).
- MP-4 Media Storage
 - Sensitive Data shall:
 - a. Be encrypted on portable devices and portable storage

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup – Public Key Infrastructure Standard

- MP-5 Media Transport
 - Sensitive Data shall: Not be transmitted via non-State-owned networks unless approved transmission protocols and encryption techniques are utilized.
 - Each agency shall:
 - Confer with departmental technical support or the State CIO for specific technology selections and implementation procedures for encryption of data.
- SC-7 Boundary Protection
 - SITSD may implement additional security measures as needed using software and/or hardware configurations for protecting the state network or ensuring secure communications. These may include encryption or filters restricting certain types of network traffic. All wireless connections to the inside (protected) portion of the network (inside) will be encrypted and authenticated. Unauthorized connections to the state network will not be permitted. Connections creating routing patterns that flood the network with unnecessary traffic are not allowed.
 - Agencies will cooperate to make shared sites secure and may incorporate encryption into data transmission between sites on the wide area network (WAN).
- SC-17 Public Key Infrastructure Certificates
 - The State of Montana issues public key certificates under a certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

3. Standards for State of Montana Public Key Infrastructure (PKI)

- a. The State Information Technology Services Bureau shall:
 - Establish and administer a Certificate Authority (CA) for the State of Montana that can issue certificates to all State of Montana Active Directory users.
 - Manage PKI certificates to the Assurance Level necessary to handle State of Montana Level 3 data classification.
 - Implement an end user PKI certificate registration/renewal Web Interface
 - Enterprise Key Management within the CA capable of recovering PKI certificates for all end users of the CA. Key recovery shall be limited to trusted roles following a two-person integrity rule for additional access control.
- b. Each State Agency:
 - May establish one or more Trusted Agent roles for issuing PKI certificates to their end users based on positive identification of the end user.

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup – Public Key Infrastructure Standard

- Each Trusted Agent must be approved by the State of Montana Chief Information Security Officer (CISO) through a program administered by the Enterprise Security Program.
- May request the assistance of another State of Montana authorized Trusted Agent for vetting end users.
- c. Every State Employee that has an Active Directory account shall:
 - Be vetted by a Trusted Agent prior to being issued a PKI certificate.
 - Be issued a PKI certificate to, at a minimum, digitally sign all email sent by that employee by default.
 - Be issued a PKI certificate to encrypt email sent to other State employees that is required to be encrypted by policy or law.
 - Use their individual PKI certificates, in accordance with organizational policy, to digitally sign email sent for official business to external entities that will trust the State of Montana Certificate Authority.
 - Use their individual PKI certificates, in accordance with organizational policy, to encrypt email sent for official business to external entities that will trust the State of Montana Certificate Authority.
 - Use their individual PKI certificates, in accordance with organizational policy, to encrypt individual files using authorized tools.
 - Use their individual PKI certificates, in accordance with organizational policy, to digitally sign electronic documents that accept PKI certificates.
- d. The CISO Enterprise Security Program shall
 - Administer a Trusted Agent program for the State of Montana.
 - Partner with each agency to facilitate an appropriate level of registration and training for all State employees serving in the following roles:
 - CA Administrator
 - Trusted Agent
 - End user
 - Partner with each agency to facilitate an appropriate level of awareness for the following PKI capabilities
 - a. Email encryption
 - b. Email digital signature
 - c. Electronic document signing
 - d. Local file encryption
 - Develop and maintain a Certificate Policy document based on National Institute of Standards Interagency Report 7924
 - Develop and maintain a Certificate Practices Statement document based on the Internet Engineering Task Force Public Key Infrastructure X.509 Certification Practices Framework.

STATE OF MONTANA

Montana Information Security Advisory Council

Best Practices Workgroup – Public Key Infrastructure Standard

4. Compliance

Compliance shall be evidenced by implementing the best practices standards above as well as adhering to the use of PKI certificates as described in the State of Montana Certificate Policy and the associated State of Montana Certification Practices Statement. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this Public Key Infrastructure Standard are made by submitting an [Action Request form](#). Requests for exceptions are made by submitting an [Exception Request form](#). Changes to policies and standards will be prioritized and acted upon based on impact and need.