Smart Initiatives Initiative

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO THE VOTERS

The Attorney General of California has prepared the following title and summary of the chief purpose and points of the proposed measure:

DIGITAL SIGNATURE. ELECTION PETITIONS. PUBLIC AND PRIVATE TRANSACTIONS. INITIATIVE STATUTE. Establishes a state agency to issue a digital certificate to any California resident. Requires certificate to generate a verified digital signature that can be used to subscribe to any authorized public or private sector electronic transaction. Authorizes use as driver license, identification or voter registration card at no additional charge. Requires election officials to validate and count digital signatures for candidacy, initiative, referendum and recall petitions if transmitted to a secure website provided by candidate or proponent. Preserves traditional signature methods. Imposes imprisonment and fines for violations of this system. Summary of the estimate by Legislative Analyst and Director of Finance of fiscal impact on state and local governments: Measure would result in unknown, major one-time costs to develop the systems, and could result in unknown major (probably in the range of tens of millions of dollars) annual net costs to state and local governments.

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

We, the undersigned, registered, qualified voters of California, residents of ______________County (or City and County), hereby propose amendments to the Elections Code and the Government Code, relating to secure online identification and petitioning, and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any special statewide election held prior to that general election or otherwise provided by law. The proposed statutory amendments (full title and text of the measure) read as follows:

SECTION 1. This act shall be known and may be cited as the Smart Initiatives Initiative.

SECTION 2. Chapter 8 (commencing with Section 9700) is added to Division 9 of the Elections Code, to read:

CHAPTER 8. ELECTRONIC PROCEDURES

9700. (a) Notwithstanding any other provision of law, any petition circulated pursuant to this division may be signed using a digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 of the Government Code.

(b) This section shall not be construed to preclude the collection of signatures for a petition by any other means authorized by law.

9701. (a) A proponent of a measure for which a petition is circulated under this division may collect digital signatures generated by digital certificate pursuant to Section 9700, by posting the petition at a website managed by the proponent for that purpose. A candidate for office may, under the provisions of this division, collect and submit signatures in lieu of paying all or part of a filing fee required to run for that office.

(b) A certificated copy of the petition, properly formatted and in compliance with all other standards required by this division, except as to signature spaces, shall be provided online to potential signers of it by displaying the document (other than its signature spaces) in a manner that securely presents an unalterable image equivalent to that normally required for paper versions of the petition, using document exchange and management software approved by the Department of Information Technology for this purpose.

[c] (1) The petition displayed as described in subdivision (b) shall provide a means whereby a user may generate a digital signature on the petition, using a digital certificate, as described in Section 9700, with software approved for this purpose. The signer shall also provide any additional information required by law.

(2) In order to prevent the submission of multiple signatures by the same individual, the computer system hosting the measure shall be programmed to accept only one digital signature generated by the single digital certificate issued to each eligible person, and to reject all subsequent efforts to sign the petition with that digital certificate.

(d) The identity of any person generating a digital signature on a petition pursuant to this section shall be protected as provided by law. No part of this chapter shall be construed to abrogate any right of privacy otherwise protected under law.

(e) Any person who digitally signs a petition pursuant to this section may withdraw that digital signature as provided in Section 9602, except that the request for withdrawal may be submitted by electronic means, using a digital signature generated by digital certificate.

9702. (a) The petition shall be submitted to the appropriate elections official for filing and validation either on electronic storage media delivered physically to the official or by transmission to the official over the Internet under secure conditions, as approved by the Department of Information Technology, at the discretion of the proponent.

(b) Notwithstanding any other provision of law, petitions for which digital signatures have been collected under this chapter may be filed with the appropriate elections official by the proponent, using the methods set out in Section 9702 (a), at any time prior to the final date for filing the petition and the digital signatures contained therein shall be validated or rejected by that elections official within three (3) working days of their receipt.

[c] Signatures generated by digital certificates under this chapter shall be validated by the elections official responsible for validating signatures for the petition in question, using the most rigorous methods of digital authentication available, in conjunction with, or using procedures approved by, the Digital ID Issuing Authority.

9703. (a) In the case of initiative, referendum, and recall petitions, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to qualify the measure for the ballot in question. In the case of signatures to be collected and submitted in lieu of requiring a candidate for public office to pay all or part of a filing fee for that office, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to exempt that candidate from having to pay all or part of the filing fee for that office. The tally of validated signatures collected shall be forwarded to the Secretary of State by the appropriate elections official on an ongoing basis.

(b) The Secretary of State shall provide and update information showing the number of validated digital signatures collected, based on the most recent information provided by the appropriate elections official or officials, at the official website of the Secretary of State.

9704. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

9705. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal code, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 3. Section 16.5 of the Government Code is amended to read:

16.5. (a) In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:

(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 regulations adopted by the Secretary of State. Initiation regulations shall be adopted no later than January 1, 1997. In developing these regulations, the secretary shall seek the advice of public and private entities, including, but not limited to, the Department of Information Technology, the California Environmental Protection Agency, and the Department of General Services. Before the secretary adopts the regulations, he or she shall hold at least one public hearing to receive comments.

(b) The use or acceptance of a digital signature shall be at the option of the parties, except as provided in Chapter 8 (commencing with Section 9700) of Division 9 of the Elections Code and as provided in Section 11791 of the Government Code. Nothing in this section shall require a public entity to use or permit the use of a digital signature.

[c] Digital signatures employed pursuant to Section 710066 of the Public Resources Code are exempted from this section.

(d) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.

SEC. 4. Chapter 7.5 (commencing with Section 11790) is added to Part 1 of Division 3 of Title 2 of the Government Code, to read:

CHAPTER 7.5. DIGITAL IDENTIFICATION ISSUING AUTHORITY

11790. (a) The Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall collaborate to establish the Digital ID Issuing Authority of the State of California, whose mission shall be to efficiently and cost-effectively provide California residents with a high-level digital certificate in an easy-to-use form.

(b) The Digital ID Issuing Authority of the State of California shall, either on its own or by contracting with a suitable private supplier or suppliers, develop, design, implement and maintain a system capable of establishing the identity of individuals with sufficient assurance to issue them the digital certificates called for in this division, of interacting with recipients of these certificates so as to allow them to personalize and secure for their sole use the digital certificates they are issued; of maintaining in good order the databases containing the digital certificates they issue and any other associated data necessary to the efficient functioning of the digital certificate system; of keeping this system current by adding new users as they are issued digital certificates, removing users whose certificates are revoked, or when a user becomes deceased or permanently relocates out of the state, and changing any relevant data about users in a timely manner; and of providing to all electoral and other state and local agencies, in an accurate and speedy manner, the authentication of the digital signatures generated by the certificates it has issued, whether in the context of official petitions, transactions with government, or transactions in the private sector.

(c) (1) The Digital ID Issuing Authority, in collaboration with each recipient, shall generate and issue an individualized digital certificate belonging solely to that recipient. Through the use of passwords, biometrics or other means, this digital certificate shall be rendered accessible solely to the person to whom it is issued, as specified in Section 16.5 (a) (3) of the Government Code, and cited in SEC. 3 of this division. The digital certificates created by the authority according to these procedures shall then be loaded onto smart cards that use the best generally available technology, and that shall be used as the substrate for the driver license or identification card issued by the Department of Motor Vehicles to each applicant/recipient of these licenses and cards, unless an applicant/recipient specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their driver license or identification card.. A smart card containing the registrant's personalized digital certificate shall be provided to registered voters who have neither driver's licenses nor identification cards, as the substrate of their voter registration cards, unless the registrant specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their voter registration card. Anyone eligible to receive a digital certificate on a smart card under the provisions of this division may, at their discretion, receive a smart card without a digital certificate as the substrate of the driver license, identification card, or voter registration card to which they are entitled. The smart cards provided under the provisions of this division may, as practicable, be "contactless," allowing their use at a distance, and may include optical storage areas, allowing users to store and retrieve large amounts of data on and from their cards. There shall be no additional fees charged to users (holders of driver licenses, identification cards, or voter registration cards) for the provision of the digital certificate or smart card.

(2) For purposes of this subdivision, the following definitions shall apply:

(A) "Smart card" means a card with a built-in microprocessor and memory that is capable of receiving, storing, processing, and transmitting electronic data.

(B) "Substrate" means the physical material of an identification card, upon which information is placed.

[c] As part of the process by which a holder personalizes his or her certificate and through which the Digital ID Issuing Authority establishes the identity of the holder, each holder of the state-issued digital certificate may request the Digital ID Issuing Authority to send the holder, free of charge, a complete and accurate digital copy of his or her digital certificate by electronic mail to up to and including ten electronic mail addresses provided by the holder. Pursuant to this subdivision, the digital certificate holder may request, as part of their allotted downloaded copies, that some of these copies be transmitted to cellular phones and/or other mobile or fixed wireless digital devices of their choice. The Digital ID Issuing Authority shall comply with all such requests.

11791. (a) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 shall be accepted by any state entity that offers secure transactions over the Internet, as complete and adequate proof of an individual's identity, and as capable of generating a "digital signature," as defined in Section 16.5, for purposes of executing any form, document, or other instrument related to the transaction, and that digital signature shall be deemed to constitute that individual's assent to the terms of the transaction and shall be accepted as such by the state entity involved.

(b) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 may be used for any personal or commercial purpose for which identification is required, and for generating a valid and acceptable legal signature as required, as provided under Title 2.5 (commencing with Section 1633.1) of Part 2 of Division 3 of the Civil Code.

11792. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

11793. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 5. (a) The California Supreme Court shall have original jurisdiction in any legal action or proceeding to challenge the validity of this act.

(b) The proponents of this act shall have standing to defend the act in any such action or proceeding.

SEC. 6. The Legislature may amend this act only by a statute passed by a two-thirds vote of the membership in each house of the Legislature that is consistent with and furthers the purposes of this act.

SEC. 7. The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provisions or applications.