

---

Cyber Security Standard S10-006

**Cryptographic Controls**

Original Publication Date: February 12, 2010  
Revision Date: July 30, 2010

---

**Thomas D. Smith**  
**Director**  
**New York State**  
**Office of Cyber Security**  
**30 South Pearl Street**  
**Albany, N.Y. 12207-3425**

## CYBER SECURITY STANDARD

Reference:	<b>S10-006, V1.1</b>
Standard Title:	<b>Cryptographic Controls</b>
Related Policy:	<b>Cyber Security Policy P03-002, Information Security Policy</b>
Replaces & Supersedes:	<b>Cyber Security Standard S10-006, V1.0, February 12, 2010</b>
Authority:	<b>Section 715 of the Executive Law</b>
Issued By:	<b>Thomas D. Smith, Director, NYS Office of Cyber Security</b>
Original Publication Date:	<b>February 12, 2010</b>
Revision Date:	<b>July 30, 2010</b>

# TABLE OF CONTENTS

---

<b>TABLE OF CONTENTS</b> .....	<b>3</b>
<b>PURPOSE</b> .....	<b>4</b>
<b>SCOPE</b> .....	<b>4</b>
<b>STANDARD</b> .....	<b>5</b>
PREFACE .....	5
CRYPTOGRAPHIC CONTROLS .....	5
<i>Policy</i> .....	5
<i>Standard</i> .....	6
<i>Guidelines</i> .....	8
<b>DOCUMENT CHANGE MANAGEMENT</b> .....	<b>9</b>
<b>DEFINITIONS &amp; ACRONYMS</b> .....	<b>9</b>
<b>CONTACT INFORMATION</b> .....	<b>9</b>
<b>APPENDIX A</b> .....	<b>10</b>

## ***PURPOSE***

---

The purpose of the Cyber Security Standards is to define a set of minimum security requirements that all *State Entities (SE)* must meet. These *Standards* shall serve as best practices for the State University of New York and the City University of New York campuses. Any *SE* may, based on its individual business needs and specific legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA), exceed these security requirements, but must, at a minimum, achieve the security levels required by these *Standards*.

The primary objective of the Cyber Security Standards is to provide specific technical requirements. These *Standards* cover details such as implementation steps, *systems* design concepts, software interface mechanisms and other specifics.

## ***SCOPE***

---

The Cyber Security Standards apply to all *SEs*. These *Standards* are not intended to unilaterally change the terms and conditions of employment. All *SEs*, when coming into compliance with these *Standards*, must consider all terms and conditions of employment including collective bargaining agreements.

These *Standards* are applicable to *SEs*, staff and all others, including outsourced *third parties*, which have access to or manage *SE information*. Where conflicts exist between these *Standards* and a *SE's standards*, the more restrictive *standards* will take precedence. The Cyber Security Standards for *SEs* encompass all *systems*, automated and manual, for which the *State* has administrative responsibility, including *systems* managed or hosted by *third parties* on behalf of the *SE*. It addresses all *information*, regardless of the form or format, which is created or used in support of business activities of *SEs*. These *Standards* must be communicated to all staff and all others who have access to or manage *SE information*.

## STANDARD

---

### Preface

The Cyber Security Standards are a statement of the minimum requirements, ethics, responsibilities and accepted behaviors required to establish and maintain a secure environment, and achieve the *State's information security* objectives. Compliance with these *Standards* is mandatory. The Cyber Security Standards set the direction, give specific guidance and define requirements for *information security* related processes and actions across *SEs*. These *Standards* document many of the security practices already in place in some *SEs*. Senior management is fully committed to *information security* and agrees that every person employed by or on behalf of New York State government has important responsibilities to continuously maintain the security of *SE data*.

Policies alone will not offer *SEs* the guidance necessary to implement the Cyber Security Policy and meet the objectives of the *State*. *Standards* provide this support and guidance by defining what is to be accomplished in specific terms. These *Standards* provide specific mandatory activities, actions, rules or regulations designed to reinforce **Cyber Security Policy P03-002**.

### Cryptographic Controls (P03-002, Part 11. Systems Development and Maintenance Policy)

#### Policy

- A. *Encryption* is an important security layer that is used to protect the *confidentiality* of *information*. *Encryption* is an effective tool in mitigating the *threat* of *unauthorized access* to *data*. However, there are other *threats*, such as a hacker gaining access to an authorized *user* account or process, where more stringent *controls* and/or the use of multiple *encryption* levels must be considered.
- B. Based on a *risk assessment*, the required level of protection should determine the strength of the *encryption* employed. In deciding what is best for the *SE*, the benefits of both stand-alone and enterprise level *encryption* solutions must be considered. Attention must also 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.

## Standard

- A. *Encryption* products for *confidentiality* of *data at rest* and *data in transit* must incorporate Federal Information Processing Standard (FIPS) approved algorithms for *data encryption*, e.g., Advanced Encryption Standard (AES) or Triple Data Encryption Standard (Triple DES). The use of proprietary algorithms is not allowed for any *encryption* purpose.
- B. All *encryption* methodologies and products must be approved in writing by the *SE* Information Security Officer (*ISO*) and documented to show that the *SE* has taken due diligence in choosing a method or product that has received substantial positive review by reputable *third party* analysts.
- C. *Encryption* is required for *data in transit* in the following situations:
1. When electronic *Personal, Private or Sensitive Information (PPSI)* is transmitted (includes email, FTP, etc.) outside of an *SE approved storage facility*.
  2. When connecting to the *SE* internal network(s) over a wireless network.
  3. When remotely accessing the *SE* internal network(s) or devices over a shared (e.g., NYeNET, *Internet*) or personal (e.g., Bluetooth, infrared) network. This does not apply to publically accessible resources or remote access over a point to point dedicated connection.
  4. When electronic *information* used to authenticate the identity of an individual or process (i.e., PIN, password, *passphrase*) is 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., userID).
- D. Appropriate *encryption* methods for *data in transit* include, but are not limited to, Transport Layer Security (TLS), Secure Socket Layer (SSL) 3.0, Secure Shell (SSH) 2.0 or later, Wi-Fi Protected Access (WPA) version 2 or later and Virtual Private Networks (VPNs).
- E. *Encryption* is required for *data at rest*, as follows:
1. For the devices listed below, regardless of whether or not they are in an *approved storage facility*:
    - a. *SE* laptops accessing or containing any *SE information*;
    - b. *Third party* laptops that access or contain *SE PPSI*;
    - c. All *Personal Digital Assistants (PDAs)*, including Blackberries, smartphones, etc., that access or contain any *SE information*; and
    - d. All USB Flash Drives containing any *SE information*.
  2. *Full disk encryption* is required for all *SE* laptops that access or contain *SE information*. *Full disk encryption* products must use pre-boot *authentication* except where the *SE ISO* has determined that the risk of not using pre-boot *authentication* has been mitigated with *compensating controls* and it has been approved in writing

by *SE* executive management. *Compensating controls* **must** include disabling all 1394 host controllers (Firewire, PCI, Cardbus, etc.) unless necessary to meet a documented business requirement. *SEs* may also consider multifactor *authentication* and/or storing *encryption* keys on a separate device as additional *compensating controls*.

3. When outside of an *approved storage facility*, *SE* laptops and *third party* laptops that access or contain *SE PPSI* must be powered down (i.e., shut down or hibernated) when unattended.
4. When electronic *PPSI* is transported or stored outside of an *SE approved storage facility*.

**Note:** Portable *electronic storage media* containing *PPSI* that is unable to be encrypted, due to technical constraints, business limitations or statutory requirements, must have a documented exception. Exceptions are not permitted for laptops, *Personal Digital Assistants (PDAs)*, or USB Flash Drives.

Exceptions must be processed and approved in writing by *SE* executive management, after recommendation by the *SE ISO*. A record of the approved exception shall be maintained by the *SE ISO*. In addition, the following handling controls must be in place when unencrypted media containing *PPSI* is taken outside of an *approved storage facility*:

- a. Hand delivery by *SE workforce* or delivery via courier (e.g., OGS, FedEx, UPS, US Postal Service);
- b. Receipt confirmation; and
- c. Double-sealed in appropriate secure container, addressed to specific recipient with no special marking on outer container.

The exception will be reviewed at least annually by the *SE ISO* to certify that the need is still valid and required and the controls in place are appropriate and current. For purposes of compliance reporting, any such exceptions shall not count toward compliance.

5. When electronic *information* used to authenticate the identity of an individual or process (i.e., PIN, password, *passphrase*) is stored or transported. 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., userID).
- F. *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. an automated inventory system; or
  3. manual record keeping.

## Guidelines

- A. Due to the prevalence of incorrectly implemented cryptography, *encryption* products should have FIPS 140 (Security Requirements for *Cryptographic* Modules) validation and be operated in FIPS mode. Refer to Appendix A - Guidance in Selecting FIPS 140 Validated Products for further information.
- B. *SEs* should look to replace implementations of SSL 3.0 with SSL 3.1 (TLS 1.0), or later, as soon as practicable. SSL 3.0 relies in part on the use of a *cryptographic* algorithm, MD5, which is not FIPS-Approved and has been proven to have security weaknesses

## ***DOCUMENT CHANGE MANAGEMENT***

---

Requests for changes to this *Standard* must be presented by the *SE ISO* to the New York State Office of Cyber Security (OCS). If the *State ISO* for OCS agrees to the change, he or she will formally draft the change and have it reviewed and approved through the normal OCS approval process. Each *SE ISO* will be responsible for communicating the approved changes to their organization.

This *Standard* will be reviewed at a minimum on an annual basis.

## ***DEFINITIONS & ACRONYMS***

---

Definitions and acronyms for New York State Cyber Security policies, *standards* and *guidelines* can be found in the Definitions and Acronyms document, available at [www.cscic.state.ny.us/lib/policies/](http://www.cscic.state.ny.us/lib/policies/).

## ***CONTACT INFORMATION***

---

Questions concerning this *Standard* may be directed to OCS at (518) 474-0865.

## APPENDIX A

### GUIDANCE FOR SELECTING FIPS 140 VALIDATED PRODUCTS

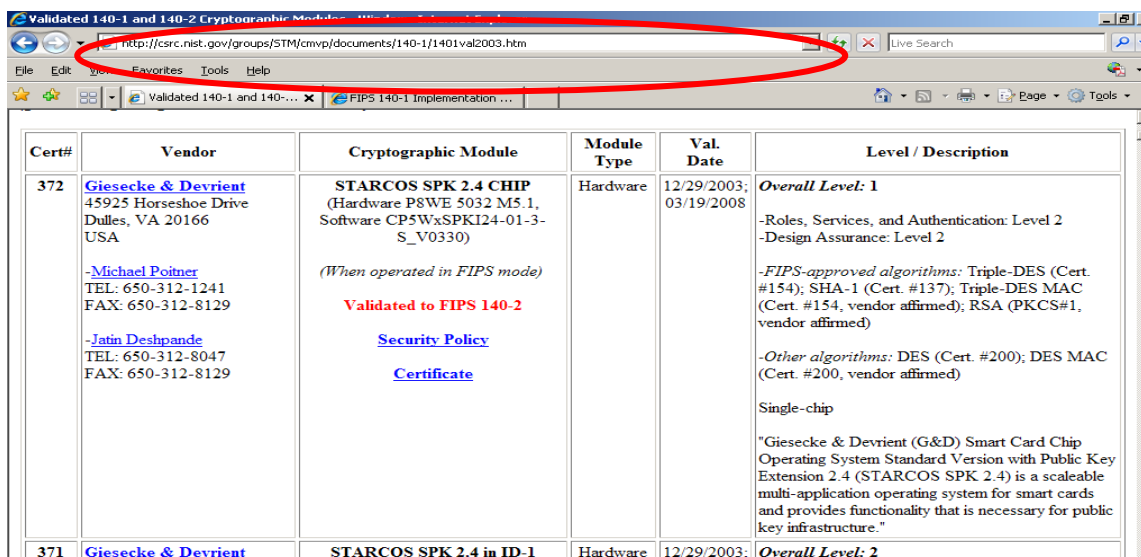
All government agencies that use *cryptographic*-based systems to protect *Personal, Private or Sensitive Information (PPSI)*, need to have a minimum level of assurance that the product's stated security claim is valid.

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) 140-1 *Security Requirements for Cryptographic Modules*, and other 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	<a href="#">Giesecke &amp; Devrient</a> 45925 Horseshoe Drive Dulles, VA 20166 USA  <a href="#">-Michael Poitner</a> TEL: 650-312-1241 FAX: 650-312-8129  <a href="#">-Jatin Deshpande</a> TEL: 650-312-8047 FAX: 650-312-8129	<b>STARCOS SPK 2.4 CHIP</b> (Hardware P8WE 5032 M5.1, Software CP5WxSPKI24-01-3- S_V0330)  (When operated in FIPS mode)  <b>Validated to FIPS 140-2</b>  <a href="#">Security Policy</a>  <a href="#">Certificate</a>	Hardware	12/29/2003; 03/19/2008	<b>Overall Level: 1</b>  -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)  Single-chip  "Giesecke & Devrient (G&D) Smart Card Chip Operating System Standard Version with Public Key Extension 2.4 (STARCOS SPK 2.4) is a scalable multi-application operating system for smart cards and provides functionality that is necessary for public key infrastructure."
371	<a href="#">Giesecke &amp; Devrient</a>	<b>STARCOS SPK 2.4 in ID-1</b>	Hardware	12/29/2003;	<b>Overall Level: 2</b>

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**

Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
1040	<p><a href="#">Cisco Systems, Inc.</a> 170 West Tasman Drive San Jose, CA 95134 USA</p> <p>-Michael Soto TEL: 408-902-8125 FAX: 408-902-8095</p>	<p>Cisco 3825 and Cisco 3845 Integrated Services Routers (Hardware Versions: 3825 and 3845; Firmware Version: 12.4(15)I3)</p> <p><i>(When operated in FIPS mode)</i></p> <p><b>Validated to FIPS 140-2</b></p> <p><a href="#">Security Policy</a></p> <p><a href="#">Certificate</a></p>	Hardware	10/14/2008	<p><b>Overall Level: 2</b></p> <p><i>-FIPS-approved algorithms:</i> . and #795), HMAC (Certs: #50 RNG (Cert. #456), RSA (Cert (Certs: #317 and #794), Triple #210 and #683)</p> <p><i>-Other algorithms:</i> Diffie-Hell agreement, key establishment n provides 80 or 96 bits of encry RSA (key wrapping, key establ methodology provides between of encryption strength); MD5; RC4; DES</p> <p>Multi-chip standalone</p> <p>The Cisco 3800 Series feature deliver multiple high-quality sin services at wire speeds up to T. The Cisco 3800 Series routers encryption acceleration on the r</p>
1039	<a href="#">Cisco Systems</a>	Cisco 2851 Integrated Services Router	Hardware	10/14/2008	<b>Overall Level: 2</b>

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**

Cert#	Vendor	Cryptographic Module	Module Type	Val. Date	Level / Description
1010	<p><a href="#">Microsoft Corporation</a> One Microsoft Way Redmond, WA 98052-6399... USA</p> <p>-Dave Eriant TEL: 425-704-7984 FAX: 425-936-7329</p>	<p>Windows Server 2008 Enhanced Cryptographic Provider (RSAENH) (Software Version: 6.0.6001.22202)</p> <p><i>(When operated in FIPS mode with Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1006 operating in FIPS mode)</i></p> <p><b>Validated to FIPS 140-2</b></p> <p><a href="#">Security Policy</a></p> <p><a href="#">Certificate</a></p>	Software	08/15/2008	<p><b>Overall Level: 1</b></p> <p><i>Operational Environment Tested as me Level 1 with Microsoft Windows Server (x86 Version); Microsoft Windows Serv (x64 version); Microsoft Windows Serv (IA64 version) (single-user mode)</i></p> <p><i>-FIPS-approved algorithms:</i> AES (Ce #739), HMAC (Cert. #408), RNG (SP 90, vendor affirmed); RSA (Certs. #355 #355); SHS (Cert. #753); Triple-DES (#656)</p> <p><i>-Other algorithms:</i> DES; MD2; MD4; RC2; RC4; RSA (key wrapping, key establishment methodology provides bet and 150 bits of encryption strength; non-compliant less than 80 bits of encryption strength)</p> <p>Multi-chip standalone</p> <p>*RSAENH encapsulates several differen cryptographic algorithms in an easy-to-u cryptographic module accessible via the</p>

## 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	<a href="#">Giesecke &amp; Devrient</a> 45925 Horseshoe Drive Dulles, VA 20166 USA  - <a href="#">Michael Poitner</a> TEL: 650-312-1241 FAX: 650-312-8129  - <a href="#">Jatin Deshpande</a> TEL: 650-312-8047 FAX: 650-312-8129	<b>STARCOS SPK 2.4 CHIP</b> (Hardware P8WE 5032 M5.1, Software CP5WxSPK124-01-3- S_V0330)  (When operated in FIPS mode)  Validated to FIPS 140-2 <a href="#">Security Policy</a> <a href="#">Certificate</a>	Hardware	12/29/2003; 03/19/2008	<b>Overall Level: 1</b>  -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)  Single-chip  "Giesecke & Devrient (G&D) Smart Card Chip Operating System Standard Version with Public Key Extension 2.4 (STARCOS SPK 2.4) is a scaleable multi-application operating system for smart cards and provides functionality that is necessary for public key infrastructure."
371	<a href="#">Giesecke &amp; Devrient</a>	<b>STARCOS SPK 2.4 in ID-1</b>	Hardware	12/29/2003	<b>Overall Level: 2</b>

## 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.