State of California
Office of Administrative Law

In re:
Secretary of State

Regulatory Action:

Title 02, California Code of Regulations

Amend sections: 22000, 22002, 22003, 22005
Repeal section: 22004

NOTICE OF APPROVAL OF CERTIFICATE OF COMPLIANCE

Government Code Sections 11349.1 and 11349.6(d)

OAL Matter Number: 2021-0105-03

OAL Matter Type: Certificate of Compliance (C)

This certificate of compliance makes permanent emergency action no. 2020-0415-02E, which replaced the existing Approved List of Digital Signature Certification Authorities with the requirement that public entities only accept certificates from authorities recognized by at least one of the three certificate programs identified in the proposed regulations.

OAL approves this regulatory action pursuant to section 11349.6(d) of the Government Code.

Date: February 17, 2021

Eric Partington
Senior Attorney

For: Kenneth J. Pogue
Director

Original: Alex Padilla, Secretary of State
Copy: Taylor Kayatta

STATE OF CALIFORNIA--OFFICE OF ADMINISTRATIVE LAW

NOTICE PUBLICATION/REGULATIONS SUBMISSION

CERT

STD. 400 (REV. 10/2019)

(See instructions on reverse)

For use by Secretary of State only

OAL FILE NUMBERS	NOTICE FILE NUMBER	REGULATORY ACTION NUMBER	EMERGENCY NUMBER
	Z-2020-1030-02	2021-0105-03C	

For use by Office of Administrative Law (OAL) only

2021 JAN -5 P 4:21

OFFICE OF ADMINISTRATIVE LAW

NOTICE

REGULATIONS

ENDORSED - FILED
In the office of the Secretary of State
of the State of California

FEB 17 2021
1:21 P.M.

AGENCY WITH RULEMAKING AUTHORITY: Secretary of State

AGENCY FILE NUMBER (If any):

A. PUBLICATION OF NOTICE (Complete for publication in Notice Register)

1. SUBJECT OF NOTICE	TITLE(S)	FIRST SECTION AFFECTED	2. REQUESTED PUBLICATION DATE

3. NOTICE TYPE	4. AGENCY CONTACT PERSON	TELEPHONE NUMBER	FAX NUMBER (Optional)
☐ Notice re Proposed Regulatory Action ☐ Other			

OAL USE ONLY	ACTION ON PROPOSED NOTICE	NOTICE REGISTER NUMBER	PUBLICATION DATE
	☐ Approved as Submitted ☐ Approved as Modified ☐ Disapproved/ Withdrawn	2020, 46-Z	11/13/2020

B. SUBMISSION OF REGULATIONS (Complete when submitting regulations)

1a. SUBJECT OF REGULATION(S): Digital Signatures

1b. ALL PREVIOUS RELATED OAL REGULATORY ACTION NUMBER(S): 2020-0415-02E

2. SPECIFY CALIFORNIA CODE OF REGULATIONS TITLE(S) AND SECTION(S) **(Including title 26, if toxics related)**

SECTION(S) AFFECTED (List all section number(s) individually. Attach additional sheet if needed.)

ADOPT:

AMEND: 22000, 22002, 22003, 22005

TITLE(S): 2

REPEAL: 22004

3. TYPE OF FILING

- ☐ Regular Rulemaking (Gov. Code §11346)
- ☐ Resubmittal of disapproved or withdrawn nonemergency filing (Gov. Code §§11349.3, 11349.4)
- ☐ Emergency (Gov. Code, §11346.1(b))
- ☒ Certificate of Compliance: The agency officer named below certifies that this agency complied with the provisions of Gov. Code §§11346.2-11347.3 either before the emergency regulation was adopted or within the time period required by statute.
- ☐ Resubmittal of disapproved or withdrawn emergency filing (Gov. Code, §11346.1)
- ☐ Emergency Readopt (Gov. Code, §11346.1(h))
- ☐ File & Print
- ☐ Other (Specify)
- ☐ Changes Without Regulatory Effect (Cal. Code Regs., title 1, §100)
- ☐ Print Only

4. ALL BEGINNING AND ENDING DATES OF AVAILABILITY OF MODIFIED REGULATIONS AND/OR MATERIAL ADDED TO THE RULEMAKING FILE (Cal. Code Regs. title 1, §44 and Gov. Code §11347.1)

5. EFFECTIVE DATE OF CHANGES (Gov. Code, §§ 11343.4, 11346.1(d); Cal. Code Regs., title 1, §100)

- ☐ Effective January 1, April 1, July 1, or October 1 (Gov. Code §11343.4(a))
- ☒ Effective on filing with Secretary of State
- ☐ §100 Changes Without Regulatory Effect
- ☐ Effective other (Specify)

6. CHECK IF THESE REGULATIONS REQUIRE NOTICE TO, OR REVIEW, CONSULTATION, APPROVAL OR CONCURRENCE BY, ANOTHER AGENCY OR ENTITY

- ☒ Department of Finance (Form STD. 399) (SAM §6660) per DOF request
- ☐ Fair Political Practices Commission
- ☐ State Fire Marshal
- ☐ Other (Specify)

7. CONTACT PERSON	TELEPHONE NUMBER	FAX NUMBER (Optional)	E-MAIL ADDRESS (Optional)
Taylor Kayatta	(916) 695-1530		tkayatta@sos.ca.gov

8. I certify that the attached copy of the regulation(s) is a true and correct copy of the regulation(s) identified on this form, that the information specified on this form is true and correct, and that I am the head of the agency taking this action, or a designee of the head of the agency, and am authorized to make this certification.

SIGNATURE OF AGENCY HEAD OR DESIGNEE: Susan Lapsley, Deputy SOS — DATE: 1/4/2021

TYPED NAME AND TITLE OF SIGNATORY: Susan Lapsley, Deputy Secretary of State

For use by Office of Administrative Law (OAL) only

ENDORSED APPROVED

FEB 17 2021

Office of Administrative Law

California Secretary of State
Regulatory Action: Digital Signatures
Proposed Regulation Text (Certificate of Compliance)

Title 2. Administration
Division 7. Secretary of State
Chapter 10. Digital Signatures

The California Secretary of State is proposing to make permanent the temporary emergency regulations related to Sections 22000, 22002, 22003, 22004, and 22005. Those emergency regulations are effective as of April 22, 2020. Changes to the emergency regulations are shown in strikethrough and underline, with eliminated text struck and new text underlined.

22000. Definitions.

(a) For purposes of this chapter, and unless the context expressly indicates otherwise:
(1) "Digitally signed communication" is a message that has been processed by an acceptable technology, pursuant to section 23003, in such a manner that ties the message to the signer.
(2) "Message" means a digital representation of information intended to serve as a written communication provided to a public entity by a public entity or a private entity.
(3) "Person" means a human being or any organization capable of signing a document, either legally or as a matter of fact.
(4) "Public entity" means the public entity as defined by California Government Code Section 811.2.
(5) "Signer" means the person who signs a digitally signed communication with the use of an acceptable technology to uniquely link the message with the person sending it.
(6) "Technology" means the computer hardware- and/or software-based method or process used to create digital signatures.

Note: Authority cited: Section 16.5, Government Code. Reference: Section 16.5, Government Code.

22002. Criteria for State to Determine if a Digital Signature Technology is Acceptable for Use by Public Entities.

(a) An acceptable technology must be capable of creating signatures that conform to requirements set forth in California Government Code Section 16.5, specifically:
(1) It is unique to the person using it;
(2) It is capable of verification;
(3) It is under the sole control of the person using it;
(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and
(5) It conforms to Title 2, Division 7, Chapter 10 of the California Code of Regulations.

Note: Authority cited: Section 16.5, Government Code. Reference: Section 16.5, Government Code.

22003. Acceptable Technologies.

(a) The technology known as Public Key Cryptography is an acceptable technology for use by public entities in California, provided that the digital signature is created consistent with the following provisions:

(1) Definitions. For purposes of section 22003(a), and unless the context expressly indicates otherwise:

(A) "Asymmetric cryptosystem" means a computer algorithm or series of algorithms which utilize two different keys with the following characteristics:

(i) One key signs a given message;

(ii) One key verifies a given message; and

(iii) The keys have the property that, knowing one key, it is computationally infeasible to discover the other key.

(B) "Certificate" means a computer-based record which:

(i) Identifies the certification authority issuing it;

(ii) Names or identifies its subscriber;

(iii) Contains the subscriber's public key;

(iv) Is digitally signed by the certification authority issuing or amending it; and

(v) Conforms to widely used industry standards, including, but not limited to, ISO x.509 and PGP certificate standards.

(C) "Certification Authority" means a person or entity that issues a certificate, or in the case of certain certification processes, certifies amendments to an existing certificate.

(D) "Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem. The keys have the property that the public key can verify a digital signature that the private key creates.

(E) "Practice statement" means documentation of the practices, procedures and controls employed by a Certification Authority.

(F) "Private key" means the key of a key pair used to create a digital signature.

(G) "Proof of Identification" means the document or documents presented to a Certification Authority to establish the identity of a subscriber.

(H) "Public key" means the key of a key pair used to verify a digital signature.

(I) "Subscriber" means a person who:

(i) Is the subject listed in a certificate;

(ii) Accepts the certificate; and

(iii) Holds a private key which corresponds to a public key listed in that certificate.

(2) California Government Code Section 16.5 requires that a digital signature be 'unique to the person using it.' A public key-based digital signature may be considered unique to the person using it if:

(A) The private key used to create the signature on the document is known only to the signer;

(B) The digital signature is created when a person runs a message through a one-way function, creating a message digest, then encrypting the resulting message digest using an asymmetrical cryptosystem and the signer's private key;

(C) Although not all digitally signed communications will require the signer to obtain a certificate, the signer is capable of being issued a certificate to certify that he or she controls the key pair used to create the signature; and

(D) It is computationally infeasible to derive the private key from knowledge of the public key.

(3) California Government Code Section 16.5 requires that a digital signature be 'capable of verification.' A public key-based digital signature is capable of verification if:

(A) The acceptor of the digitally signed document can verify the document was digitally signed by using the signer's public key to decrypt the message; and

(B) If a certificate is a required component of a transaction with a public agency, the issuing Certification Authority, either through a certification practice statement or through the content of the certificate itself, must identify which, if any, form(s) of identification it required of the signer prior to issuing the certificate.

(4) California Government Code Section 16.5 requires that the digital signature remain 'under the sole control of the person using it.' Whether a signature is accompanied by a certificate or not, the person who holds the key pair, or the subscriber identified in the certificate, assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature pursuant to California Evidence Code Section 669.

(5) The digital signature must be linked to the message of the document in such a way that if the data are changed, the digital signature is invalidated.

(6) If the signature is accompanied by a certificate, the certificate is from a Certification Authority that, at the time of signing, is included in at least one of the following third-party certificate program lists:

(A) Apple Root Certificate Program

(B) Microsoft Trusted Root Program

(C) Mozilla Root Program

(b) The technology known as "Signature Dynamics" is an acceptable technology for use by public entities in California, provided that the signature is created consistent with the following provisions:

(1) Definitions. For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:

(A) "Handwriting Measurements" means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.

(B) "Signature Digest" is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

(C) "Expert" means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to California Evidence Code Section 720.

(D) "Signature Dynamics" means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

(2) California Government Code Section 16.5 requires that a digital signatures be 'unique to the person using it.' A signature digest produced by Signature Dynamics technology may be considered unique to the person using it if:

(A) The signature digest records the handwriting measurements of the person signing the document using signature dynamics technology;
(B) The signature digest is cryptographically bound to the handwriting measurements; and
(C) After the signature digest has been bound to the handwriting measurements, it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

(3) California Government Code Section 16.5 requires that a digital signature be 'capable of verification.' A signature digest produced by signature dynamics technology is capable of verification if:
(A) The acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison; and
(B) If signature verification is a required component of a transaction with a public entity, the handwriting measurements can allow an expert handwriting and document examiner to assess the authenticity of a signature.

(4) California Government Code Section 16.5 requires that a digital signature remain 'under the sole control of the person using it.' A signature digest is under the sole control of the person using it if:
(A) The signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message; and
(B) The signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

(5) The signature digest produced by signature dynamics technology must be linked to the message in such a way that if the data in the message are changed, the signature digest is invalidated.

Note: Authority cited: Section 16.5, Government Code. Reference: Section 16.5, Government Code.

22004. REPEALED.

22005. Criteria for Public Entities to Use in Accepting Digital Signatures.

(a) Prior to accepting a digital signature, public entities shall ensure that the level of security used to identify the signer of a document is sufficient for the transaction being conducted.
(b) Prior to accepting a digital signature, public entities shall ensure that the level of security used to transmit the signature is sufficient for the transaction being conducted.
(c) If a certificate is a required component of a digital signature transaction, public entities shall ensure that the certificate format used by the signer is sufficient for the security and interoperability needs of the public entity.
(d) Prior to accepting a digital signature, public entities shall ensure that it is created by an acceptable technology pursuant to section 22003.

Note: Authority cited: Section 16.5, Government Code. Reference: Section 16.5, Government Code.