GSA

GSA Office of Governmentwide Policy

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

THRU: 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 Entrust Managed Services Public Key Infrastructure (EMS PKI) System.

1. References:

   a) OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

   b) NIST Special Publication 800-37: Guide for Security Certification and Accreditation of Federal Information Systems, May 2004.

   c) Entrust Managed Services Public Key Infrastructure (EMS PKI) Certification and Accreditation Submittal Package, December 17, 2006.

   d) Request for Authority to Operate (ATO) Decision for the Entrust Managed Services Public Key Infrastructure (EMS PKI), December 17, 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 EMS PKI system had an internal and external security assessment conducted on it and a review of the operations compliance System Security Plan (SSP) Public Key Infrastructure (PKI) offering against the Entrust Certification Practice Statement (CPS) for U.S. Federal PKI Common Policy Framework, Version 1.3.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

3. I have reviewed the Entrust Certification and Accreditation package submitted by Entrust on January 16, 2007. Based on the review of the Entrust Certification and Accreditation package, I hereby authorize operation of the EMS PKI system for three years.

4. Entrust must take the necessary administrative action(s) to address all low level vulnerabilities noted in the scan report dated January 30, 2007 within 30 days of the ATO recommendation, and all medium level vulnerabilities within 10 days of the ATO recommendation.

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 Entrust EMS PKI system beyond that specified in item 4 above.

a. The C&A package is a "living document", it is therefore recommended that Entrust institute a reliable mechanism to keep C&A documentation current throughout the life-cycle of the EMS PKI system.

b. Issues arising from items c through e below that impacts the overall security of the Entrust EMS PKI system should be promptly integrated in the POAM and addressed in a timely manner.

c. During the C&A period, Entrust must continue to monitor the system in accordance with the provisions detailed in NIST Special Publications 800-37. It is recommended that Entrust 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 Entrust also employ the Open Web Application Security Project (OWASP) security tools to facilitate Entrust EMS PKI 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 Entrust Program Manager and ISSM as applicable.

5. The point of contact for the operation of the Entrust EMS PKI system is Judith Spencer, Identity Management Division (MEI), GSA Central Office, 1800 F Street NW, Washington, DC 20405, (202) 208-6576.

Mary J. Mitchell
Approved by

Feb 12, 2007
Date