OhioDAS Service · Support · Solutions | Office of Information Technology

State of Ohio IT Standard

Standard Number: ITS-SEC-01	Title: Data Encryption and Cryptography
Effective Date: 07/25/2007	**Issued By:** R. Steve Edmonson, Director, State Chief Information Officer
Version Identifier: 1.0	**Published By:** Investment and Governance Division, Ohio Office of Information Technology

1.0 Purpose

This state IT standard defines the minimum requirements for ***cryptographic algorithms*** that are ***cryptographically strong*** and are used in ***security services*** that protect at-risk or sensitive data as defined and required by agency or state bulletin, policy or rule. This standard does not classify data elements; does not define the security schemes and mechanisms for devices such as tape backup systems, storage systems, mobile computers or removable media; and does not identify or approve secure transmission protocols that may be used to implement security requirements.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this state IT standard is applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.

3.0 Background

Protecting sensitive data is a responsibility shared within and across state agencies. The unauthorized disclosure of at-risk or sensitive data and personal identifying information as a result of security breaches, such as the loss of portable devices and media or the malicious theft of electronic data, is a serious liability to the state. These events can diminish the confidentiality, integrity, and availability of the state's information, compromising public trust and the state's ability to deliver services to citizens.

Provisioning services to citizens is happening in an ever increasingly complex manner. The information systems span secure and insecure physical environments and can

Office of the State CIO | 30 E. Broad Street, 39th Floor | Columbus, Ohio 43215
614.644.6446 | 614.644.9382 | State.CIO@oit.ohio.gov

Robert Blair, Director
Stuart R. Davis, Assistant Director/
State Chief Information Officer

encompass both trusted and untrusted networks. Policy measures such as requiring certain password strength or limiting uses, physical measures such as key-card doors and concealed wires, and legal measures such as prohibiting theft and eavesdropping by statute, only provide a limited degree of defense against today's threats. Modern cryptographic methods, based on mathematics and independent verification, are often necessary to increase security assurance and protect data that is considered sensitive, has a high value, or is vulnerable to unauthorized disclosure or modification when stored or during transmission over a network.

The National Institute for Science and Technology (***NIST***) conducts extensive research and development in cryptography techniques. Their publications include technical standards for data encryption, digital signature and message authentication as well as guidelines for implementing information security and managing cryptographic keys. These standards and guidelines have been mandated for use in federal agencies and adopted by state governments and private enterprises. Industry has responded by developing security products that have been officially validated to meet the rigorous requirements of NIST.

This state IT standard adopts a subset of the NIST standards and guidelines for implementing cryptographically strong information security for the State of Ohio. These cryptography methods are currently deployed by state agencies, generally accepted and significantly in use in other states as well as the private sector, and have been rigorously proven to be technically sound.

4.0 Standard

A security service conforming to this state IT standard embeds validated ***cryptographic modules*** (see section 4.1) and uses approved cryptographic algorithms (see section 4.2) in its implementation. Furthermore, the description of the cryptographic implementation shall be kept confidential (see section 4.3). Any use of cryptographic modules for electronic signatures must also comply with rule 123:3-1-01 of the Ohio Administrative Code.

4.1 Approved Cryptographic Modules

4.1.1 Validated Cryptographic Modules

Cryptographic modules embedded in security services validated under the Cryptographic Module Validation Program (***CMVP***) in accordance with NIST FIPS Publication 140-2 are approved for use by this standard. Cryptographic module validation must be evidenced by a NIST-issued certificate number.

4.1.2 Pre-Validation List of Cryptographic Modules

Cryptographic modules that are on the ***CMVP Pre-validation List*** (see Related Resources) are approved for use by this standard, except such deployment may be further limited or prohibited by agency or state bulletin, policy or rule. Submission for testing is not a guarantee of eventual validation and, consequently, may pose a security risk. Agencies should be deliberate in determining whether their use of an un-validated cryptographic module is appropriate. If a cryptographic module in use as allowed by this section is subsequently removed from the pre-validation list without a certificate, continued use of the cryptographic module must cease immediately.

4.2 Approved Cryptographic Algorithms

The specification of a cryptographically strong algorithm includes the name of the algorithm, a reference to its formal description, and the ***security strength*** that must be used with the algorithm to achieve a specified ***security lifetime***.

4.2.1 Symmetric Key Ciphers for Data Encryption

Cryptographic modules that use a ***symmetric key cipher*** (sometimes referred to as private key encryption) employing a shared secret key must adhere to the specifications in Table 4-1.

Table 4-1. Symmetric Key Cipher Specifications
Version 1.0 - Approved 07/25/2007

Name	Description and Reference Document	security strength to achieve specified security lifetime (minimum key length in bits)		
		through year 2010	through year 2030	beyond year 2030
AES	Advanced Encryption Standard block cipher based on the "Rijndael" algorithm NIST FIPS PUB 197 "Advanced Encryption Standard (AES)," November 2001.	128-bit keys	128-bit keys	128-bit keys
TDES	Triple Data Encryption Standard (or Triple DES) block cipher NIST SP 800-67 "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," May 2004.	three unique 56-bit keys	three unique 56-bit keys	**CANNOT BE USED**

NOTES:
1. AES implemented with 192-bit and 256-bit keys exceeds the security strength for all security lifetimes specified in this table.

4.2.2 Asymmetric Key Ciphers for Digital Signatures

Cryptographic modules that use ***asymmetric key ciphers*** (also known as public key encryption) that employ a pair of cryptographic keys consisting of one public key and one private key must adhere to the specifications in Table 4-2.

Table 4-2. Asymmetric Key Cipher Specifications
Version 1.0 - Approved 07/25/2007

Name	Description and Reference Document	security strength to achieve specified security lifetime (minimum key length in bits)		
		through year 2010	through year 2030	beyond year 2030
RSA	"Rivest-Shamir-Aldeman" algorithm for public-key cryptography RSA Laboratories, "PKCS#1 v2.1: RSA Cryptography Standard," June 2002.	1024-bit keys	2048-bit keys	3072-bit keys
DSA	Digital Signature Algorithm NIST FIPS PUB 186-2 "Digital Signature Standard (DSS)," with Change Notice 1, October 2001.	1024-bit keys	2048-bit keys	3072-bit keys
ECDSA	Elliptic Curve Digital Signature Algorithm NIST FIPS PUB 186-2 "Digital Signature Standard (DSS)," with Change Notice 1, October 2001.	160-bit keys	224-bit keys	256-bit keys

NOTES:
1. Only "RSA Signature Scheme with Appendix – Public Key Cryptography Standards #1, version 1.5 (PKCS1-v1-5)" and "RSA Signature Scheme with Appendix – Probabilistic Signature Scheme (PSS)" of the RSA Cryptography Standard are approved for use by this standard.

4.2.3 Message Authentication

Message authentication code (MAC) algorithms are used to provide security services for data authentication and integrity. They are used to establish the origin of information in a two-way exchange and support determining that information was not changed after it was transmitted. MAC algorithms must adhere to the specifications in Table 4-3.

Table 4-3. MAC Algorithm Specifications
Version 1.0 - Approved 07/25/2007

Name	Description and Reference Document	security strength to achieve specified security lifetime (minimum key length in bits or hash size)		
		through year 2010	through year 2030	beyond year 2030
CCM-AES	Counter with Cipher Block Chaining-Message Authentication Code (CCM) using AES symmetric key block cipher NIST SP 800-38C "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality," May 2004.	AES with 128-bit keys	AES with 128-bit keys	AES with 128-bit keys
CMAC-AES	Cipher-based MAC (CMAC) using AES symmetric key block cipher NIST SP 800-38B "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," May 2005.	AES with 128-bit keys	AES with 128-bit keys	AES with 128-bit keys
MAC-TDES	Message authentication code algorithm using the Triple DES block cipher NIST FIPS PUB 113, "Computer Data Authentication," May 1985.	TDES with three unique 56-bit keys	TDES with three unique 56-bit keys	**CANNOT BE USED**
HMAC	Keyed-hash message authentication code algorithm NIST FIPS PUB 198 "The Keyed-Hash Message Authentication Code (HMAC)," March 2002.	160-bit hash	160-bit hash	160-bit hash

NOTES:
1. AES implemented with 192-bit and 256-bit keys exceeds the security strength for all security lifetimes specified in this table.

4.2.4 Secure Hashing

A secure ***hash algorithm*** can be used to support implementation of keyed-hash message authentication, digital signature algorithms, key derivation functions and random number generators. Cryptographic modules that use a secure hash algorithm shall adhere to the specification in Table 4-4.

Table 4-4. Secure Hash Specifications
Version 1.0 - Approved 07/25/2007

Name	Description and Reference Document	security strength to achieve specified security lifetime (minimum hash size)		
		through year 2010	through year 2030	beyond year 2030
SHA-n	A secure hash algorithm that produces a hash size of "n" NIST FIPS PUB 180-2, "Secure Hash Standard," February 2004.	224-bit hash	224-bit hash	256-bit hash

NOTES:
1. In general notation SHA-n indicates a hash function that provides n-bit hash value. However, SHA-1 indicates a hash function with a 160-bit hash value that was originally specified in NIST FIPS PUB 180-1.
2. SHA-1 has recently been demonstrated to be inadequate for providing security strength necessary for a security lifetime through the year 2010.
3. SHA-384 and SHA-512 exceed the security strength for all security lifetimes specified in this table.

4.3 Cryptographic Key Security

Documents describing all implementation aspects of cryptographic key generation and management by the security service shall be kept confidential and are considered a "security record" for the purposes of ORC 149.433. These documents contain information directly used for protecting or maintaining the security of public office against attack, interference or sabotage and must be adequately protected using strong cryptographic methods.

4.4 Revision to the Standard

The Statewide IT Standards Manager will ensure this standard is reviewed and updated in response to advances in cryptography research, discovery of security vulnerabilities and breaches, and changes in federal, state and local laws that mandate data protection and privacy. Discovery of potential threats or mathematical weakness reducing the security provided through the use of this standard will be immediately investigated by the Statewide IT Standards Manager. Any technology breakthrough in the cryptography algorithms specified in this standard will cause the Statewide IT Standards Manager to reevaluate this standard and provide necessary revisions.

The Statewide IT Standards Manager is tracking the development of the next version of NIST FIPS PUB 140-2, which has been released for comment as of the date of this standard. When it becomes official, this standard will be reviewed and updated as appropriate.

4.5 Exceptions to the Standard

There are no exceptions to this state IT standard.

5.0 References

5.1 Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," defines the authority of the state CIO to establish State of Ohio IT standards as they relate to the acquisition and use of information technology by state agencies, including, but not limited to, hardware, software, technology services and security.

5.2 Ohio Revised Code Section 149.433.

Section 149.433 of the Ohio Revised Code exempts security and infrastructure records from public record requests.

5.3 NIST Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules." U.S. Department of Commerce. May 25, 2001.

FIPS Pub 140-2 Annex A, "Approved Security Functions for FIPS PUB 140-2," includes a list of approved security functions for encryption (symmetric key), signature (asymmetric key), message authentication, hashing and random number generators.

5.4 NIST Special Publication 800-57, "Recommendation for Key Management – Part 1: General." U.S. Department of Commerce. March 2007.

Special Publication 800-57, Part 1 provides general guidance and best practices for management of cryptographic keying materials. It provides background information and establishes frameworks to support appropriate decisions when selecting and using cryptographic mechanisms.

5.5 NIST Special Publication 800-21, "Guideline for Implementing Cryptography In the Federal Government: Second Edition." U.S. Department of Commerce. December 2005.

Special Publication 800-21 provides a set of guidelines for selecting, specifying, employing, and evaluating cryptographic protection mechanisms.

5.6 Rule 123:3-1-01 of the Ohio Administrative Code.

Rule 123:3-1-01 of the Ohio Administrative Code establishes the minimum requirements for creating, maintaining and using electronic signatures and records; the type, manner and format of electronic signatures; and security processes and procedures.

6.0 Definitions

Asymmetric Key Cipher	A cryptographic algorithm that uses two encryption keys: the private key, which is never shared and is used when the data is encrypted, and the public key, which is shared and used when the data is decrypted. One drawback with asymmetric key ciphers is that they can be more computationally intense than comparably secure symmetric ciphers, therefore requiring more resources to achieve the same security.
Cipher	A cryptographic algorithm used to encrypt or decrypt data.

CMVP	Cryptographic Module Validation Program (CMVP) was established by NIST and the Communications Security Establishment (CSE) of Canada in July 1995. All cryptographic module testing under CMVP is handled by one of thirteen accredited third-party testing laboratories.
CMVP Pre-validation List	CMVP Pre-validation List includes cryptographic module and vendor names that are in the process of FIPS PUB 140-2 validation. Participation in this listing is a joint decision by the vendor and testing laboratory. Posting on the list does not imply guarantee of final FIPS PUB 140-2 validation. The list is updated weekly by NIST.
Cryptographic Algorithm	A computational procedure that takes variable inputs, including a cryptographic key, and produces an output intended to implement a security function. There are three classes of cryptographic algorithms: hash functions, symmetric key ciphers and asymmetric key ciphers. These are defined by the number of cryptographic keys used with the algorithm (0, 1, or 2, respectively).
Cryptographic Module	A combination of hardware, software and firmware that implements a security service using one or more cryptographic algorithms.
Cryptographically Strong	Describes a quality attribute of a security function that means, in comparison to other methods, the function has greater resistance against attack. Security functions approved in this standard are deemed cryptographically strong in particular against attacks of brute force key search that intend to access the sensitive data protected by the specified algorithms.
Hash Algorithm	A function that maps a bit string of arbitrary length into a fixed length bit string. Secure hash functions are resistant to computational attacks that attempt to determine any input that maps to any pre-specified output.
Message Authentication Code	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data.
NIST	National Institute of Science and Technology (NIST) is a federal agency within the U. S. Department of Commerce that establishes technology, measurement and national standards for information security as well as other areas.
Security Lifetime	The estimated time period during which data protected by a specific cryptographic algorithm remains secure.
Security Service	A cryptography mechanism used to provide confidentiality, data integrity, authentication, authorization or non-

repudiation of information. A security service is often used to protect cryptographic keying material.

Security Strength — A "number" associated with the amount of work that is required to "break" a cryptographic algorithm or systems. In this standard, security strength is specified in "bits" such as the following: 128-bits or 160-bits.

Symmetric Key Cipher — A cryptographic algorithm that uses a single key to encrypt data. In practice, the two parties that encrypt and decrypt data must agree on the encryption key in advance. Symmetric key ciphers can be significantly faster than asymmetric key ciphers, but the necessity of exchanging keys increases their vulnerability.

7.0 Related Resources

Document Name
NIST Computer Security Resource Center, Cryptographic Toolkit: http://csrc.nist.gov/CryptoToolkit/
NIST Computer Security Resource Center, CMVP Pre-validation List: http://csrc.nist.gov/cryptval/140-1/140PreVal.pdf

8.0 Implementation – Referencing the Standard

This state IT standard can be incorporated by reference into state or agency security policies. This standard should be invoked by reference when cryptographically strong security functions are required or mandated for the protection of critical or sensitive data. It can also be used in application and system specification documents as well as procurement documents, or in circumstances with less critical security requirements.

This standard and its specifications are invoked by incorporating a reference similar to one of the following:

- "… in conformance with Ohio State IT Standard ITS-SEC-01, "Data Encryption and Cryptography."
- "… as described in section 4.1.1, "Symmetric Key Ciphers for Data Encryption" of Ohio State IT Standard ITS-SEC-01, "Data Encryption and Cryptography."
- "… as specified in Table 4-1, "Symmetric Key Cipher Specifications" of Ohio State IT Standard ITS-SEC-01, "Data Encryption and Cryptography."

9.0 Revision History

Date	Description of Change
07/25/2007	Version 1.0, Original Standard
07/01/2008	Scheduled Standard Review

10.0 Inquiries

For information regarding this or any state IT standard, please contact:

State IT Standards Manager
Enterprise Architecture & Standards
Investment and Governance Division
Ohio Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

Telephone: 614.995.9928
Facsimile: 614.644.9152
Email: State.ITStandards.Manager@oit.ohio.gov

State of Ohio IT Standards can be found online at: www.ohio.gov/itp

11.0 Attachments

None.