California Secretary of State
Regulatory Action: Digital Signatures
Proposed Regulation Text

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

The California Secretary of State is proposing to amend the following existing regulations: Sections 22000, 22002, 22003, and 22005. The California Secretary of State is also proposing to repeal the following existing regulation: Section 22004. Changes to existing, permanent regulation text 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 ~~a computer~~an acceptable technology, pursuant to section 23003, in such a manner that ties the message to the ~~individual that signed the message~~signer.
(2) "Message" means a digital representation of information intended to serve as a written communication ~~with~~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. ~~List of~~ 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 ~~in Section 22003(a)1-5.~~:

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

~~(A) "Acceptable Certification Authorities" means a certification authority that meets the requirements of either Section 22003(a)6(C) or Section 22003(a)6(D).~~

~~(B) "Approved List of Certification Authorities" means the list of Certification Authorities approved by the Secretary of State to issue certification for digital signature transactions involving public entities in California.~~

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

(i) ~~one~~One key signs a given message;

(ii) ~~one~~One key verifies a given message; and~~,~~

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

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

(i) ~~identifies~~Identifies the certification authority issuing it;

(ii) ~~names~~Names or identifies its subscriber;

(iii) ~~contains~~Contains the subscriber's public key; ~~and~~

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

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

(~~E~~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.

(~~F~~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.

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

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

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

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

(~~K~~I) "Subscriber" means a person who:

(i) ~~is~~Is the subject listed in a certificate;

(ii) ~~accepts~~Accepts the certificate; and

(iii) ~~holds~~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~~, and~~;

(B) ~~the~~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~~, and,~~;

(C) ~~although~~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~~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~~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~~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) Acceptable Certification Authorities~~

~~(A) The California Secretary of State shall maintain an "Approved List of Certificate Authorities" authorized to issue certificates for digitally signed communication with public entities in California.~~

~~(B) Public entities shall only accept certificates from Certification Authorities that appear on the "Approved List of Certification Authorities" authorized to issue certificates by the California Secretary of State.~~

~~(C) The Secretary of State shall place Certification Authorities on the "Approved List of Certification Authorities" after the Certification Authority provides the Secretary of State with a copy of an unqualified performance audit performed in accordance with standards set in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards No. 70 (S.A.S. 70) "Reports on the Processing of Service Transactions by Service Organizations" (1992) to ensure that the Certification Authorities' practices and policies are consistent with the Certifications Authority's stated control objectives. The AICPA Statement on Auditing Standards No. 70 (1992) is hereby incorporated by reference.~~

~~(i) Certification Authorities that have been in operation for one year or less shall undergo a SAS 70 Type One audit - A Report of Policies and Procedures Placed in Operation, receiving an unqualified opinion.~~

~~(ii) Certification Authorities that have been in operation for longer than one year shall undergo a SAS 70 Type Two audit - A Report Of Policies And Procedures Placed In Operation And Test Of Operating Effectiveness, receiving an unqualified opinion.~~

~~(iii) To remain on the "Approved List of Certification Authorities" a Certification Authority must provide proof of compliance with Section 20003(a)(6)(C)(ii) to the Secretary of State every two years after initially being placed on the list.~~

~~(D) In lieu of completing the auditing requirement in Section 22003(a)(6)(C), Certification Authorities may be placed on the "Approved List of Certification Authorities" upon providing the Secretary of State with proof of accreditation that has been conferred by a national or international accreditation body that the Secretary of State has determined utilizes accreditation criteria that are consistent with the requirements of Section 22003(a)(1) (5).~~

~~(i) Certification Authorities shall be removed from the "Approved List of Acceptable Certifications Authorities" unless they provide current proof of accreditation to the Secretary of State at least once per year.~~

~~(ii) If the Secretary of State is informed that a Certification Authority has had its accreditation revoked, the Certification Authority shall be removed from the "Approved List of Certification Authorities" immediately.~~

(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 ~~in Section 22003(b)(1) (5).~~:

(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 ~~s720.~~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~~The signature digest records the handwriting measurements of the person signing the document using signature dynamics technology~~, and~~;

(B) ~~the~~The signature digest is cryptographically bound to the handwriting measurements~~,~~; and

(C) ~~after~~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~~The acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison~~,~~; and

(B) ~~if~~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~~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~~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. Provisions for Adding New Technologies to the List of Acceptable Technologies.**~~

~~(a) Any individual or company can, by providing a written request that includes a full explanation of a proposed technology which meets the requirements of Section 22002, petition the California Secretary of State to review the technology. If the Secretary of State determines that the technology is acceptable for use with the state, the Secretary of State shall adopt regulation(s), pursuant to the Administrative Procedure Act, which would add the proposed technology to the list of acceptable technologies in Section 22003.~~

~~(b) The Secretary of State has 180 calendar days from the date the request is received to review the petition and inform the petitioner, in writing, whether the technology is accepted or rejected. If the petition is rejected, the Secretary of State shall provide the petitioner with the reasons for the rejection.~~

~~(1) If the proposed technology is rejected, the petitioner can appeal the decision through the Administrative Procedures Act (Government Code Section 11500 et seq).~~

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

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.