# 캘리포니아 주, 전자서명 규정 (발췌)

22003.(a) (6) 허용된 인증기관

(A) 캘리포니아 주 국무장관은 캘리포니아 주의 공공기관과의 전자 서명 통신을 위한 인증서를 발급하도록 허가된 '허용된 인증기관 목록'을 유지한다.

(B) 공공기관은 캘리포니아 주 국무장관이 인증서 발급을 허가한 '허용된 인증기관 목록'에 있는 인증기관의 인증서만을 인정한다.

(C) 인증기관의 운영과 정책이 해당 인증기관이 공표한 보안 통제 목표에 부합하는지를 확인하기 위해 미국 공인회계사협회(AICPA)가 발간한 감사 기준 No. 70 (S.A.S 70)("서비스 업체의 서비스 거래 처리 보고에 관한 감사 기준")에 따라 수행된 업무감사에서 유보 없는 적정 판정을 받고 그 감사보고서를 인증기관이 국무장관에 제출하면 국무장관은 그 인증기관을 '허용된 인증기관 목록'에 추가한다. 감사 기준 No. 70 에 대한 AICPA 설명서는 이 규정의 일부를 이룬다.

> (i) 운영을 시작한지 1 년 미만인 인증기관은 SAS 70 의 Type 1 감사를 수검하여 유보 없는 적정 의견을 받아야 함.
>
> (ii) 운영기간이 1 년 이상인 인증기관은 SAS 70 의 Type 2 감사를 수검하여 유보 없는 적정 의견을 받아야 함.
>
> (iii) '허용된 인증기관 목록'에 남아있으려면, 인증기관은 목록에 포함된 이후 2 년마다 Section 20003(a)(6)(C)(ii)을 준수하고 있다는 증빙자료를 국무 장관에게 제출해야 한다.

(D) Section 22003(a)(6)(C)의 감사 요건을 충족하는 대신에, 인증기관은 Section 22003(a)(1)-(5)의 요건에 부합하는 인정 기준을 사용하는 것으로 국무장관이 판단하는 국내 혹은 국제적 인정 기관이 수여하는 인정 증서를 국무장관에게 제출하면 '허용된 인증기관 목록'에 등재될 수 있다. 이 경우,

> (i) 최소한 1 년 마다 현재 유효한 인정 증서를 국무장관에게 제출하지 않는 경우 '허용된 인증기관 목록'에서 제외된다.
>
> (ii) 인증기관의 인정이 해당 인정 기관에 의하여 취소된 사실이 국무장관에게 보고될 경우, 해당 인증기관은 '허용된 인증기관 목록'에서 즉시 제외된다.

## State of California, Digital Signatures Regulations

22003(a)(6)

**(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.

[출처: http://www.sos.ca.gov/digsig/digital-signature-regulations.htm ]