



Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	No: NYS-S14-007
IT Standard: Encryption	Updated: April 15, 2016
	Issued By: NYS Office of Information Technology Services Standard Owner: Enterprise Information Security Office

1.0 Purpose and Benefits of the Standard

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 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), 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.

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

3.0 Scope

This standard applies to all systems, which includes websites and web services, for which the State 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 U.S. 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 (i.e., Green Cards), U.S. 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 at a minimum of 128 bit strength. Minimum key length for digital signatures and public key encryption is 2048. Hashing functions must have a minimum key length of 256. Approved algorithms are contained in Appendix A. Use of outdated, cryptographically broken, or proprietary algorithms is prohibited.

Due to the prevalence of incorrectly implemented cryptography, encryption products must have FIPS 140 (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 (i.e., 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 law or regulation requires encryption of data in transit.

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. State websites and web services, are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP). State public facing websites must automatically redirect HTTP requests to HTTPS websites.

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 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 Information Assurance 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 in order 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. All new websites and web services within the scope of this policy must immediately comply with this standard. All existing websites and web services within the scope of this policy, must be compliant with this standard by December 1, 2016, or have an approved exception request on file with the Enterprise Information Security Office.

The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this standard. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

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

6.0 Definitions of Key Terms

Encryption	A technique used to protect the confidentiality of information. The process transforms ("encrypts") readable information into unintelligible text through an algorithm and associated cryptographic key(s).
Mobile Device	A computing device in a small form factor that has at least one network connection interface, non-removable and/or removable storage, and is portable, including but not limited to smartphones, Personal Digital Assistants (PDAs), tablets, laptops, smart watches and wearable devices.
Portable Storage Device	A storage device that is capable of being physically transported, including but not limited to USB/flash drives/thumb drives, external hard drives, tapes, CDs, DVDs and cameras.

7.0 ITS Contact Information

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

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
1220 Washington Avenue – Bldg. 7A, 4th Floor
Albany, NY 12242
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to the Enterprise Information Security Office at
eiso@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Review Schedule and Revision History

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
03/20/2017	Scheduled Standard Review	

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 140-2](#)

APPENDIX A - Approved Algorithms

Algorithm	Minimum Key Length	Use Case
AES	128	Data Encryption
RSA	2048	Digital Signatures Public Key Encryption
ECDSA	256	Digital Signature Public Key Encryption
SHA	256	Hashing

APPENDIX B - Guidance for Selecting FIPS 140 Validated Products

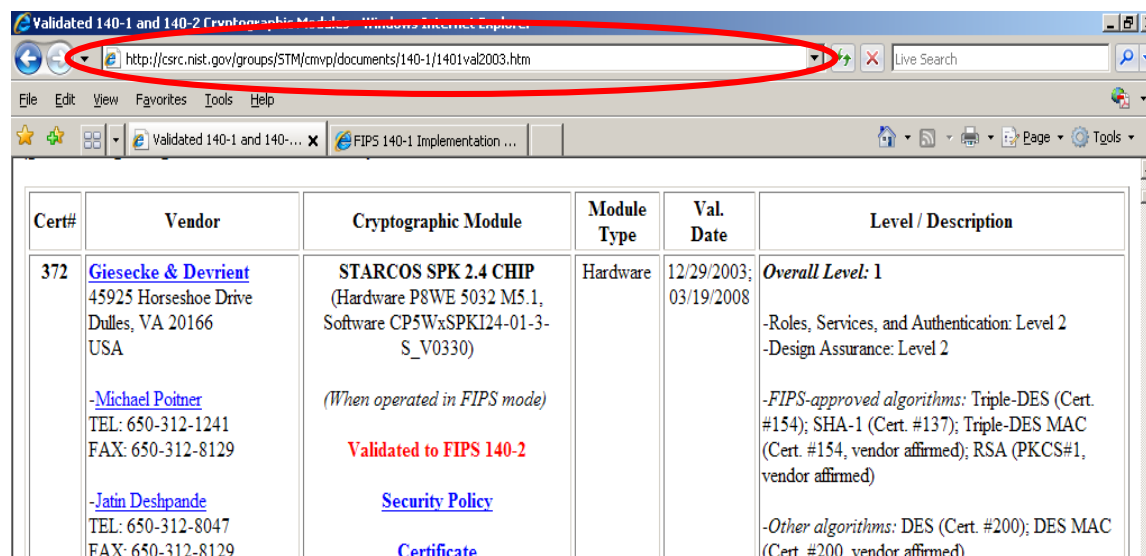
All government agencies that use cryptographic-based systems to protect Personal, Private or Sensitive Information (PPSI), need to have a minimum level of assurance that the product's stated security claim is valid.

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.

Figure 1: Screenshot of NIST CMVP Validation List for All Years



Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
372	Giesecke & Devrient 45925 Horseshoe Drive Dulles, VA 20166 USA -Michael Poitner TEL: 650-312-1241 FAX: 650-312-8129 -Jatin Deshpande TEL: 650-312-8047 FAX: 650-312-8129	STARCOS SPK 2.4 CHIP (Hardware P8WE 5032 M5.1, Software CP5WxSPKI24-01-3- S_V0330) (When operated in FIPS mode) Validated to FIPS 140-2 Security Policy Certificate	Hardware	12/29/2003; 03/19/2008	Overall Level: 1 -Roles, Services, and Authentication: Level 2 -Design Assurance: Level 2 -FIPS-approved algorithms: Triple-DES (Cert. #154); SHA-1 (Cert. #137); Triple-DES MAC (Cert. #154, vendor affirmed); RSA (PKCS#1, vendor affirmed) -Other algorithms: DES (Cert. #200); DES MAC (Cert. #200 vendor affirmed)

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.

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.

Figure 2: Certificate Number on NIST CMVP Validation List

1040	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134 USA -Global Certification Team TEL: CST Lab: NVLAP 200427-0	Cisco 3825 and Cisco 3845 Integrated Services Routers (Hardware Versions: 3825 and 3845; Firmware Versions: 12.4(15)T3[1] and 12.4(15)T10[2]) <i>(When operated in FIPS mode)</i> Validated to FIPS 140-2 Security Policy Certificate	Hardware	10/14/2008; 08/28/2009; 10/23/2009; 05/28/2010; 02/23/2012	Overall Level: 2 <i>-FIPS Approved algorithms: A</i> (Certs. #50, #436 [1] and #696 (Certs. #379 [1] and #576 [2]); DES (Certs. #210, #683 [1] and <i>-Other algorithms: Diffie-Hell</i> <i>provides 80 or 96 bits of encry</i> <i>key establishment methodolog</i> <i>compliant less than 112 bits of</i> DES Multi-chip standalone "The Cisco 3800 Series feature simultaneous services at wire s routers offer embedded encryp
------	--	--	----------	--	---

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

- The module has been designed for compliance to FIPS 140-x.
- 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-x.
- The module meets all the requirements of FIPS 140-x.
- The module implements FIPS Approved algorithms; including having algorithm certificates.
- The module follows the guidelines detailed in FIPS 140-x.

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.

Figure 3: Version Number and Operating Systems on NIST CMVP Validation List

1010	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA -Dave Friant TEL: 425-704-7984 FAX: 425-936-7329 CST Lab: NVLAP 200427-0	Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) (Software Versions: 6.0.6001.22202 and 6.0.6002.18005) <i>(When operated in FIPS mode with Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1006 operating in FIPS mode)</i> Validated to FIPS 140-2 Security Policy Certificate	Software	08/15/2008; 07/24/2009	Overall Level: 1 -Operational Environment: Tested as meeting Level 1 with Microsoft Windows Server 2008 (x86 Version); Microsoft Windows Server 2008 (x64 version); Microsoft Windows Server 2008 (IA64 version) (single-user mode) -FIPS Approved algorithms: AES (Cert. #739); HMAC (Cert. #408); RNG (SP 800-90, vendor affirmed); RSA (Certs. #353 and #355); SHS (Cert. #753); Triple-DES (Cert. #656) -Other algorithms: DES; MD2; MD4; MD5; RC2; RC4; RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
------	---	--	----------	---------------------------	--

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.

Figure 4: Security Policy on NIST CMVP Validation List

Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
372	Giesecke & Devrient 45925 Horseshoe Drive Dulles, VA 20166 USA - Michael Poirner TEL: 650-312-1241 FAX: 650-312-8129 - Jatin Deshpande TEL: 650-312-8047 FAX: 650-312-8129	STARCOS SPK 2.4 CHIP (Hardware P8WE 5032 M5.1, Software CP5WxSPKI24-01-3- S_V0330) (When operated in FIPS mode) Validated to FIPS 140-2 Security Policy Certificate	Hardware	12/29/2003; 03/19/2008	Overall Level: 1 -Roles, Services, and Authentication: Level 2 -Design Assurance: Level 2 -FIPS-approved algorithms: Triple-DES (Cert. #154); SHA-1 (Cert. #137); Triple-DES MAC (Cert. #154, vendor affirmed); RSA (PKCS#1, vendor affirmed) -Other algorithms: DES (Cert. #200); DES MAC (Cert. #200 vendor affirmed)

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.