digital-signatures.md

```
---
lang: en
title: 'Digital Signatures | California Secretary of State'
viewport: 'width=device-width'
---

Digital Signatures
==================

Title 2. Administration
-----------------------

### Division 7. Secretary of State Chapter 10. Digital Signatures

These  permanent  regulations  are  temporarily
superseded by  emergency regulations  effective from
4/22/2020 through 10/20/2020, or  until that date is
extended  or  the  emergency  regulations  are  made
permanent by regulatory action. See
[emergency regulations]
(https://www.sos.ca.gov/administration/regulations/current-regulations/technology/

+ [22000](#22000) Definitions.
+ [22001](#22001) Digital Signatures Must Be  Created By An Acceptable
                  Technology.
+ [22002](#22002) Criteria  For  Determining  If A  Digital  Signature
                  Technology Is Acceptable.
+ [22003](#20203) List of Acceptable Technologies.
+ [22004](#22004) Provisions For  Adding New Technologies to  the List
                  of Acceptable Technologies.
+ [22005](#22005) Issues to Be Addressed By Public Entities When Using
                  Digital Signatures.

------------------------------------------------------------------------

22000. Definitions. {#22000}
--------------------

1.  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 in such a manner that ties the message
        to the individual that signed the message.

    2.  "Message" means a digital representation of information intended
        to serve as a written communication with a public 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.
0  [2 lines]
        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.

22001. Digital Signatures Must Be Created by an Acceptable Technology. {#22001}
```

digital-signatures-emergency-regulations.md

```
---
lang: en
title: 'Digital Signatures (Emergency Regulations) | California Secretary of State
viewport: 'width=device-width'
---

Digital Signatures (Emergency Regulations)
==========================================

Title 2. Administration
-----------------------

### Division 7. Secretary of State Chapter 10. Digital Signatures

These  emergency  regulations  are  effective  from
4/22/2020 through 10/20/2020, or  until that date is
extended or  the regulations  are made  permanent by
regulatory action.

+ [22000](#22000) Definitions.
+ [22001](#22001) Digital Signatures Must Be  Created By An Acceptable
                  Technology.
+ [22002](#22002) Criteria  For  Determining  If A  Digital  Signature
+                 Technology Is Acceptable for Use by Public Entities.
+ [22003](#20203) Acceptable Technologies.
+ [22004](#22004) Repealed

+ [22005](#22005) Criteria  for Public  Entities to  Use in  Accepting
                  Digital Signatures.

------------------------------------------------------------------------

22000. Definitions. {#22000}
--------------------

1.  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.
0  [2 lines]
        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.*

22001. Digital Signatures Must Be Created by an Acceptable Technology. {#22001}
```

```
1.  For a digital signature to be valid for use by a public entity, it
    must be created by a technology that is acceptable for use by the
    State of California.

22002. Criteria for State to Determine if a Digital Signature Technology Is Accept

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;
5.  It conforms to Title 2, Division 7, Chapter 10 of the California
    Code of Regulations.

22003. List of Acceptable Technologies. {#20203}

1. 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 provisions in
   Section 22003(a)1-5.

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

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


      2.  "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.

      3. "Asymmetric cryptosystem" means a computer algorithm or
         series of algorithms which utilize two different keys with
         the following characteristics:
          1.  One key signs a given message;
          2.  One key verifies a given message; and
          3.  The keys have the property that, knowing one key, it is
              computationally infeasible to discover the other key.

      4. "Certificate" means a computer-based record which:
          1.  Identifies the certification authority issuing it;
          2.  Names or identifies its subscriber;
          3.  Contains the subscriber's public key; and
          4.  Is digitally signed by the certification authority issuing or
              amending it, and
          5.  Conforms to widely-used industry standards, including,
              but not limited to ISO x.509 and PGP certificate
              standards.

      5.  "Certification Authority" means a person or entity that issues a
          certificate, or in the case of certain certification processes,
```

```
1.  For a digital signature to be valid for use by a public entity, it
    must be created by a technology that is acceptable for use by the
    State of California.

*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 Accept

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. {#20203}

1. 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:


      1. "Asymmetric cryptosystem" means a computer algorithm or
         series of algorithms which utilize two different keys with
         the following characteristics:
          1.  One key signs a given message;
          2.  One key verifies a given message; and
          3.  The keys have the property that, knowing one key, it is
              computationally infeasible to discover the other key.

      2. "Certificate" means a computer-based record which:
          1.  Identifies the certification authority issuing it;
          2.  Names or identifies its subscriber;
          3.  Contains the subscriber's public key;
          4.  Is digitally signed by the certification authority issuing or
              amending it; and
          5.  Conforms to widely-used industry standards, including,
              but not limited to, ISO x.509 and PGP certificate
              standards.

      3.  "Certification Authority" means a person or entity that issues a
          certificate, or in the case of certain certification processes,
```

```
128           certifies amendments to an existing certificate.
129
130       6.  "Key pair" means a private key and its corresponding public key in
131           an asymmetric cryptosystem. The keys have the property that the
132           public key can verify a digital signature that the private key
133           creates.
134
135       7.  "Practice statement" means documentation of the practices,
136           procedures and controls employed by a Certification Authority.
137
138       8.  "Private key" means the key of a key pair used to create a digital
139           signature.
140
141       9.  "Proof of Identification" means the document or documents presented
142           to a Certification Authority to establish the identity of a
143           subscriber.
144
145       10. "Public key" means the key of a key pair used to verify a digital
146           signature.
147
148       11. "Subscriber" means a person who:
149           1.  Is the subject listed in a certificate;
150           2.  Accepts the certificate; and
151           3.  Holds a private key which corresponds to a public key listed in
152               that certificate.
153
154   2.  California Government Code § 16.5 requires that a digital
155       signature be 'unique to the person using it'. A public key-based digital
156       signature may be considered unique to the person using it, if:
157
158       1.  The private key used to create the signature on the document is
159           known only to the signer, and
160
161       2.  The digital signature is created when a person runs a message
162           through a one-way function, creating a message digest, then
163           encrypting the resulting message digest using an asymmetrical
164           cryptosystem and the signer\'s private key, and,
165
166       3.  Although not all digitally signed communications will require the
167           signer to obtain a certificate, the signer is capable of being
168           issued a certificate to certify that he or she controls the key pair
169           used to create the signature, and
170
171       4.  It is computationally infeasible to derive the private key from
172           knowledge of the public key.
173
174   3.  California Government Code § 16.5 requires that a digital
175       signature be 'capable of verification'. A public-key based digital
176       signature is capable of verification if:
177
178       1.  The acceptor of the digitally signed document can verify the
179           document was digitally signed by using the signer's public
180           key to decrypt the message; and
181 0 [2 lines]----------------------------------------------------------------------
183           public agency, the issuing Certification Authority, either through a
184           certification practice statement or through the content of the
185           certificate itself, must identify which, if any, form(s) of
186           identification it required of the signer prior to issuing the
187           certificate.
188
189   4.  California Government Code § 16.5 requires that the digital
190       signature remain 'under the sole control of the person using it'.
191       Whether a signature is accompanied by a certificate or not, the person
192       who holds the key pair, or the subscriber identified in the certificate,
193       assumes a duty to exercise reasonable care to retain control of the
194       private key and prevent its disclosure to any person not authorized to
195       create the subscriber's digital signature pursuant to
196       Evidence Code Section 669.
```

```
124           certifies amendments to an existing certificate.
125
126       4.  "Key pair" means a private key and its corresponding public key in
127           an asymmetric cryptosystem. The keys have the property that the
128           public key can verify a digital signature that the private key
129           creates.
130
131       5.  "Practice statement" means documentation of the practices,
132           procedures and controls employed by a Certification Authority.
133
134       6.  "Private key" means the key of a key pair used to create a digital
135           signature.
136
137       7.  "Proof of Identification" means the document or documents presented
138           to a Certification Authority to establish the identity of a
139           subscriber.
140
141       8.  "Public key" means the key of a key pair used to verify a digital
142           signature.
143
144       9.  "Subscriber" means a person who:
145           1.  Is the subject listed in a certificate;
146           2.  Accepts the certificate; and
147           3.  Holds a private key which corresponds to a public key listed in
148               that certificate.
149
150   2.  California Government Code Section 16.5 requires that a digital
151       signature be 'unique to the person using it'. A public key-based digital
152       signature may be considered unique to the person using it if:
153
154       1.  The private key used to create the signature on the document is
155           known only to the signer;
156
157       2.  The digital signature is created when a person runs a message
158           through a one-way function, creating a message digest, then
159           encrypting the resulting message digest using an asymmetrical
160           cryptosystem and the signer\'s private key;
161
162       3.  Although not all digitally signed communications will require the
163           signer to obtain a certificate, the signer is capable of being
164           issued a certificate to certify that he or she controls the key pair
165           used to create the signature; and
166
167       4.  It is computationally infeasible to derive the private key from
168           knowledge of the public key.
169
170   3.  California Government Code Section 16.5 requires that a digital
171       signature be 'capable of verification'. A public-key based digital
172       signature is capable of verification if:
173
174       1.  The acceptor of the digitally signed document can verify the
175           document was digitally signed by using the signer's public
176           key to decrypt the message; and
177 0 [2 lines]----------------------------------------------------------------------
179           public agency, the issuing Certification Authority, either through a
180           certification practice statement or through the content of the
181           certificate itself, must identify which, if any, form(s) of
182           identification it required of the signer prior to issuing the
183           certificate.
184
185   4.  California Government Code Section 16.5 requires that the digital
186       signature remain 'under the sole control of the person using it'.
187       Whether a signature is accompanied by a certificate or not, the person
188       who holds the key pair, or the subscriber identified in the certificate,
189       assumes a duty to exercise reasonable care to retain control of the
190       private key and prevent its disclosure to any person not authorized to
191       create the subscriber's digital signature pursuant to California
192       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
   1. 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.
   2. 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.
   3. 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.
      1. 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.
      2. 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.
      3. 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.
   4. 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).
      1. 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.
      2. 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.

2. 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 provisions in Section

22003(b)(1)-(5).
   1. Definitions. For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:

      1. "Handwriting Measurements" means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person

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:

   1. Apple Root Certificate Program
   2. Microsoft Trusted Root Program
   3. Mozilla Root Program

2. 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:

      1. "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.

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

    3.  "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.

    4.  "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 § 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:

    1.  The signature digest records the handwriting measurements of the
        person signing the document using signature dynamics technology, and

    2.  The signature digest is cryptographically bound to the handwriting
        measurements, and

    3.  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 § 16.5 requires that a digital
    signature be capable of verification. A signature digest produced by
    signature dynamics technology is capable of verification if:

    1.  The acceptor of the digitally signed message obtains the handwriting
        measurements for purposes of comparison, and

    2.  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 § 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:

    1.  The signature digest captures the handwriting measurements and
        cryptographically binds them to the message directed by the signer
        and to no other message, and

    2.  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.

----------
----------

22004. Provisions for Adding New Technologies to the List of Acceptable Technologi
----------

1.  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
```

```
writes it by hand with a pen or stylus on a flat surface.

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

    3.  "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.

    4.  "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:

    1.  The signature digest records the handwriting measurements of the
        person signing the document using signature dynamics technology;

    2.  The signature digest is cryptographically bound to the handwriting
        measurements; and

    3.  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:

    1.  The acceptor of the digitally signed message obtains the handwriting
        measurements for purposes of comparison; and

    2.  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:

    1.  The signature digest captures the handwriting measurements and
        cryptographically binds them to the message directed by the signer
        and to no other message; and

    2.  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. {#22004}
----------
----------
----------
----------
----------
----------
----------
```

```
331     Administrative Procedure Act, which would add the proposed
332     technology to the list of acceptable technologies in Section 22003.
333 2.  The Secretary of State has 180 calendar days from the date the
334     request is received to review the petition and inform the
335     petitioner, in writing, whether the technology is accepted or
336     rejected. If the petition is rejected, the Secretary of State shall
337     provide the petitioner with the reasons for the rejection.
338     1.  If the proposed technology is rejected, the petitioner can
339         appeal the decision through the Administrative Procedures Act
340         (Government Code Section 11500 et seq).
341
342 22005. Criteria for Public Entities To Use in Accepting Digital Signatures. {#2200
343 ------------------------------------------------------------------------------
344
345 1.  Prior to accepting a digital signature, public entities shall ensure
346     that the level of security used to identify the signer of a document
347     is sufficient for the transaction being conducted.
348
349 2.  Prior to accepting a digital signature, public entities shall ensure
350     that the level of security used to transmit the signature is
351     sufficient for the transaction being conducted.
352
353 3.  If a certificate is a required component of a digital signature
354     transaction, public entities shall ensure that the certificate
355     format used by the signer is sufficient for the security and
356     interoperability needs of the public entity.
```

```
276
277 22005. Criteria for Public Entities To Use in Accepting Digital Signatures. {#2200
278 ------------------------------------------------------------------------------
279
280 1.  Prior to accepting a digital signature, public entities shall ensure
281     that the level of security used to identify the signer of a document
282     is sufficient for the transaction being conducted.
283 2.  Prior to accepting a digital signature, public entities shall ensure
284     that the level of security used to transmit the signature is
285     sufficient for the transaction being conducted.
286 3.  If a certificate is a required component of a digital signature
287     transaction, public entities shall ensure that the certificate
288     format used by the signer is sufficient for the security and
289     interoperability needs of the public entity.
```