



# Office of Information Technology Services

State Capitol P.O. Box 2062  
Albany, NY 12220-0062  
[www.its.ny.gov](http://www.its.ny.gov)

<b>New York State Information Technology Standard</b>	<b>No:</b> NYS-S14-007
<b>IT Standard:</b>  <b>Encryption</b>	<b>Updated:</b> 07/16/2020
	<b>Issued By:</b> NYS Office of Information Technology Services  <b>Owner:</b> Chief Information Security Office

## 1.0 Purpose and Benefits

---

Encryption is a cryptographic operation that is used to enhance security and protect the State's electronic data ("data") by transforming readable information ("plaintext") into unintelligible information ("ciphertext"). Encryption is an effective tool in mitigating the threat of unauthorized access to data.

## 2.0 Authority

---

*Section 103(10) of the State Technology Law* provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines](#).

## 3.0 Scope

---

This standard applies to all "State Government" entities as defined in Executive Order 117 or "State Agencies" as defined in Section 101 of the State Technology Law ("State Entities"), their employees, and all others, including third parties (such as local governments, consultants, vendors, and contractors), that use or access any ITS Information Technology Resource for which ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS. While a

State Entity may adopt a different standard, such a standard shall at minimum include the requirements of this standard.

This standard applies to all systems, which includes websites and web services, for which the SE has administrative responsibility, including those managed and hosted by third-parties on behalf of the State.

## 4.0 Information Statement

---

The need for encryption of information is based on its classification, risk assessment results, and use case.

Attention must be given to the regulations and national restrictions (e.g., export controls) that may apply to the use of cryptographic techniques in different parts of the world. The US Government restricts the export, disclosure, or release of encryption technologies to foreign countries or foreign nationals, including “deemed exports” to foreign nationals within the United States (excluding those foreign nationals with permanent resident visas (e.g., Green Cards), US citizenship, or ‘protected person’ status). If you have any questions, please contact Counsel and Legal Services.

Encryption products for confidentiality of data at rest and data in transit must incorporate Federal Information Processing Standard (FIPS) approved algorithms for data encryption. Approved encryption algorithms are contained in [Appendix A](#).

Hashing algorithms transform a digital message into a short representation for use in digital signatures and other applications to validate the integrity of the message

Although hash functions such as SHA 1, provide a certain amount of security strength, it does not meet all security requirements for keyed-hash functions such as HMAC SHA 1. Refer to [FIPS 180-4 Secure Hash Standard \(SHS\)](#) for more information on different types of application hashing algorithms as well as [Appendix A](#).

Hashing algorithms can be used for multiple purposes including but not limited to, digital signatures, message authentication codes, key derivation functions, pseudo random functions.

Approved hashing functions are contained in [Appendix A](#).

Use of outdated, cryptographically broken, proprietary encryption algorithms/hashing functions is prohibited.

Due to the prevalence of incorrectly implemented cryptography, encryption products must have [FIPS 140-3 Security Requirements for Cryptographic Modules](#) validation and be operated in FIPS mode. Refer to [Appendix B](#) - Guidance in Selecting FIPS 140 Validated Products for further information.

Electronic information used to authenticate the identity of an individual or process (e.g., PIN, password, passphrase) must be encrypted when stored, transported or transmitted. This does not include the distribution of a one-time use PIN, password, passphrase, token

code, etc., provided it is not distributed along with any other authentication information (e.g., user-ID).

A system's security plan must include documentation to show appropriate review of encryption methodologies and products. This will demonstrate due diligence in choosing a method or product that has received substantial positive review by reputable third-party analysts.

#### **4.1 Data in Transit**

Encryption is required for data in transit in the following situations:

1. When electronic Personal, Private or Sensitive Information (PPSI) is transmitted (including, but not limited to, e-mail, File Transfer Protocol (FTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP), etc.).
2. When encryption of data in transit is prescribed by law or regulation.
3. When connecting to the State internal network(s) over a wireless network.
4. When remotely accessing the State internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, infrared) network. This does not apply to remote access over a State managed point to point dedicated connection.
5. When data is being transmitted with a State public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP) where technically feasible. State public facing websites must utilize HTTP Strict Transport Security (HSTS), automatically redirecting HTTP requests to HTTPS websites where technically feasible. Minimum browser support is listed in Appendix C.

Appropriate encryption methods for data in transit include, but are not limited to, Transport Layer Security (TLS) 1.2 or later, Secure Shell (SSH) 2.0 or later, Wi-Fi Protected Access (WPA) version 2 or later (with WiFi Protected Setup disabled) and encrypted Virtual Private Networks (VPNs). Components should be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.

#### **4.2 Data at Rest**

Encryption is required for data at rest, as follows:

1. For the systems listed below:
  - a. desktops that access or contain State Entity (SE) PPSI;
  - b. data stores (including, but not limited to, databases, file shares) that contain SE PPSI;
  - c. all mobile devices, whether State issued or third-party, that access or contain any SE information; and
  - d. all portable storage devices containing any SE information.

2. When electronic PPSI is transported or stored outside of a State facility.

Full disk encryption is required for all State issued laptops that access or contain SE information. Full disk encryption products must use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.

To mitigate attacks against encryption keys, when outside of State facilities, SE laptops and third-party laptops that access or contain SE PPSI must be powered down (i.e., shut down or hibernated) when unattended.

SEs must have a process or procedure in place for confirming devices and media have been successfully encrypted using at least one of the following, listed in preferred order:

1. automated policy enforcement;
2. automated inventory system; or
3. manual record keeping.

#### **4.3 Key Management**

The SE must ensure that a secure environment is established to protect the cryptographic keys used to encrypt and decrypt information. Keys must be securely distributed and stored.

Access to keys must be restricted to only individuals who have a business need to access the keys.

Unencrypted keys must not be stored with the data that they encrypt.

Keys will be protected with an authentication token that conforms to the identified assurance level as per the [NYS-P20-001 Digital Identity Policy](#).

Compromise of a cryptographic key would cause all information encrypted with that key to be considered unencrypted. If a compromise has been discovered a new key must be generated and used to continue protection of the encrypted information. Specific circumstances should be evaluated to determine if a breach notification is required.

Encryption keys and their associated software products must be maintained for the life of the archived data that was encrypted with that product.

## **5.0 Compliance**

---

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, State Entities shall request an exception through the Chief Information Security Office [exception process](#).

## 6.0 Definitions of Key Terms

---

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

## 7.0 Contact Information

---

Submit all inquiries and requests for future enhancements to the policy owner at:

**Chief Information Security Office**  
**Reference: NYS-S14-007**  
**NYS Office of Information Technology Services**  
**1220 Washington Avenue, Building 5**  
**Albany, NY 12226**  
**Telephone: (518) 242-5200**  
**Email: [CISO@its.ny.gov](mailto:CISO@its.ny.gov)**

Statewide technology policies, standards, and guidelines may be found at the following website: <http://www.its.ny.gov/tables/technologypolicyindex>

## 8.0 Revision History

---

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
03/21/2014	Original Standard Release; <i>replaces CSCIC/OCS Cryptographic Controls (S10-006) and Key Management Standards (S10-007) and ITS Encryption Standard (ITS-S07-001)</i>	Thomas Smith, Chief Information Security Officer
03/20/2015	Allow for UEFI Secure Boot in place of pre-boot authentication. Require TPM for pre-boot authentication. Minor wording clarifications.  Updated key length for ECDSA and SHA from 224 to 256 in Appendix A.	Deborah A. Snyder, Deputy Chief Information Security Officer
03/15/2016	Require all websites and web services within scope to be accessible through a secure connection (HTTPS). Revised TLS 1.1 to 1.2	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy

		Chief Information Security Officer
06/26/2017	Add Appendix C - Minimum Browser Support	Deborah A. Snyder, Acting Chief Information Security Officer
07/16/2020	Update revised Scope and Authority and update links from Identity Assurance to Digital Identity	Karen Sorady, Chief Information Security Officer

## 9.0 Related Documents

---

[NIST Special Publication 800-111, Guide To Storage Encryption Technologies For End User Devices](#)

[NIST Special Publication 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths](#)

[NIST Special Publication 800-57, Part 1, Recommendation for Key Management – Part 1: General](#)

[NIST Federal Information Processing Standard \(FIPS\) Publication 140-3](#)

[NIST Federal Information Processing Standard \(FIPS\) Publication 198-1](#)

[NIST Federal Information Processing Standard \(FIPS\) Publication 180-4](#)

[NIST Special Publication 800-107, Revision 1, Recommendation for Applications Using Approved Hash Algorithms](#)

## APPENDIX A - Approved Algorithms

<b>Algorithm</b>	<b>Minimum Key Length</b>	<b>Use Case</b>
AES	128	Data Encryption
RSA	2048	Digital Signatures Public Key Encryption
ECDSA	256	Digital Signature Public Key Encryption
SHA	256	Hashing
HMAC SHA 1	112	Keyed-Hash Message Authentication Code

## APPENDIX B – Guidance for Selecting FIPS 140 Validated Products

All government agencies that use cryptographic-based systems to protect Personal, Private or Sensitive Information (PPSI), need to have a minimum level of assurance that the product's stated security claim is valid.

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) cryptography-based standards.

**Historically, over 48% of cryptographic modules that have undergone FIPS validation had security flaws that were corrected during testing. In other words, without validation, users would have had only a 50-50 chance of buying correctly implemented cryptography.**

The list of FIPS validated cryptographic modules can be found on the NIST web site at <http://csrc.nist.gov/groups/STM/cmvp/validation.html>. The list can be searched by vendor or by year of validation.

It is important to note that the items on this list are cryptographic modules which may either be an embedded component of a product or application, or a complete product in and of itself. In addition, it is possible that vendors who are not found on this list might incorporate a validated cryptographic module from this list into their own products and components.

When selecting a product from a vendor, verify that the application or product that is being offered is either a validated cryptographic module itself (e.g., full disk encryption solution, SmartCard) or the application or product uses an embedded validated cryptographic module (toolkit, etc.) by confirming the module's validation certificate number. Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module which provides all the cryptographic services in the solution and references the module's validation certificate number. This number can be checked against the CMVP validation list. If the information does not agree, the vendor is not offering a validated solution.

Be aware that vendors may sometimes make invalid conformance claims such as:

- The module has been designed for compliance to FIPS 140-3.
- The module has been pre-validated and is on the CMVP pre-validation list.
- The module will be submitted for testing.
- The module has been independently reviewed and tested to comply with FIPS 140-3.
- The module meets all the requirements of FIPS 140-3.
- The module implements FIPS Approved algorithms; including having algorithm certificates.
- The module follows the guidelines detailed in FIPS 140-3.

**A cryptographic module does not meet the requirements or conform to the FIPS standard unless a reference can be made to the validation certificate number.**

Users must also be cognizant of the version number of the validated cryptographic module and, for software products, the operating systems that it has been tested on. Only the version numbers listed in the Cryptographic Module column of the CMVP list are FIPS validated and only when run on the operating systems listed in the Level/Description column.

### **FIPS Mode**

Many validated products have the capability to operate in FIPS mode, as well as non-FIPS mode. Operating in FIPS mode will ensure that the module uses only FIPS approved encryption algorithms.

Vendors provide a “Security Policy” as part of their module/product validation. This “Security Policy” can be found under the Cryptographic Module column on the CMVP list. The “Security Policy” will provide information on how to configure the module in a FIPS mode of operation and how the module functions to meet the FIPS requirements.

### **Modules in Process**

NIST maintains a Modules in Process list. Inclusion on the list is at the option of the vendor. Posting on this list does not imply a guarantee of final FIPS validation. Therefore, SEs that deploy a module before it is validated incur a level of risk in that the module may never be validated, or the version submitted for testing is not the version that is validated.

APPENDIX C – Minimum Browser Support

<b>Browser</b>	<b>Supported Version</b>
<b>Google Android OS Browser</b>	Android 6.0-6.0.1, 7.0-7.1.0 and higher
<b>Google Chrome</b>	49 and higher
<b>Mozilla Firefox</b>	49 and higher
<b>Microsoft Internet Explorer</b>	IE 11 or higher
<b>Microsoft Edge</b>	Edge 12 or higher
<b>Microsoft Edge</b>	Edge 13 for Windows 10 Mobile v1511 or higher
<b>Microsoft Internet Explorer Mobile</b>	None – No support for Windows Phone 8.1 or below
<b>Opera Browser</b>	37 or higher
<b>Apple Safari</b>	10 or higher & macOS 10.12 or higher
<b>Apple Safari Mobile</b>	10 or higher & iOS 10 or higher