State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0530: Public Key Infrastructure and Certificates

Revised: February 10, 2025

1.0 PURPOSE

This policy establishes public key infrastructure (PKI) guidelines for the practices of issuing public key certificates and/or obtaining public key certificates under an appropriate certificate authority (CA).

2.0 SCOPE

This policy applies to all WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) bureaus and offices, contractors, business associates, and vendors, who must comply with applicable federal requirements, as well as Executive Branch policies, as appropriate.

3.0 POLICY

3.1 All connectivity by the Office of Management Information Services (OMIS) to the Centers for Medicare and Medicaid Services (CMS) Federal Data Services Hub (FDSH) will be protected with Secure Hash Algorithm, standard cryptographic hash function encryption for all certificates. This requirement applies to all formal production and test environments.

3.2 Any requests to provide evidence of updated certificates for compliance will be provided upon request.

3.3 Should other regulatory agencies require a lesser or stronger certification the stronger encryption will be applied.

3.4 All private keys will be securely stored and maintained in an auditable database of private key histories for recovery purposes.

3.4.1 A credential must be maintained over its lifecycle. This may include revocation, re-issuance/replacement, re-enrollment, expiration, personal identification number (PIN) reset, suspension, or re-instatement.

3.4.2 If a new certificate or public/private key pair is issued, those along with the existing and previously escrowed certificates and keys will be stored for recovery.

3.4.2.1 Any requests for key recovery must be submitted in writing to the OMIS Information Security Officer (ISO). The ISO will work with the West Virginia Office of Technology (WVOT), as necessary.

3.4.2.2 If denied at this level, the requestor must begin the process of applying for a new certificate or public/private key pair.

3.4.2.3 If approved, the request must be finalized by the OMIS ISO and forwarded to the Key Recovery Agent at the issuing Certificate Authority.

3.4.2.4 These transactions for request, whether approved or denied, will be recorded along with key histories for recovery purposes.

3.5 OMIS will leverage certificate authentication to verify the identity of a user or third-party. This will include the following:

3.5.1 Obtaining confirmation that the certificate includes an Object Identifier (OID) indicating which policy was followed. This will establish:

3.5.1.1 Identity proofing;

3.5.1.2 Cryptographic strength; and

3.5.1.3 Whether tokens or smart cards are used.

3.5.2 Evaluating the OID of each certificate to determine its trustworthiness for a given application, such as PIV-reliant.

3.5.2.1 Determine if the cross-certificate was issued by a Federal PKI Management Authority.

3.5.2.2 Determine which standard policies should be considered valid for the issuer.

3.5.3 Reviewing certificate revocation lists (CRL), published or otherwise, made available by the issuing certificate authority to verify trusted certificates.

4.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

5.0 DEFINITIONS

5.1 **Authentication –** the process of verifying the identity of a user.

5.2 **Certificate Authentication** – a process that provides assurance of the source and integrity of the certificate.

5.3 Certificate Authority (CA) – the entity that issues certificates to subjects.

5.4 Certificate Revocation Lists (CRLs) – A CRL is a list that is published by the CA at defined intervals and contains certificates that have not yet expired, but which are identified as invalid (revoked). Certificates may be revoked for a number of reasons, including a change in the information contained in the certificate or a suspected compromise of the private key associated with the public key in the certificate.

5.5 Digital Certificates – a type of credential in digital format that proves the authenticity of an identity claim by an individual system or object.

5.6 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the DH, DHF, DoHS and the OSA to be subject to this policy. This definition does not create any additional rights or duties.

5.7 Federal Data Services Hub - The CMS federally managed service to transmit data between federal and state Administering Entities and to interface with federal agency partners and data sources.

5.8 Office of Management Information Services (OMIS) - This office reports directly to the DH, DHF, and DoHS Cabinet Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the Departments.

5.9 Privacy Officer – The official responsible for facilitating the Executive Branch's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.

5.10 Private Key - A tiny bit of code paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format. Public and private keys are paired for secure communication, such as email.

5.11 Public Key Infrastructure (PKI) – a framework that is established to issue, maintain and revoke public key certificates.

5.12 Self-signed Certificates – a public key certificate whose digital signature may be verified by the public key contained within the certificate. The signature on a self-signed certificate protects the integrity of the data but does not guarantee the authenticity of the information. The trust of self-signed certificates is based on the secure procedures used to distribute them.

5.13 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.* The WVOT is responsible for establishing technology policy, creating and supporting technology infrastructure (including the provision of training), evaluating equipment and services, and reviewing information technology contracts.

6.0 REFERENCES/RELATED MATERIAL

6.1 FICAM Roadmap and Implementation Guidance, v2, December 2011

6.2 NIST SP 800-57, Recommendation for Key Management – Part 1: General (Revision 5), May 2020

6.3 FIPS PUB 180-4, Secure Hash Standard (SHS), August 2015

6.4 IRS Publication 1075

6.5 CMS - HHS Policy for Encryption of Computing Devices and Information - December 9, 2022

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	05/11/2021	Approved
Version 1.1	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Overall review of content - Revised language throughout
Version 1.2	02/07/2023	Annual Review; checked links for accuracy

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0530: Public Key Infrastructure and Certificates

Revised: February 10, 2025

Version 1.3	02/14/2024	Annual Update - changed “DHHR” to “Departments of Health, Health Facilities, Human Services, and Office of Shared Administration”, updated links, overall review of content, revised language throughout
Version 1.4	02/10/2025	Annual Review