

**CI-FSS-052 AUTHENTICATION PRODUCTS AND SERVICES
(MAY 2006)**

(a) General Background.

(1) Authentication Products and Services provide for authentication of individuals for purposes of physical and logical access control, electronic signature, and performance of E-business transactions and delivery of Government services. Authentication Products and Services consist of hardware, software components and supporting services that provide for identity assurance.

(2) Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors" establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Further, the Directive requires the Department of Commerce to promulgate a Federal standard for secure and reliable forms of identification within six months of the date of the Directive. As a result, the National Institute of Standards and Technology (NIST) released Federal Information Processing Standard (FIPS) 201: Personal Identity Verification of Federal Employees and Contractors on February 25, 2005. FIPS 201 requires that the digital certificates incorporated into the Personal Identity Verification (PIV) identity credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. In addition, FIPS 201 requires that Federal identity badges referred to as PIV credentials, issued to Federal employees and contractors comply with the Standard and associated NIST Special Publications 800-73, 800-76, 800-78, and 800-79.

(b) Special Item Numbers.

(1) The General Services Administration has established the E-Authentication Initiative (see URL: <http://cio.gov/eauthentication>) to provide common infrastructure for the authentication of the public and internal federal users for logical access to Federal E-Government applications and electronic services. To support the government-wide implementation of HSPD-12 and the Federal E-Authentication Initiative, GSA is establishing the following Special Item Numbers (SINs):

(i) SIN 132-60: Access Certificates for Electronic Services (ACES) Program. This program provides identity management and authentication services and ACES digital certificates for use primarily by external end users to access Federal Government electronic services and transactions in accordance with the X.509 Certificate Policy for the Federal ACES Program.

(ii) SIN 132-61: PKI Shared Service Providers (PKI SSP) Program. This program provides PKI services and digital certificates for use by Federal employees and contractors to the Federal Government in accordance with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

(iii) SIN 132-62: HSPD-12 Product and Service Components, SIN 132-62 is established for products and services for agencies to implement the requirements of HSPD-12, FIPS-201 and associated NIST special publications. The HSPD-12 implementation components specified under this SIN are:

(A) PIV enrollment and registration services and products

- (1) Hardware and Software Products
- (2) Deployment Services
- (3) Managed Service

(B) PIV systems infrastructure Services and Products

- (1) Hardware and software products
- (2) Deployment Services
- (3) Managed Service

(C) PIV Card Management and Production Services, and Products

- (1) Hardware and Software Products

- (2) Deployment Services
- (3) Managed Services

(D) PIV Card Finalization Services and Products

- (1) Hardware and Software Products
- (2) Deployment Services
- (3) Managed Services

(E) PIV System Integration Services, and Products (Bundled)

- (1) "Pure" Integration Services
- (2) Turn-Key Integrated Services and Products
- (3) Managed Services

(F) Physical Access Control Products and Services,

(G) Logical Access Control Products and Services,

(H) Approved FIPS 201-Compliant Products and Services.

(c) Qualification Information.

(1) All of the products and services for the SINs listed above must be qualified as being compliant with Government-wide requirements before they will be included on a GSA Information Technology (IT) Schedule contract. The Qualification Requirements and associated evaluation procedures against the Qualification Requirements for each SIN and the specific Qualification Requirements for HSPD-12 implementation components are presented at the following URL: <http://www.idmanagement.gov>.

(2) In addition, the National Institute of Standards and Technology (NIST) has established the NIST Personal Identity Verification Program (NPIVP) to evaluate integrated circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform card and reader interface testing for interoperability. Products that are approved as FIPS-201 compliant through these evaluation and testing programs may be offered directly through SIN 132-62 under the category "Approved FIPS 201-Compliant Products and services.

(d) Qualification Requirements.

(1) Offerors proposing products and services under Special Item Numbers (SINs) 132-60, 132-61 and 132-62 are required to provide the following:

(i) Proposed items must be determined to be compliant with Federal requirements for that Special Item Number. Qualification Requirements and procedures for the evaluation of products and services are posted at the URL: <http://www.idmanagement.gov>. GSA will follow these procedures in qualifying offeror's products and services against the Qualification Requirements for applicable to SIN. Offerors must submit all documentation certification letter(s) for HSPD-12, SINs 132-60, 132-61 and 132-62 at the same time as submission of proposal. Award will be dependent upon receipt of official documentation from the Acquisition Program Management Office (APMO) listed below verifying satisfactory qualification against the Qualification Requirements of the proposed SIN(s).

(ii) After award, Contractor agrees that certified products and services will not be offered under any other SIN on any GSA Multiple Award Schedule.

(iii) (A) If the Contractor changes the products or services previously qualified, GSA may require the contractor to resubmit the products or services for re-qualification.

(B) If the Federal Government changes the qualification requirements or standards, Contractor must resubmit the products and services for

re-qualification.

(e) Demonstrating Conformance.

(1) The Federal Government has established Qualification Requirements for demonstrating conformance with the Standards. The following websites provide additional information regarding the evaluation and qualification processes:

(i) For Access Certificates for Electronic Services (ACES) and PKI Shared Service Provider (SSP) Qualification Requirements and evaluation procedures:
<http://www.idmanagement.gov>;

(ii) For HSPD-12 Product and Service Components Qualification Requirements and evaluation procedures: <http://www.idmanagement.gov>;

(iii) For FIPS 201 compliant products and services qualification and approval procedures:
<http://www.csrc.nist.gov/piv-project/> and <http://www.smart.gov> .

(f) Acquisition Program Management Office (APMO).

(1) GSA has established the APMO to provide centralized technical oversight and management regarding the qualification process to industry partners and Federal agencies. Contact the following APMO for information on the E-Authentication Qualification process.

(i) The Acquisition Program Management Office point-of-contact for Access Certificates for Electronic Services (ACES – SIN 132-60) is:

Stephen P. Duncan
Program Manager
E-Authentication Program Management Office
2011 Crystal Drive, Suite 911
Arlington, VA 22202
stephen.duncan@gsa.gov
703.872.8537

(ii) The Acquisition Program Management Office Point-of-contact for Shared Services Provider (SSP) Program (SIN 132-61) is:

Judith Spencer
Office of Electronic Gov't & Technology
1800 F Street, NW, Room 2011
Washington, DC 20405
Judith.spencer@gsa.gov
202-208-6576

(iii) The Acquisition Program Management Office point-of-contact for HSPD-12 Products and Services or bundled Solutions (SIN 132-62) is:

Mike Brooks
Director, Center for Smartcard Solutions
Office of Center for Smartcard Solutions
1800 F Street, N.W., Room 5010
Washington, DC 20405
202.501.2765 (telephone)
202.208.3133 (fax)

(iv) The Acquisition Program Management Office point-of-contact for FIPS 201 Evaluation Program Approved Products List (Sin 132-62) is:

April Giles
FIPS 201 Evaluation Program Chief Architect

Identity Management Division
GSA Office of Government-wide Policy
202.501.1123 (telephone)