The California State University
INFORMATION SECURITY MANAGEMENT

CSU Electronic and Digital Signature Standards and Procedures, 8100.S01

Last Revised: **05/21/2012**

REVISION CONTROL

Document Title:	CSU Digital Signature Standards and Procedures
Author:	Information Security and Identity Access Management
File Reference:	CSU Electronic and Digital Signature Standards.docx

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
N/A	Sheryl Okuno	Original Document - LA	N/A
08/16/2011	Michael Trullinger	Release of New Document	Multiple
09/26/2011	Javier Torner		Multiple
09/27/2011	Mark Hendricks		Multiple
09/29/2011	Michael Trullinger	Review – No Significant Additions	Multiple
11/04/2011	Mark Hendricks		Multiple
11/09/2011	Working Group		Multiple
11/09/2011	Michael Trullinger		Multiple
11/10/2011	Michael Trullinger & Mark Hendricks	Corrections and Revision	Multiple
12/14/2011	Michael Trullinger	Included feedback from ISAC	Multiple
04/27/2012	Michael Trullinger	Feedback from OGC, Risk Management, HRM, Audit	Multiple
05/21/2012	Michael Trullinger	Minor Corrections – 1.0 Release	Multiple

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
Click here to enter Review Date	Click here to enter Reviewer	Click here to enter Reviewed, Recommended or Approved

Table of Contents

Page

Introduction

As organizations move away from paper documents with ink signatures, the ability to sign electronic transactions and documents for business, financial, or other reasons is important, if not essential. There is a considerable amount of confusion surrounding signature technologies, and how they might be used for purposes such as signing an electronic document, signing or encrypting an email, or indicating approval in an electronic workflow process.

These standards and procedures are meant to be referenced by anyone requesting, using, or accepting a CSU approved electronic signature and their intent is to:

- Provide the framework for evaluating the appropriateness of an electronic signature technology for an intended purpose
- Establish a CSU System-wide standard for the management and issuance of "key material" used for digital signatures
- Enable greater adoption of digital signature technology across the CSU to streamline business processes, improve identity proofing processes, and increase information security

The legal definition for electronic signatures has been established in the US Federal Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000 and is very broad. A risk based evaluation using OMB 04, 04 "E-Authentication Guidance for Federal Agencies" and NIST SP800-63 must be performed by an organization to determine risks associated with using an electronic signature method and the quality as well as security of the electronic signature method required.

For many day-to-day cases, a simple electronic signature (generated through an authentication or "click to accept" process) is adequate to indicate that an individual has demonstrated intent to sign or approve a transaction. Others cases will require or prefer use of a digital signature.

A digital signature is a very specific form of an electronic signature which uses cryptography to establish the authenticity and validity of the signature with much greater certainty. A digital signature may be utilized where an electronic signature is required. For transactions where there is a greater risk to the CSU, or where a "wet" signature is typically required, digital signatures must be used instead of a simple electronic signature.

Entities Affected

These standards and procedures apply to all members of the CSU community and govern all applications of digital signatures used to conduct official University business. They also apply to transactions between the CSU and other parties.

1.0 Electronic and Digital Signature Definition

An ***electronic signature*** is an electronic sound (e.g., audio files of a person's voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record (ESIGN Act of 2000). A digitally reproduced (e.g. scanned) physical signature is a common example.

A ***digital signature*** is the cryptographic transformation of data, which when added to a message, allows the recipient to verify the signer and whether the initial message has been altered or the signature forged since the

transformation was made. A digital signature is an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a handwritten signature.

Electronic signatures issued by the CSU are considered property of the CSU and are for University business only. Private keys used for digital signatures are considered 'Level 1' confidential data whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damages to the CSU, its students, its employees, or its customers.

2.0 Electronic and Digital Signature Legality

Under California law, a digital signature has the same force and effect as a manual signature. A digital signature may be affixed to any written communication with the University in which a signature is required so long as it complies with the requirements of California Government Code section 16.5 and these Standards and Procedures.

The legality and enforceability of a signature are typically evaluated based on the answer to the following questions:

- Does a signature represent the intent of the signatory?
- Could the statement have been altered?
- How certain is the signatory's identity?

Simple Electronic Signatures may convey the intent of an individual to sign and are often easier to implement, but usually cannot provide satisfactory assurance if authentication, non-repudiation, and integrity are legally required. Determining appropriateness of an electronic signature type (e.g. digital signatures using PKI or a simpler electronic signature) is based on level of risk. A higher assurance level signature may be required for enforceability.

3.0 Reasons for Applying a Digital Signature

The most common reasons for applying a digital signature are authentication, integrity, and non-repudiation.

Authentication

Digital signatures can be used to authenticate the source of messages, documents, and digital content. When ownership of a digital signature secret is known to a specific person only, the digital signature created by that secret can be used to validate authenticity of a person's digital signature.

Integrity

A recipient may need confidence that content they have received has not been altered during transmission. Although encryption technology can be used to secure transmissions, it does not guarantee that the content being protected has not been changed without the author's knowledge. The integrity of authorship of digitally signed content is maintained with or without encryption, as long as the process used to create, store, or retrieve the digitally signed content does not permit content to be changed without invalidating (and where appropriate removing) the signature.

Non-repudiation

Digital signatures can provide non-repudiation. Non-repudiation means that signatories cannot successfully claim they did not sign a message while concurrently claiming that the secret part remained solely in their possession. Some non-repudiation practices include a time stamp for the digital signature that can be used to determine signature validity when the date and time of a compromised secret can be determined.

4.0 General Standards and Requirements

A digital signature is based on an asymmetric cryptosystem that uses a mathematical formula to scramble content. With use of appropriate technology, signatories can encrypt (scramble) content, and recipients can decrypt (unscramble) and verify it. To affix a digital signature or scramble electronic content, a signatory must obtain a digital signature from an accepted authority which typically consists of an electronic asymmetric key-pair (includes a private (secret) key and publicly distributable key).

For a digital signature to be considered valid, it must be:

- Capable of verification
- Linked to content in such a manner that if the content is changed, the digital signature is invalidated (and where appropriate and necessary, removed).
- In conformity with Title 2, Division 7, Chapter 10, of the California Code of Regulations
- Issued by an authority

5.0 Acceptable Use

Electronic and digital signatures are permissible for many record types and activities. Digital Certificates, specifically, can be issued for the purposes of authentication, signing and securing e-mail messages or electronic documents, and encrypting content. Procedures used for issuing certificates that will be used to encrypt sensitive documents and data, including S/MIME email messages, should be carefully developed after assessing retention requirements since key backup and/or escrowing may be necessary to decrypt the source content. If a Digital Certificate is issued for authentication and signing only, key backup and escrow may be unnecessary.

5.1 Agreement to Conduct Electronic Transactions

Digital signatures may be used for transactions between the campus, the Chancellor's Office, and outside parties only when the parties have agreed to conduct transactions by electronic means. The party's agreement to conduct transactions electronically may be informal or recognized through a contract, including cases where a party's action indicates agreement.

5.2 Signature Required by University Policy

When a CSU or campus policy requires that a record have the signature of a responsible person, that requirement can be met if the associated digital signature was issued and is maintained using an approved digital signature method and procedure.

5.3 Signature Required by Law

When an authorized representative of a CSU campus uses an approved digital signature method for a signing required by a third party, the CSU will consider the valid digital signature as having met the requirement.

6.0 Risk-based Approach for Determining Appropriate Electronic Signature Type

Individuals and organizations within the CSU wanting to use electronic signatures must conduct a thorough review of associated risks and must select the appropriate, approved technology. OMB 04-04, FIPS 199, and NIST 800-64 provide mechanisms to establish risk and consequences for business processes.

6.1 Level of Assurance for Authentication Definitions

Electronic authentication is the process of establishing confidence in user identities electronically presented to an information system (NIST SP800-63). "Level of Assurance" is the structure used by the CSU to define the technical and procedural practices to determine authentication certainty.

6.2 Determining Risk

OMB 04-04 "E-Authentication Guidance for Federal Agencies" defines four levels of identity authentication, their associated technical requirements, and risk assessment criteria for determining the impact of authentication errors. In their simplest terms, they are:

- **Level 1**: Little or no confidence in the asserted identity's validity.
- **Level 2**: Some confidence in the asserted identity's validity.
- **Level 3**: High confidence in the asserted identity's validity.
- **Level 4**: Very high confidence in the asserted identity's validity.

OMB 04-04 also identifies six potential impact categories for authentication errors:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Impact values assigned by OMB for these categories of harm are defined in Federal Information Processing Standard 199, "Standard for Security Categorization of Federal Information and Information Systems."

Impact Values (FIPS 199)

- **Low**: The loss of confidentiality, integrity and availability could be expected to have a limited adverse effect on organizational operations, organization assets or individuals.
- **Moderate**: The loss of confidentiality, integrity and availability could be expected to have a serious adverse effect on organizational operations, organization assets or individuals.

- **High**: The loss of confidentiality, integrity and availability could be expected to have a severe or catastrophic adverse affect on organizational operations, organization assets or individuals.

Potential Impact of Financial Loss

- **Low**: at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- **Moderate**: at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High**: severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

Table 1 *– Maximum Potential Impacts for Each Assurance Level*

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	L	M	M	H
Financial loss or agency liability	L	M	M	H
Harm to agency programs or public interests		L	M	H
Unauthorized release of sensitive information		L	M	H
Personal Safety			L	M-H
Civil or criminal violations		L	M	H

NIST 800-63 Electronic Authentication Guideline provides technical requirements for each of the authentication levels of assurance defined in OMB 04-04. Each assurance level has defined controls for identity proofing, token (secret) requirements, and authentication/assertion protection mechanisms as published in NIST 800-63.

7.0 Evaluation Process for Use of Electronic Signature

7.1 Evaluation of Risk

An evaluation must first be performed by the authoritative Operational Unit to determine risks associated with using an electronic signature, including the quality, security, and method required for a given type of content or document. This evaluation process should use the E-Authentication Guidance for Federal Agencies, OMB 04-04 for reference and guidance. The results of that assessment must be documented and included with the official record of approval and any proposals submitted to the record custodian.

7.2 Determination of Electonic Signature Methodology

The electronic signature type selected for a document, content, method, or business process should be commensurate to the assurances needed to mitigate the identified risks. Additionally, specifications for recording, documenting, and/or auditing the electronic signature as required for non-repudiation and other legal requirements shall also be determined by the authoritative operational unit. The lowest cost and least complex method for mitigating risk are generally acceptable. The *National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines* publication (referenced in this document) should be consulted when making this determination.

7.3 Use of "Lower Assurance" Electronic Signature Methods

Operational Units that propose electronic signature methods that are at a lower level of assurance than indicated in the risk assessment process shall:

- Describe the reason for variance
- Identify the potential risk of using a tool from a lower assurance level than the risk assessment identifies
- Justify why a lower assurance level method is appropriate
- Identify the steps that will be taken to mitigate the risk
- Obtain the signed approval of the operational unit director and include it with the official record approving use of an electronic signature method

8.0 Acceptable Forms of Electronic Signatures

8.1 Electronic Forms

The selection of an option (e.g. tick box or button) on an electronic form to indicate agreement can be used as a replacement for written signatures when the appropriate functional requirements are met and the technology used records:

- Intent of agreement
- Information that clearly identifies (e.g. by recording the login username) the individual who has 'signed' the agreement
- Within an auditable trail that the form was signed

Furthermore, the signatory's identity must be accessible for the length of the retention period required for the form, as set out in the CSU or Campus Records Retention Schedule. The technology used should also restrict the form once 'signed' such that the contents of the form cannot be changed without the signature being invalidated.

8.2 Scanned Image of a Handwritten Signature

A scanned image of a handwritten signature can be used as an equivalent to a written signature if signing internal CSU data when the appropriate security requirements have been met. Scanned images of a signature must only be used where express permission has been granted by the author and is considered acceptable for high volume processes such as mass mailings. Given the ease with which images may be manipulated, images without other forms of authenticity should be used for **low risk transactions only.**

8.3 Authorization by Email

Acceptance or agreement of intent through an official, controlled Email system (e.g. receipt of an email through the University email system) may be used when the appropriate functional requirements, risk, and security have been carefully considered. Given the ease with which emails may be manipulated, email receipts without other forms of authenticity should only be used for **low risk transactions** and may not be accepted from "generic or shared" email accounts unless the appropriate controls are in place to establish the actual sender.

9.0 Acceptable Forms of Digital Signatures

For a digital signature to be valid it must be created by a technology accepted for use by the State of California and that has been adopted by the CSU. Acceptable California State technologies currently include public key cryptography and signature dynamics. The most common technology used is public key cryptography. It has a greater degree of verifiability than signature dynamics, does not require the additional handwriting analysis steps of signature dynamics, and is *the only technology accepted by the CSU*.

9.1 Public Key Cryptography

Public Key Cryptography

Public Key Cryptography (PKC) signatures allow for third party verification of a signature and are affixed to electronic content using software enhancements to existing applications and web browsers. PKC signatures accepted by the CSU must be issued through a Public Key Infrastructure (PKI) scheme and which results in an asymmetrical digital certificate.

9.2 Encryption

Custodians or users of institutional administrative data who deploy personal digital certificates for encryption must establish procedures ensuring that the CSU has access to all such records and data. Each major operating unit deploying personal digital certificates for encryption is required to implement procedures to archive, secure, and utilize “master recovery keys”.

Any custodian or user of institutional administrative data who deploys software or algorithmic programs to encrypt data is required to inform his or her supervisor prior to deployment and disclose, in a comprehensible form, the keys or other means to access the data.

10.0 Digital Certificates

10.1 Minimum Requirements

For a digital certificate to be considered valid, it must follow California State requirements and:

- Identify the issuing Certificate Authority (CA) that has been authorized by the California Secretary of State.
- Uniquely identify its subscriber
- Include its subscriber's public key
- Identify its operational period
- Be comparable against a well-known Certificate Revocation List (CRL) to confirm its validity
- Be digitally signed by the issuing CA

10.2 Approved Authorities

A *Certificate Authority* is commonly a well-known, third party entity that is entrusted to issue digital certificates, verify matching of pubic keys to identity information, and provide a current revocation list. A Certificate Authority, or their delegates, has the responsibility to verify the identity of a subscriber before issuing a certificate.

California State

The list of approved California State authorities is currently available at:

http//www.sos.ca.gov/digsig/

California State University System

The CSU has adopted the InCommon Client Certificate Service as a preferred vendor for PKI digital signature certificates. The California Secretary of State has approved and included this CA in their list under their root name, "COMODO Ltd".

11.0 Issuance and Maintenance

Individuals and organizations within the CSU that want to use electronic signatures must conduct a thorough review of associated risks and must select the appropriate approved technology. OMB 04-04, FIPS 199, and NIST 800-64 provide mechanisms to establish risk and consequences for business processes. If the decision to use digital signature certificates is made, the appropriate validation type must also be selected.

InCommon Digital Certificate Validation Types

A **Standard Validation** type certificate may be issued to an individual whose campus identity meet both Federal NIST Level 1 requirements and these additional requirements:

- Has a valid I-9 Employment Eligibility Verification form or comparable form on record with the issuing campus.
- Has an electronic credential* provided by the campus that can be uniquely matched to the individual's valid I-9 record or comparable form
- Was issued in such a way that ensures and maintains:
  - Single ownership and use of the credential
  - Distribution which ties the unique electronic credential to the individual who submitted the associated I-9 record or comparable form

When met, a digital certificate may be issued through automated processes using that electronic credential*. Standard validation certificates are currently available for employees only.

A **High Validation** type certificate may be issued to an individual whose campus identity verification processes meet Federal NIST Level 3 requirements as well as requirements for issuance of a Standard Validation type certificate. High Validation certificates may not be issued through an automated process.

12.0 Registration

Registration is the process by which an individual or server identifies and authenticates itself before a digital certificate can be obtained. Applications and servers that require the ability to electronically sign a transaction may be issued a certificate through a designated data steward. Data stewards must submit documentation that includes a description of ongoing system administration and maintenance practices, system access controls procedures, event logging configurations, and security incident response procedures prior to issuance.

12.1 Duration and Expiration

All digital signatures must contain an expiration date. It is recommended that the expiration date not exceed one year from the date of original issue or date of last renewal and may not exceed 3 years.

12.2 Revocation

When a signature is issued, it is expected to be in use for its entire validity period; however, circumstances may require it to be invalidated sooner. Revocation may be requested by the subscriber, a Data Steward, or Information Security under the following conditions:

- The individual who was issued the signature has undergone a name change
- There is a reason to believe that the secret portion of the signature or the storage of it has been compromised
- There is substantive reason to believe that misuse has occurred or is likely to occur
- There is reason to believe the signature is not being used in compliance with these standards
- Related security concerns were identified during an audit
- The subscriber's relationship with the issuing campus has been discontinued
- The minimum requirements for the issued signature are no longer met by the subscriber

13.0 Storage and Protection

13.1 Escrow

The purpose of escrowing electronic signatures or portions of them is to provide access to institutional administrative data by ensuring that access does not become dependent on a single individual or an obscure method of storing and/or protecting them. Signatures or portions of them used for encrypting content require escrowing. Escrowing of private keys for digital signatures must be maintained by the Certificate Authority (CA) issuing the keys.

13.2 Key Recovery

Campuses must develop procedures for retrieval of escrowed materials, such as private keys.

Campus Key recovery procedures should include the following:

- Formal process for logging key recovery and approval
- Key recovery authorization should include at least one campus official. For instance; Key recovery may be approved by the appropriate Data Steward and the campus Information Security Officer.

13.3 User Device Storage

Certificates issued for low to medium risk application may be installed in desktop applications such as email clients and web browsers. High Risk/Level of Assurance certificates must be stored in FIPS 140 approved trusted cryptographic devices such as a smartcard or e-Token device. Private keys are CSU Level 1 data and must be protected via encryption.

13.4 Retention

Record Retention

Electronic signature archives and system activity logs must be retained in accordance with CSU Records Retention policies. Record retention schedules should be updated to reflect the use of electronic and digital signatures, as well as encryption.

The minimum record retention period for registration data for digital certificates is seven years and six months beyond the expiration (or revocation, whichever is later). All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

13.5 Recovery, Including Disasters

Campuses and the Chancellor's Office must develop procedures for business continuity and disaster recovery of master recovery keys.

14.0 Roles and Responsibilities

14.1 Digital Signature Subscriber

A subscriber is the individual who has been provided a digital signature certificate for the purpose of signing. The subscriber is responsible for:

- Providing accurate information when applying for a digital certificate
- Taking reasonable precautions to protect and not share the secret portion of the digital certificate (e.g. storing a certificate private key in a password-protected container), ensuring that the digital certificate is under their sole control
- Using the digital certificate only for authorized, legal and University purposes
- Providing written notification to campus Information Security immediately if the secret portion of the signature is believed to have been compromised
- Using their digital certificate for authorized purposes
- Renewal of expired certificates

14.2 Certificate Administration

Certificate administrators are the parties responsible for management of certificate infrastructure, up to and including those responsible for issuance and distribution of digital certificates. The parties are responsible for:

Certificate Authority

- Adequately and safely storing backup copies of all files necessary to re-establish and operate the Certificate Authority
- Timely publication of certificates and revocation information

System

- Protection of escrowed materials, and institutional escrow keys required for certificate retrieval
- Delegation of authority to issue certificates

Issuance and Distribution

- Notification of issuance of a certificate to the subscriber who is the subject of the certificate
- Notification of issuance of a certificate to others than the subject of the certificate

14.3 Data Steward

Data stewards are the individual(s) responsible for a segment of institutional data. Data stewards are responsible for the following as it relates to digital signatures of content germane to their duties:

- Physical and electronic security of any signed data
- Evaluation of transactions enabled by digital signature
- Seeking approval for use of a digital signature from University Legal Counsel or Information Security
- Seeking technical advice from Information Technology Services
- Acknowledgement of applicable liability caps and warranties
- Digital signature verification

14.4 Campus and Chancellor's Office

CSU Campuses, and likewise the CSU Chancellor's Office, is responsible for maintaining operational and business practices in accordance with these standards and procedures.

14.5 University Legal Counsel

University Legal Counsel may be requested to review and potentially approved the proposed use of a digital signature to determine if it is legally permitted.

14.6 Information Security Office

The Information Security Office is responsible for providing security guidance and for assisting in the auditing process, where assigned. The responsibilities may include and are not limited to:

- Reviewing the digital signature uses and providing recommendations to Data Stewards and the campus Vice President for Administration, including evaluation of associated risks
- Assuring proper issuance and maintenance of campus procedures and subscriber credentials
- Notifying a Certificate Administration and Data Stewards within 24 hours of suspected compromises
- Reviewing digital signature implementations and conducting and documenting periodic audits of those implementations at least every three years
- Providing assistance to develop new (or refine existing) campus practices and procedures to ensure protection of digital signatures and their appropriate use
- Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended
- Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended

14.7 Campus Vice President for Administration

The Vice President for Administration is responsible for delegating campus electronic and digital signature review and audit responsibilities. Final approval or dismissal of campus use of a digital signature is at the Vice President

for Administration's discretion. Determination of approval or dismissal for specific uses may also be made after a review has been conducted by the appropriate data steward.

15.0 Appendix A: Definitions

#	Term	Definition
1.	**Approved Certification Authorities**	The list of certification authorities approved to issue certificates for digital signatures.
2.	**Asymmetric Cryptosystem**	A computer algorithm or series of algorithms which utilize two different keys with the following characteristics • one key signs or decrypts content; • one key verifies or encrypts content; and, • the keys have the property that, even when one key is known, it is computationally infeasible to discover the other key.
3.	**Asymmetric Key-Pair**	A private key and its corresponding public key in an asymmetric cryptosystem. Public keys can be used to verify a digital signature created with the corresponding private key and to encrypt content.
4.	**Certificate Authority**	A person or entity that issues a certificate and certifies amendments to an existing certificate.
5.	**Compromised**	
6.	**Digital Certificate**	Also known as a public key certificate or identity certificate, a digital certificate is an electronic document which uses a digital signature to bind a public key with an identity, such as the name of a person or an organization and address. The certificate can be used to verify that a public key belongs to a person.
7.	**Digital Signature**	A *digital signature* is the cryptographic transformation of data, which when added to content, allows the recipient to authenticate the signatory and whether the content has been altered or the signature forged since the transformation was made.
8.	**Data Steward**	An individual who is responsible for the maintenance and protection of data. The duties include but are not limited to performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in CSU/campus security policies and standards.
9.	**Electronic Credential**	Digital documents or identifiers that are bound to a natural person's identity for the purposes of authentication.
10.	**Electronic Signature**	Any electronic data that carries the intent of a signature (not all electronic signatures use digital signatures).
11.	**Level 1 Confidential Data**	Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.
12.	**Master Recovery Key**	
13.	**Private Key**	The secret key of a key pair used to create a digital signature or decrypt data.
14.	**Public Key**	The well-known key of a key pair used to verify a digital signature or to encrypt data.
15.	**Public Key Cryptography**	An encryption method that uses an asymmetric key-pair.
16.	**Signature Dynamics**	A measurement of the way a person writes his or her signature by hand on a flat surface, binding the measurements to a message through the use of cryptographic techniques.
17.	**Sole Control**	
18.	**Subscriber**	An individual or organization that has been provided one or more digital documents or

#	Term	Definition
		identifiers (username, certificate) from an issuing authority.

Appendix B: Contacts

For questions regarding this standard, contact:

CO Manager:
Mr. Mark Crase
Chief Technology Officer, Cyberinfrastructure Services
CSU Office of the Chancellor
mcrase@calstate.edu

Subject Matter Experts:

Mr. Michael Trullinger
Associate Director, Identity and Access Management
CSU Office of the Chancellor
mtrullinger@calstate.edu

Javier Torner, Ph.D.
Information Security Officer & Interim Associate Vice President, IRT
CSU San Bernardino
jtorner@csusb.edu

Appendix C: Applicable Federal and State Laws and Regulations

State	Title
California Civil Code, Division 3, Part 2, Title 2.5 §1633.1 – 1633.17	**California Uniform Electronic Transactions Act (UETA)** http//www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1633.1-1633.17 This Act facilitates electronic transactions consistent with other applicable law and specifies consistent practices concerning electronic transactions.
California Code of Regulations, Title 2, Division 7, Chapter 10	**Digital Signatures** http//www.sos.ca.gov/digsig/digital-signature-regulations.htm This regulation describes acceptable technology for digital signatures.
U.S.C. section 7001	**Electronic Signatures in Global and National Commerce Act of 2000** http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
California Government Code, Section 16.5	**Digital Signatures** http://www.sos.ca.gov/digsig/code-section-16-5.htm

Appendix D: Other Resources and Related Documentation

ID / Control #	Title
Integrated CSU Administrative Manual Section General Accounting 3701.01	**Digital Signatures** http//www.calstate.edu/icsuam/sections/3000/3701.01.shtml This document specifies the requirements for the use of digital signatures in lieu of handwritten signatures.
CSU Executive Order No. 1031	**Executive Order No. 1031:** System-wide Records/Information Retention and Disposition Schedules Implementation http//www.calstate.edu/EO/EO-1031.html This document ensures compliance with legal and regulatory requirements and best practices of records/information retention and disposition.
CSU Information Security Policy	**The California State University Information Security Policy** http//www.calstate.edu/icsuam/sections/8000/8000.0.shtml
Pending	**The California State University Information Security Standards** http://www.calstate.edu/ This document specifies CSU information security standards.
InCommon	**InCommon Client Certificate Service Overview** https://www.incommon.org/cert/clientcerts.html