



California ISO
Your Link to Power

**Application and CUDA-ISO® Integration
Standards and Guidelines**

 California ISO Your Link to Power	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

REVISION HISTORY

VERSION NO.	DATE	DESCRIPTION
1.0	11/19/1998	Initial Release.
1.1		Minor upgrades.
1.2		Minor upgrades.
1.3		Minor upgrades.
1.4	08/05/1999	Minor upgrades.
1.5	08/15/2000	Minor upgrades.
2.0	07/09/2002	Re-release with Major Format, Content and Title Changes.
2.1	08/08/2002	Re-released with Minor Upgrades—references to other docs.
2.2	09/16/2003	Minor Format Changes. Added Subsection 4.6.1.
2.3	05/16/2005	Minor changes.
2.4	06/21/06	Minor changes; Logo change
2.5	08/28/08	Identified changes for RIG certificate use
2.6	09/10/08	Changed document classification in order to post requirements for potential RIG/DPG vendors

 California ISO <small>Your Link to Power</small>	Corporate Standards and Guidelines	Review Date: No.	09/10/08 TBD
	Information Security-Cryptography	Version No.:	2.6
Application and CUDA-ISO Integration Standards and Guidelines		Effective Date	09/01/2003

TABLE OF CONTENTS

REVISION HISTORY I

1. INTRODUCTION 1

1.1. PURPOSE 1

1.2. SCOPE 1

2. DEFINITIONS 1

2.1. STANDARD 1

2.2. GUIDELINE 1

2.3. PROCEDURE 1

3. STANDARDS AND GUIDELINES 2

3.1. APPLICATION SECURITY FUNCTION STANDARDS 2

3.2. APPLICATION CONTROL FUNCTION STANDARDS 3

3.3. APPLICATION CONFIGURATION STANDARDS 3

3.3.1. *Existing Applications Communicating Via Standard Internet Application Protocols* 3

3.3.2. *Existing Applications Communicating Via Proprietary Application Protocols* 3

3.3.3. *New Applications* 3

3.3.4. *External Entities Interfacing with CAISO Applications* 4

3.4. CRYPTOGRAPHIC SECURITY STANDARDS 4

4. ASSURANCE LEVEL SELECTION GUIDELINES 4

4.1. GCP ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES 5

4.2. HIGH ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES 5

4.3. MEDIUM ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES 5

4.4. BASIC ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES 6

4.5. TEST ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES 6

4.6. CUDA-ISO® ASSURANCE LEVEL SELECTION MATRIX 6

4.6.1. *Change of Assurance Level* 7

5. COMPLIANCE TEST CRITERIA 7

5.1. MINIMUM TESTS 7

6. COMPLIANCE 8

7. REFERENCES 9

8. APPROVAL 9

8.1. STANDARDS AND GUIDELINES APPROVAL 9

 California ISO <small>Your Link to Power</small>	Corporate Standards and Guidelines	Review Date: No.	09/10/08 TBD
	Information Security-Cryptography	Version No.:	2.6
Application and CUDA-ISO Integration Standards and Guidelines		Effective Date	09/01/2003

1. INTRODUCTION

1.1. PURPOSE

The purpose of these standards and guidelines is to provide the CAISO enterprise-wide integration standards and guidelines between application and CAISO's Public Key Infrastructure (PKI) implementation known as Cryptographic Universal Design Architecture (CUDA-ISO®). These standards and guidelines include decision guidelines pertaining to CUDA-ISO® standards, as well as fundamental compliance test criteria to ensure that the integration is acceptable.

These standards and guidelines provide a general guide for integrating public key infrastructure security into applications. Project Team Leaders or Business Unit Managers must consult with Information Security regarding specific requirements for their application.

1.2. SCOPE

These standards and guidelines encompass all existing systems and applications, including hardware, software, and databases, as well as acquisitions and new application developments. These standards and guidelines also apply to the interfaces of any external entities that interact with CAISO systems.

2. DEFINITIONS

2.1. STANDARD

A standard is defined as a rule that must be implemented and followed to implement and comply with a policy(s). Standards provide specific details of roles and responsibilities, and define standard methods and tools to be used to comply with the policies. Standards provide additional information regarding why the policy is needed, how to implement the policies, and further explains consequences for non-compliance. The words "**must**" and "**shall**" will identify standards.

2.2. GUIDELINE

A guideline is defined as a highly recommended rule that should be implemented and followed to further enhance the mandatory standards and provide greater assurance of policy implementation and compliance. These guidelines potentially can become a standard as time progresses. The words "**should**" and "**may**" will identify guidelines.

2.3. PROCEDURE

A procedure is a series of specific instructions or steps taken that, when completed, accomplishes a desired and expected outcome. Documented procedures assist in implementing the standards and guidelines by describing the necessary tasks, identifying the responsible personnel to perform the tasks, and explaining the desired outcome. CAISO Directors will approve company Procedures.

 California ISO Your Link to Power	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

3. STANDARDS AND GUIDELINES

In support of the [CAISO Cryptographic Architecture and Standards](#), as well as the [CAISO Information Security Policy](#), these standards and guidelines enable system and application developers and administrators to fully leverage the CAISO Public Key Infrastructure (PKI) implementation (CUDA-ISO®) in order to provide the highest possible level of information security.

Information Security established an enterprise wide information security architecture based on CUDA-ISO® and fundamental information security measures. Refer to the [CAISO Enterprise Security Architecture](#) for additional details. CUDA-ISO® provides digital certificates to every user/system and application identified and selected according to these standards and guidelines. All future system and application development must consult with Information Security to determine if CUDA-ISO® is appropriate

3.1. APPLICATION SECURITY FUNCTION STANDARDS

Every application must provide the following security functions:

1. Mutually identify (where feasible) and authenticate the communicating parties based on their digital certificates. Additionally, in SSL communications, servers must minimally provide server-side authentication, versus an anonymous connection.
2. Applications must interface with CUDA-ISO® to check the validity of all certificates via a CRL, or some other appropriate method.
3. Protect, through strong encryption, the confidentiality and integrity of all data that flows between the communicating parties. Allow for RSA key exchange with strong encryption using RC4 algorithm (or equivalent) with at least 128 bit keys or 3DES (Triple DES) with 168 bit keys.
4. Generate and utilize RSA keys with a minimum of 1024 bit length.
5. Formulate standard PKCS #10 format certificate requests in either a DER or PEM encoded format (see <http://www.rsasecurity.com/rsalabs/pkcs/> for definition).
6. Process certificate chains of varying length.
7. Controlled access to resources must be based on the authenticated identity of the communicating party. That is, the name of a party as embedded in its digital certificate must be used as one of the attributes that determines access rights. Access control should also be based on the certificate's Policy OID in addition to the embedded name as another attribute determining access rights.
8. Recording an audit trail of all security sensitive events must occur. Audit records must only be available to authorized viewers. Each audit record must minimally contain the name of the communicating party, as embedded in the party's digital certificate, an accurate time-stamp, and whether the attempt was successful or not. When appropriate, additional information such as the Policy OID, and/or the network address of the party should also be included. The events that must be recorded for an audit trail include, but are not limited to:
 - a. Attempts to establish a session.
 - b. Attempts to transfer data to or from the system.
 - c. Attempts to query or change an operating parameter of the application software or the underlying hardware.
 - d. All sent or received messages that bear a digital signature.
 - e. And specifically for RIGs, attempts to login via an attached console.
9. Optionally, interface with a tamper evident cryptographic module that stores the systems secret key and is capable of performing cryptographic functions. The module should minimally conform to FIPS 140-1 level 1 or FIPS 140-2 level 1 or higher standards, depending on the application or device.

Formatted: Bullets and Numbering

 California ISO Your Link to Power	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

10. Demonstrate its capabilities to implement non-repudiation based on the digital certificates of the transacting parties.
11. Use accepted information security industry standard-protocols (e.g., SSL, TLS, and IPSEC) for establishing secure sessions.
12. Sessions must be renegotiated at least every 24 hours with a new symmetric key. The application must initiate the connection and renegotiate during every 24-hour period.

3.2. APPLICATION CONTROL FUNCTION STANDARDS

Every application and its underlying hardware system must adhere to the following control functions:

1. The system must not provide any direct dial-in capabilities. All dial-in access must be provided through officially approved CAISO dial-in servers. Such access is no different from any access to the application; all security functions described under [Subsection 3.1 Application Security Functions](#) apply to all access paths.
2. Systems that allow access via an attached console must minimally do so based on a user ID and password. All login attempts must be audited. Additionally, the system must always *boot-up* to a mode that requires a user ID and a password for console access. That is, it should not be possible to turn off the system, turn it back on again, and gain access to the system without a correct user ID and password. The console password must be different than the factory installed password and must adhere to the procedures described in [CAISO Information Security Standards and Guidelines](#).
3. Systems must disable all Internet application services (e.g., telnet, ftp, etc.) that are not explicitly required. All Internet application services that are required must provide the security functions described under [Subsection 3.1 Application Security Functions](#).

3.3. APPLICATION CONFIGURATION STANDARDS

3.3.1. EXISTING APPLICATIONS COMMUNICATING VIA STANDARD INTERNET APPLICATION PROTOCOLS

All applications that communicate via standard Internet application protocols (e.g., http, ftp, telnet, etc.) must be configured to provide end-to-end security. This is irrespective of whether the communicating parties are in the same subnet or not.

3.3.2. EXISTING APPLICATIONS COMMUNICATING VIA PROPRIETARY APPLICATION PROTOCOLS

Applications that use either proprietary application protocols or utilities industry specific application protocols must be minimally configured to provide site-to-site security. That is, a “site-to-site” implementation employs devices that front-end each side of the proprietary application (i.e., the client side and the server side) and provide security in “proxy mode”.

3.3.3. NEW APPLICATIONS

All new applications communicating with other new applications must be configured to provide end-to-end security. This is regardless of the application protocol and irrespective of whether the communicating parties are in the same subnet or not. New applications must demonstrate their ability to migrate to an integrated solution that fully uses the CAISO PKI. When a new application communicates with an existing application, it must be configured to match the security functionality of the existing application.

 California ISO Your Link to Power	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

3.3.4. EXTERNAL ENTITIES INTERFACING WITH CAISO APPLICATIONS

It is the sole responsibility of the companies interfacing with CAISO to ensure that their applications can communicate with CAISO's application in a secure manner.

3.4. CRYPTOGRAPHIC SECURITY STANDARDS

CUDA-ISO® has established the PKI standards to be used at CAISO. This includes the encryption strength, digital certificate and revocation lists standards, and hardware standards. This includes:

1. All digital certificates will conform to the ITU Recommendation X.509 v 3 standards.
2. Certificate Revocation Lists will conform to X.509 v 2 standards.
3. Cryptographic Hardware Modules must conform to FIPS 140-1/140-2 Level 2 1 or higher.
4. Accepted information security industry standards for establishing secure sessions include, but are not limited to:
 - a. The Secure Socket Layer (SSL) v 3.
 - b. Transport Layer Security (TLS) v 1 (a.k.a. SSL v 3.1)
 - c. Internet Engineering Task Force Standards on IP Security (IPSEC)
5. Adhere to the [CAISO Information Security Standards and Guidelines](#).
6. Adhere to the [CAISO Cryptographic Architecture and Standards](#).

4. ASSURANCE LEVEL SELECTION GUIDELINES

These guidelines will assist the Business Unit Manager, the Project Manager, and the Information Security Manager in selecting the appropriate CUDA-ISO® assurance level for the immediate project.

CAISO's implementation of PKI is called Cryptographic Universal Design Architecture (CUDA-ISO®). The building blocks include a Certificate Policy (CP) and the two Certification Practice Statements (CPS), which are legal documents on how to operate and maintain CUDA-ISO®. The following supports the PKI System:

- Certification Authorities (CAs).
- Registration Authorities (RAs)
- Public and Private Keys.
- Digital Certificates.
- Certificate Revocation Lists (CRL) Service.
- Storage Media for Private Key and Digital Certificates:
 - Cryptographic modules (PCMCIA cards), smart cards, software based.

Information Security has implemented CUDA-ISO® establishing the following levels of assurance, however, the only active levels are currently Basic Assurance (CAISO_Issuing_CA) and Test Assurance (CAISO_Test_CA):

1. The Generator Communication Project (GCP) Assurance level specifically for the Project.
2. High Assurance level (to be instantiated when required).
3. Medium Assurance level.
4. Basic Assurance level.
5. Test or Rudimentary Assurance level specifically for testing.

 California ISO Your Link to Power	Corporate Standards and Guidelines	Review Date: No.	09/10/08 TBD
	Information Security-Cryptography	Version No.:	2.6
Application and CUDA-ISO Integration Standards and Guidelines		Effective Date	09/01/2003

4.1. GCP ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES

This assurance level was originally defined for RIG to EMS communication, however, as of 2008, RIG owners can decide whether they implement more stringent methods of private key protection, such as using a cryptographic module to protect their private keys, or less stringent methods of private key protection, such as storage on the local file system. In either case, all certificates will be issued by the CAISO_Issuing_CA. The CAISO_Issuing_CA is governed by the Basic Assurance CPS.

4.2. HIGH ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES

High Assurance level digital certificates require the use of a cryptographic module, conforming to FIPS 140-2 level 2 or higher. The digital certificate and private key are stored in the cryptographic module establishing the highest degree of confidence that they cannot be compromised.

The project (other than GCP) must require a high level of security due to the criticality and sensitivity of data being transmitted. The data is so critical and sensitive, if the data were prematurely disclosed, modified or made inaccessible, the impact to operations would be catastrophic and could cause severe damage to grid reliability.

Other considerations include, but are not limited to:

- User Community—the number of users should be minimal to maintain effective management of the cryptographic modules.
- Budget—High Assurance certificates will be stored on modules that could add up considerably based on the user community population.
- Non-repudiation—along with confidentiality, integrity and availability, non-repudiation is a future capability ready to be enforced by CUDA-ISO® as applications are modified to use the capability.


CUDA-ISO® has the capability to create a new Certification Authority (CA) for High Assurance if the need arises, and CAISO has maintained its unique OID registered for this policy. The CAISO High Assurance Certification Practice Statement sets forth the requirements for issuing and using X.509 v3 digital certificates and cryptographic modules.

Two certificates should be issued to each communicating entity on separate cryptographic modules, referred to as the primary and backup modules. It is the Connecting Entity's choice whether or not to use a backup module at their site to ensure a reliable connection to CAISO. Each certificate/key pair is valid for one year, at the end of which, re-certification will need to occur in order to continue communication with CAISO. The re-certification process involves both CAISO and Connecting Entity personnel.

For additional detailed technical information, refer to the [CAISO PKI Integration Requirements and Specifications for High Assurance](#), the [CAISO High Assurance CPS](#), and the [CAISO High Assurance SAT Template](#).

4.3. MEDIUM ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES

Medium Assurance level digital certificates require the use of cryptographic modules, which conform to FIPS 140-2 level 1 or higher. These are also known as smart cards. The digital

 California ISO Your Link to Power	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

certificate and private key are stored in a smart card establishing a high degree of confidence that they cannot be compromised.

The project must require a high level of security due to the criticality and sensitivity of data being transmitted. If the data were prematurely disclosed, modified or made inaccessible, the impact to operations would be severe and could cause some damage to grid reliability.

Other considerations include, but are not limited to:

- User Community—the number of users will effect management of the smart cards.
- Budget—Medium Assurance certificates will be stored on modules that could add up considerably based on the user community population.
- Non-repudiation—along with confidentiality, integrity and availability, non-repudiation is a future capability ready to be enforced by CUDA-ISO® as applications are modified to use the capability.

For additional detailed technical information, refer to the [CAISO PKI Integration Requirements and Specifications for Medium Assurance](#), the [CAISO Medium Assurance SAT Template](#), and the [CAISO Medium Assurance CPS](#).

4.4. BASIC ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES


Basic Assurance level digital certificates require the user’s certificate and keys to be stored locally on a system. This may require the use of a browser, which conforms to domestic 128-bit encryption or higher. The digital certificate and private key are stored in a file that is installed into the browser’s database. If the user certificate is not being used in a browser, a version of SSL must be installed with a certificate storage mechanism, or some other appropriate method of certificate storage must be in place. This will provide a reasonable level of confidence that the communications are secured and the identity of the Connecting Entity is accurate.

The project must require a strong level of security due to the sensitivity of data being transmitted. If the data were prematurely disclosed, modified or made inaccessible, operations would be moderately impacted and could cause concerns to grid reliability. This is because test data is generally production grade data, and controlled access to such data is required.

For additional detailed technical information, refer to the [CAISO PKI Integration Requirements and Specifications for Basic Assurance](#), the [CAISO Basic Assurance SAT Template](#), and the [CAISO Basic Assurance CPS](#).

4.5. TEST ASSURANCE LEVEL DEFINITION AND SELECTION GUIDELINES

The Test or Rudimentary Assurance level digital certificates are used for testing purposes only. The digital certificates can be issued in place of any level of assurance required by the project—GCP, High, Medium or Basic. The certificates can be issued for use on systems, smart cards or cryptographic modules based on the project’s needs. The intent is to ensure that the application being enabled to use CUDA-ISO® is successful before going into production. Once in production, it will use the appropriate assurance level as described by its Certification Practice Statement (CPS). Test certificates should be leveraged only in development environments. Production grade certificates are issued for test, staging and production environments. CUDA-ISO® Assurance Level Selection Matrix

 California ISO Your Link to Power	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

This matrix is designed to assist CAISO management decide which assurance level is appropriate for their immediate project. The Manager of Information Security must be involved with the decision making process.

Assurance Level of Certificates and Keys

Security Requirements	Test Assurance	None	Basic Assurance	Medium Assurance	High Assurance	GCP Assurance		
	AGC Control	Testing Only					X	Catastrophic Impact
	High Security	Testing Only				X		Catastrophic Impact
	Medium Security	Testing Only			X			Severe Impact
	Low Security	Testing Only		X				Moderate Impact
	No Security		X					No Impact

Disclosure, Modification, Accessible

As the security requirements increase, so does the impact of premature disclosure, unauthorized modification and the inability to access the data or information. As the security level and impact to operations and grid reliability increases, the assurance level will also increase to maintain a higher level of confidence in the secured communication and the identity of the connecting entity.

The boxes with the “X” show the recommended selection for the project, the gray boxes could also be used with management approval including Information Security, Legal and the Project’s Department. The selection process will be conducted in accordance to this document, but as well as the [CAISO Information Security Policy](#), the [CAISO Cryptographic Architecture and Standards](#), the Assurance Level CPS, the [CAISO Information Classification Standards and Protection Procedures](#), the [CAISO User Access Criteria And Procedures](#) and the [CAISO Information Security Standards and Guidelines](#).

4.5.1. CHANGE OF ASSURANCE LEVEL

CUDA-ISO® was designed and implemented in such a way as to allow the project to change assurance level as its business environment changes. As the environment changes, so does the requirements and specification. CUDA-ISO® is flexible to manage a change of assurance to accommodate the new security requirements. To make a change, the project management team must collaborate with Legal and Information Security to determine the new requirements and justify the changes. The change can be movement to higher assurance level or a lower assurance level. Changing the assurance level will require an evaluation of the application to determine what modifications are required to accommodate the change. This includes, amongst other areas, which client certificate OID (or assurance level), is accepted by the system.

5. COMPLIANCE TEST CRITERIA

5.1. MINIMUM TESTS

 California ISO <small>Your Link to Power</small>	Corporate Standards and Guidelines Information Security-Cryptography	Review Date: No.	09/10/08 TBD
	Application and CUDA-ISO Integration Standards and Guidelines	Version No.: Effective Date	2.6 09/01/2003

Compliance with the CAISO Application and CUDA-ISO® Integration Standards and Guidelines requires that at a minimum the following tests be satisfied:

1. Test that an expired certificate is not honored.
2. Test that a revoked certificate is not honored.
3. Test that the system can minimally generate RSA 1024 bit keys.
4. Test that the system can generate standard PKCS10 formatted certificate requests.
5. Test that the system can validate certificate chains of varying length.
6. Test that all access paths to the application require mutual authentication based on a digital certificate (as feasible).
7. Test that the communicating parties are using accepted information security industry standard protocols.
8. Test that the communication is strongly encrypted with accepted information security industry standard algorithms.
9. Test that the session is renewed at least every 24 hours using a new key pair each time.
10. Test that a session does not last beyond the validity period of a party's certificate (not to exceed 24 hours after expiration).
11. Test that a session is dismantled if a party's certificate is revoked (not to exceed 24 hours after CRL installation containing revoked certificate).
12. Test that an authentic principal cannot access an application resource for which it is not authorized.
13. Test that security sensitive events are logged and can be retrieved. Each record in the log must minimally include the Distinguished Name of the Subject (or Common Name), the Distinguished Name of the Issuer, the Policy OID (if possible), the serial number of the certificate, an accurate timestamp, and if the attempt was successful or not.
14. Test that all messages that bear a digital signature are recorded and can be retrieved.
15. Test that Internet services that are not required for the operation of the system are turned off.
16. Test that the access control mechanism uses the Distinguished Name of the Subject and the Policy OID parameters for enforcing access control rules.
17. Test that access control tables can be configured to allow or deny access rights based on the Distinguished Name of the Subject and the Policy OID.

6. COMPLIANCE

There are no exceptions to these Standards. All affected CASIO personnel must comply with these Standards. Any Business Unit Manager or Director who strongly believes they have a valid technological or compelling business reason for non-compliance with these Standards, in part or in its entirety, must utilize the CAISO Exception Process. The Business Unit Manager or Director with ownership responsibility for the project in question must concur and all the affected Officers must approve the Exception in accordance with the CAISO Exception Process.

Employees affected by these Standards are subject to disciplinary action for failure to comply with its terms, up to and including immediate termination of employment. Consultants and contractors affected by these Standards will be subject to termination of their contracts or requests to remove the individual offender from the CAISO's premises and contract. In addition, all violations may result in the loss of some or all User privileges. Furthermore, some violations may constitute a criminal offense, as outlined in local, state, and federal laws, which CAISO will report to the appropriate authorities.

 California ISO <small>Your Link to Power</small>	Corporate Standards and Guidelines	Review Date: No.	09/10/08 TBD
	Information Security-Cryptography	Version No.:	2.6
Application and CUDA-ISO Integration Standards and Guidelines		Effective Date	09/01/2003

7. REFERENCES

1. Federal Information Processing Standard Publication 140-1, January 1994.
2. ITU Recommendation X.509, Information Technology, Open Systems Interconnection. The Directory: Authentication Framework, ISO/IEC JTC 1/SC 31 N 8696, 28 June 1994.
3. Security Architecture for the Internet Protocol, RFC 1825, August 1995.
4. Secure Socket Layer Version 3.0, Draft RFC, Netscape Communications Corp.
5. Cryptographic Architecture Framework for the California Independent Service Operator Information Security Infrastructure, RFC03-14, April 1998.
6. CAISO Public Key Infrastructure Operational Design, August 1998.
7. CAISO Public Key Infrastructure Gateway Interface Design, August 1998.
8. CAISO Public Key Infrastructure Application Interface Design, August 1998.
9. The Transport Layer Security Protocol Version 1.0, RFC 2246.
10. Federal Information Processing Standard Publication 140-2, October 2001 and May 2002.
11. [CAISO Information Security Standards and Guidelines](#), May 2002.
12. CAISO Cryptographic Architecture and Standards, (under development)

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Deleted: iss

8. APPROVAL

8.1. STANDARDS AND GUIDELINES APPROVAL

These Standards and Guidelines were created under a stakeholder process including CUDA Team-I, CUDA Team-II, Legal, Computer Operations, Market Operations, Grid Operations, Legal, and others. The CAISO Chief Information Officer and the Board of Governors approved CUDA-ISO®.

Responsible Manager:

James W. Sample, Manager of Information Security
 Print Manager's Name and Title

x 5891
 Telephone