




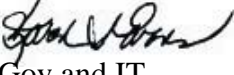
EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503


December 20, 2004

M-05-05

MEMORANDUM FOR THE CHIEF FINANCIAL OFFICERS, CHIEF INFORMATION OFFICERS, AND CHIEF ACQUISITION OFFICERS

FROM: Linda Springer   
Controller

Karen S. Evans   
Administrator, E-Gov and IT

David Safavian   
Administrator, Office of Federal Procurement Policy

SUBJECT: Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services

This Administration is committed to achieving accountability and efficiency in the operation of public programs, including through the use of information technology and electronic signatures. Previous OMB guidance instructed agencies to move to commercial managed services for public key infrastructure (PKI) and electronic signatures.<sup>1</sup> A move to a commercial service from a government operated one will save time and money. However, lack of strong government controls can create new risks not present in government operated systems. To mitigate these risks, you must use shared service providers.

**Use Shared Service Providers**

Strong government oversight and internal controls mitigate the risk of using a commercial service. For either government operated systems or those commercially provided under a contract, agencies must ensure their electronic signature systems have an adequate system of oversight and internal controls.

The General Services Administration (GSA) has created the Shared Service Provider Program to provide strong government oversight of commercial managed service providers. The list of providers certified to provide PKI services is located at <http://www.cio.gov/ficc/>. By contracting with a certified provider, agencies obtain services consistent with current electronic signature law and policy. The cost savings and benefits associated with a contractor provided service, with adequate government oversight and control, outweigh the costs of mitigating potential risks associated with contractor involvement. Qualified providers must:

---

<sup>1</sup> OMB Memorandum Streamlining Authentication and Identity Management, July 3, 2003 (<http://www.whitehouse.gov/omb/inforeg/eauth.pdf>).

- operate their certification authorities under a certificate policy developed, owned and controlled by the Federal government,
- demonstrate compliance with this policy with an annual third party audit,
- receive approval from a qualified GSA official, and
- comply with existing security law, including certification and accreditation.<sup>2</sup>

GSA will grant the provider authority to operate the service and supporting IT system. You will receive copies of GSA's authorization. However, agencies continue to have an on-going responsibility to meet all legal and OMB policy requirements on their portion of the IT system. Include these operations in your annual evaluation required by the Federal Information Security Management Act.

### **Government Accountability Office Policy**

GAO recently updated the criteria it uses to assess electronic signature systems to ensure systems are consistent with current Federal policy and best practices.<sup>3</sup> You will find the GAO document useful in developing your electronic signature systems and as a tool for periodic monitoring.

If you have any questions, please contact Jeanette Thornton, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3562, fax (202) 395-5167, e-mail [jthornto@omb.eop.gov](mailto:jthornto@omb.eop.gov).

---

2 Special Publication 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems <http://www.csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf> (May 2004)

3 GAO-04-1023R, "Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities," August 9, 2004 (<http://www.gao.gov/new.items/d041023r.pdf>), U.S.C. § 1501(a)(1)(A), GAO B-245714, "National Institute of Standards and Technology: Use of Electronic Data Interchange Technology to Create Valid Obligations," December 13, 1991.