	Georgia Technology Authority	
Title:	**Cryptographic Controls**	
PSG Number:	SS-08-040.02	**Topical Area:** Security
Document Type:	Standard	**Pages:** 4
Issue Date:	03/31/2008	**Effective Date:** 03/15/2012 (revision)
POC for Changes:	GTA Enterprise Governance and Planning	
Synopsis:	Establishes the minimum requirements for implementing cryptographic controls.	

PURPOSE

The State has a regulatory and fiduciary duty to adequately protect non-public, sensitive, private, constituent and proprietary information for which it has custodial responsibility. There are circumstances when the risk of compromise or exposure of sensitive State data is greater than acceptable and compensating security control measures are insufficient. When increased confidentiality, authenticity, integrity or non-repudiation of information is critical, the use of cryptographic controls may be warranted.

Cryptography is a discipline that embodies principles, means and methods for providing several security services: confidentiality, data integrity, authentication and non-repudiation.

This standard establishes the conditions and minimum requirements for implementing cryptographic controls in state information systems.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARDS

Agencies shall use cryptographic controls where the security objectives of confidentiality, authentication, non-repudiation or data integrity is categorized MODERATE or higher; or when the risk of compromise or exposure is greater than acceptable by the business/data owner; or when required by policy, law, or regulation.

Agencies shall select cryptographic technology based on the security objectives, applicable policies, laws and regulations and performance requirements.

Cryptographic modules, algorithms, keys and implementations used for State of Georgia information systems shall implement the requirements of FIPS 140-2 or its successors for security level 1 or higher, and preference should be given to implementations validated through the Cryptographic Module Validation Program (CMVP).

Use of cryptographic implementations that have not been validated through the CMVP must be approved by the Senior Agency Information Security Officer (SAISO). In granting such approval, the SAISO must consider the additional risks introduced by the use of a non-validated crypto module, the relative cost savings, the availability of other solutions, and gain approval from the system's business owner. These solutions must also be detailed in the system security plan including compensating controls.

When concerns about physical tampering or hacking of the cryptographic module itself are prevalent use of FIPS 140-2 security level 2 modules or higher is required.

Agencies shall implement end-to-end cryptographic security controls for, but not limited to, the following:

- For identity and authentication credentials in storage or transit
- When non-repudiation is required
- To store cryptographic algorithm and key information
- For secure wireless communications
- For any sensitive data such as transmitting a person's social security number over the internet or other communications where the risk of compromise or exposure is higher than acceptable and compensating controls are insufficient

Security officers and/or cryptographic officers shall:

- Be properly trained to ensure the continued secure operations and maintenance of the cryptographic components and proper destruction or archive of keys when a system is decommissioned.
- Be notified and participate in any process where cryptographic systems are modified and ensure all changes are in accordance with change management policies and procedures.
- Be notified when a cryptographic system, encrypted data or transmission is believed to be exposed or compromised.

SUPPLEMENTAL EXCEPTION

Encrypted data shall be decrypted prior to being transferred to the Georgia Archives for long term storage. The Georgia Archives shall assume responsibility for providing appropriate control measures to maintain the confidentiality, integrity, availability and non-repudiation of the information in their charge.
See Georgia Secretary of State – Georgia Archives http://sos.georgia.gov/archives/

Records Management -> Rules and Regulations

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Enterprise Information Security Policy (Policy)
- Use of Cryptography (Policy)

REFERENCES

- NIST Computer Security Resource Center- http://csrc.nist.gov/
  - SP 800-53 rev 3 Recommended Security Controls:
    - SC 12-Cryptographic Key Establishment and Management
    - SC 13-Use of Cryptography
  - FIPS 140-2 Security Requirements for Cryptographic Modules
  - SP 800-12 (chapter 19) Introduction to Computer Security NIST Handbook
  - SP 800-21 Guideline for Implementing Cryptography in the Federal Government
  - SP 800-57 Recommendation for Key Management
  - SP 800-56 Recommendations for Pair-Wise Key Establishment Schemes
  - SP 800-63 Electronic Authentication Guideline
  - NIST Cryptographic Key Tool Kit http://csrc.nist.gov/CryptoToolkit/tkkeymgmt.html
  - NIST Cryptographic Module Validation Program http://csrc.nist.gov/groups/STM/cmvp/index.html

TERMS and DEFINITIONS

Cryptography - A branch of applied mathematics (algorithms) concerned with encrypting and decrypting data such that the sender's identity (authentication and non-repudiation), data confidentiality, integrity or origin can be assured.

- **Encryption** - The process of converting ordinary information (plain text) into unintelligible character strings (i.e., *ciphertext*).
- **Decryption** - The reverse of encryption, moving from unintelligible ciphertext to plaintext.
- A **cipher** (or *cypher*) - One or more algorithms which perform this encryption and the reversing decryption.
- **Key** (or cryptographic key) - A parameter used in conjunction with a cryptographic algorithm that an entity with knowledge of the key can reproduce or reverse the operation (encryption or decryption) while an entity without knowledge of the key cannot.

FIPS 140-2 Validated Cryptographic Modules – cryptographic implementations

including, but not limited to, hardware components or modules, software/firmware programs or modules or any combination thereof that employ approved security functions such as cryptographic algorithms, cryptographic key management techniques, and authentication techniques and validated through the Cryptographic Module Validation Program (CMVP).

Non-Repudiation - A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party.

Authentication - A process that establishes origin of information or determines an entity's identity.

Advanced Authentication (also referred to as strong authentication) - Uses techniques that require multi-factor identity credentials to confirm a user's identity and/or authority to access information resources.

Identity/authentication credentials are information provided by a user and recognized by the system such as passwords, private keys, symmetric keys, tokens, biometric data or digital signature algorithm used to positively identify that user.