Topics:
cryptography [2] authentication [3]

Cryptographic Controls [1]

SS-08-040.03 Cryptographic Controls

Issue Date: 3/31/2008

Effective Date: 12/15/2014

PURPOSE

The State has a fiduciary duty and at times a legal responsibility to adequately protect non-public, sensitive, personnel, constituent and/or proprietary information for which it owns or has custodial responsibility. There are circumstances when the risk of compromise or exposure to sensitive state data is greater than acceptable by the data owner, or by law, 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 requiring them.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

Enterprise Information Security Charter PS-08-005 [4]

STANDARD

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 or data owner; or when required by policy, law, or regulation.

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

Cryptographic modules, algorithms, keys and implementations used for State information systems shall be compliant with FIPS 140-2 or its successors.

Use of cryptographic implementations that are not at least FIPS security level 1 compliant or do not meet minimum security requirements defined for security level 1 must be approved by the Senior Agency Information Security Officer (SAISO) and justified in an approved exception request. These cryptographic implementations must also be detailed in the system security plan including any compensating controls and a plan forward to address compliance deficiencies.

When concerns about physical tampering or hacking of the cryptographic module itself exist, use of FIPS 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