

NOV 12 2003

**CLASS DEVIATION AND DETERMINATION
TO ALLOW INDIVIDUALS, FIXED PRICE CONTRACTORS
AND OFFERORS TO USE GSA AS A SOURCE OF SUPPLY
FOR PUBLIC KEY INFRASTRUCTURE (P) SOLUTIONS**

PROLOGUE

The Government Paperwork Elimination Act (GPEA) requires Federal agencies, by October 21, 2003, to provide individuals or entities the option to submit information or transact with the agency electronically and to maintain records electronically when practicable. To implement GPEA, agencies must make appropriate use of Public Key Infrastructure solutions. Public Key Infrastructure solutions include (but is not limited to) private and public signature keys, encryption and access certificates.

Two parties who may not know each other should be able to communicate reliably through electronic means, with confidence that their communication] is protected and their identities are established with neither party being impersonated. They should also have assurance that their communication cannot be repudiated after it has occurred . Public key technology enables applications software (programs) to meet these requirements. Public key technology and digital certificates (which bind the identity of a party to his, her, or is public key) can be used to assure identity, privacy, non-repudiation, and data integrity.

Several services are available through the use of PKI solutions:

- A user can authenticate himself or herself to another party, typically a server, by digitally signing a challenge phrase (supplied by the server) with the user's private signature key. The server can use the public key in the user's digital certificate to validate the user's signature on the challenge phrase and thus authenticate the user.
- Web servers frequently have digital certificates issued to them which can be used to authenticate the server to a user and create an encrypted communications session that can be used to protect any shared secret information including Personal Identification Numbers (PINs) or passwords. Such an "encrypted" session" can prevent a malefactor from taking it over (sometimes called "hijacking") after the session has begun.
- When web servers and clients both have digital certificates, mutual strong authentication can be achieved, and each party can authenticate itself to the other.
- A document or file may be digitally signed using a party's private signature key, creating a "digital signature" that is stored with the document. At a later date, anyone can validate the signature on the document using the public key From the digital certificate issued to the signer. Validating the digital signature not only confirms who signed it, but also ensures that there have been no alterations to the document since it was signed.

- Similarly, an e-mail message may be digitally signed . Validating the signature on the e-mail can help the recipient know with confidence w o sent it, and that it was not altered during transmission.

FINDINGS

1. Public Key Infrastructure solutions are ' available under the Access Certificates for Electronic Services (ACES) program. The program manager for this activity is the GSA Federal Technology Service, while contract administration responsibility is with the Federal Supply Service.
2. Under GSA Order ADM 4800:2E (January 3, 2000) ' d Subpart 51.1 of the FAR, use of the ACES program is primarily limited to executive agencies and cost-reimbursement contractors.
3. Only the appropriate use of Public Key Infrastructure solutions will allow Federal Agencies to meet the mandate of GPO that they be able to conduct electronic transactions with individuals, bidders and contractors with an assurance of identity, privacy, non-repudiation, and data integrity.
4. ACES operates as a trusted third party for procuring PKI services. It is the only contractor operated, government managed PKI service offering available. ACES services provide for a government "approved" source of PKI services. As relying parties, agencies can be assured that the ACES Industry Partners have met the criteria as stipulated in the ACES Certificate Policy. GSA, as manager of the ACES Program, performs a rigorous Certification and Accreditation of the ACES Industry Partners Operations to ensure that they perform in conformance with all the applicable rules, regulations and guidelines in providing these services.

DETERMINATION

Providing Public Key Infrastructure solutions to offerors and contractors (whether fixed price or cost reimbursement) will facilitate agencies meeting the requirements of GPEA. Allowing offerors and contractors to use GSA as a source of supply for Public Key Infrastructure solutions is necessary to provide efficient and economical service to executive agencies. Under my authority provided by 40 USC § 501, I have determined that it is advantageous to the Government as a whole, considering issues of economy, efficiency and service, that individuals desiring to communicate electronically with federal agencies, offerors on federal procurements and fixed priced contractors be allowed to use GSA as a source of supply for Public Key Infrastructure solutions.

Having made this determination, I hereby authorize a deviation from 48 CFR 51.1. Individuals, representatives of state and local governments, offerors and contractors (fixed price and cost reimbursement) who have a need to communicate electronically with any Federal Agency are now authorized under this deviation to place orders against contracts awarded under the ACES program without regard to the restrictions and ordering procedures imposed by FAR Subpart 51.1.



Donna Bennett
Head of Contracting Activity



David Drabkin
Senior Procurement Executive