



MEMORANDUM FOR JUDITH SPENCER  
SYSTEM OWNER  
IDENTITY MANAGEMENT DIVISION (MEI)

THRU: WILLIAM G. MORGAN *William G Morgan*  
INFORMATION SYSTEM SECURITY MANAGER (ISSM)  
OFFICE OF THE CHIEF INFORMATION OFFICER (IO)

FROM: MARY J. MITCHELL *Mary J Mitchell*  
DESIGNATED APPROVAL AUTHORITY (DAA)  
DEPUTY ASSOCIATE ADMINISTRATOR  
OFFICE OF TECHNOLOGY STRATEGY (ME)

SUBJECT: Security Accreditation Decision for the VeriSign Shared Service  
Provider Managed Public Key Infrastructure (VSSP MPKI)  
System.

1. References:


- a) Federal Information Security Management Act (FISMA) P.L. 107-347, Title III, December 2002.
- b) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003.
- c) NIST SP 800-26, Revised NIST SP 800-26 System Questionnaire with NISTSP 800-53 References and Associated Security Control Mappings; April 2005.
- d) NIST SP 800-30, Risk Management Guide for Information Technology Systems; July 2002.
- e) NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

- f) NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005.
  - g) NIST SP 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems, March 2006.
  - h) NIST SP 800-59, Guidelines for Identifying an Information System as a National Security System, August 2003.
  - i) NIST SP 800-60, Guidelines Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004.
  - j) FIPS Publication 200, Minimum Security Controls for Federal Information Systems, March 2006.
  - k) VeriSign Shared Service Provider System Certification and Accreditation Submittal Package, October 30, 2006.
2. Reference (a) mandates that all major applications and general support systems used by Federal agencies be authorized to operate in writing by a management official. Therefore, the VSSP MPKI system was required to have an internal and external security assessment conducted on it and a review of this Certification and Accreditation (C&A) documentation by the Designated Approving Authority (DAA).
  3. I have reviewed the VeriSign Certification and Accreditation package submitted by VeriSign on October 30, 2006. Based on the review of the VeriSign Certification and Accreditation package, I hereby authorize operation of the VSSP MPKI system for three years.
  4. VeriSign must take the necessary administrative action to continuously ensure that all personnel, including contractors supporting the VSSP MPKI system obtained the necessary background checks.
  5. VeriSign must also ensure that all personnel including contractors that are supporting the VSSP MPKI system maintain the appropriate security training consistent with their respective roles and responsibilities.

*The following recommendations are incorporated into the accreditation decision letter to reinforce core industry best practices associated with the C&A life cycle process. These recommendations do not imply that there are any outstanding deficiencies in the VSSP MPKI system beyond those specified in items 4 and 5 above.*

- a. The C&A package is a "living document", it is therefore recommended that VeriSign institute a reliable mechanism to keep C&A documentation current throughout the life-cycle of the VSSP MPKI system.
  - b. Issues arising from items c through e below that impacts the overall security of the VSSP MPKI system should be promptly integrated in the POAM and addressed in a timely manner.
  - c. During the C&A period, VeriSign must continue to monitor the system in accordance with the provisions detailed in NIST Special Publications 800-37. It is recommended that the VeriSign perform routine internal and external scans on a monthly basis complemented by an annual in-depth penetration testing as a part of the monitoring process.
  - d. Consistent with GSA operational security framework, it is recommended that VeriSign also employ the Open Web Application Security Project (OWASP) security tools to facilitate VeriSign system life-cycle application security vulnerabilities penetration testing.
  - e. It is further recommended that risks/vulnerabilities identified in the annual WebTrust compliance audit that assesses the adequacy and effectiveness of the controls employed by Certification Authorities (CAs) be discussed with the GSA VeriSign Program Manager and ISSM as applicable.
6. The point of contact for the operation of the VSSP MPKI system is Judith Spencer, Identity Management Division (MEI), GSA Central Office, 1800 F Street NW, Washington, DC 20405, (202) 208-6576.

Approved by



---

Date

Nov 8, 2006