



March 3, 2005

Dear CIO Member:

On December 20, 2004, the Office of Management and Budget (OMB) issued memorandum M-05-05 "Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services." This technical supplement provides additional information on the Shared Service Provider Program prescribed for agency use in the OMB memorandum.

### **Definitions and Scope**

"Electronic signature" used in M-05-05 refers to technology used for identity assurance in addition to the act of affixing a legal signature to a document.

The scope of these memos is limited to Public Key Infrastructure (PKI), a cryptographically based "signature" solution. Specifically, these memos cover the deployment of PKI digital certificates to Federal employees and contractor staff on behalf of their employing agencies. They do not refer to Government-to-business or Government-to-citizen relationships. The activities of the E-Authentication initiative address credentialing and electronic signatures in these relationships.

### **Technical Requirements**

To meet the requirements of M-05-05, agencies must be compliant with the Federal PKI Common Policy Framework, the standard policy for the deployment and use of digital certificates for Federal employees, contractors and affiliates.<sup>1</sup>

All agency implementations of PKI must comply with the Common Policy Framework by October 25, 2005. This can be achieved in one of two ways:

1. **Cross-Certification with the Federal Bridge** — Agencies operating a Certification Authority that is cross-certified with the Federal Bridge at medium assurance or higher are operating in accordance with the Common Policy. Agencies operating a Certification Authority that is not cross-certified with the Federal Bridge at medium assurance or higher must achieve cross-certification by December 31, 2005, or migrate to compliance with the Common Policy Framework via a Shared Service

---

<sup>1</sup>X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, available at <http://www.cio.gov/ficc/documents/CommonPolicy.pdf>, November 1, 2004.

Provider. Subsequently, the Federal PKI Policy Authority will no longer accept applications for cross certification from Federal organizations unless such requests are accompanied by specific approval from OMB. All future cross certification activities will be reserved for facilitating interoperability with external entities (e.g. states, industry, academia, allied governments).

2. **Shared Service Provider Program** — Agencies that do not meet the criteria above are required to purchase PKI services from entities on the Shared Service Provider list posted at [www.cio.gov/ficc](http://www.cio.gov/ficc), when implementing PKI for their employees and contract staff. Entities included on the Shared Service Provider list have undergone a review process in order to ensure their compliance with the Federal PKI Common Policy Framework and are specifically authorized to issue certificates under the Common Policy.

### **Access Certificates for Electronic Services**

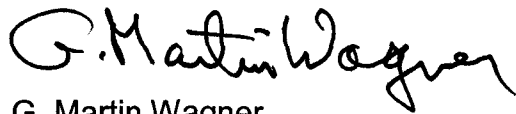
The Access Certificates for Electronic Services (ACES) program administered by General Services Administration (GSA) provides PKI services to a large variety of communities, including unaffiliated individuals, business affiliates, and Federal employees. The majority of ACES services are unaffected by this requirement and continue to be a viable solution for Government-to-citizen, Government-to-business, and Government to Government interactions. Only the Federal Employee PKI Certificate service within ACES is required to undergo review to join the Shared Service Provider program. This is underway. The ACES Federal Employee PKI Certificate services will complete the process and be recognized as Shared Service Providers by October 25, 2005.

### **Impact of Homeland Security Presidential Directive (HSPD) 12**

HSPD-12 requires the use of identification credentials by Federal employees and contractors that meets a government-wide standard. This standard includes access to federally controlled information systems. To meet the logical access requirements of HSPD-12, the standard will specify that agencies must be compliant with the Federal PKI Common Policy Framework discussed above. This ensures agencies compliance with both M-05-05 and HSPD-12 and promotes interoperability across the Government.

For questions regarding this memorandum, contact Judith Spencer, Office of Governmentwide Policy, General Services Administration, phone (202) 208-6576, fax (202) 501-6455, e-mail: [judith.spencer@gsa.gov](mailto:judith.spencer@gsa.gov).

Sincerely,

A handwritten signature in black ink that reads "G. Martin Wagner". The signature is written in a cursive style with a large, prominent "G" at the beginning.

G. Martin Wagner  
Associate Administrator