



General Services Administration

Federal Supply Service
Authorized Federal Supply Schedule Price List

GSA Schedule 70

SIN 132-51, Information Technology Services

Includes resources and facilities management, database planning and design, systems analysis and design, network services, programming, millennium conversion services, conversion and implementation support, network services project management, data/records management, subscriptions/publications (electronic media), and other services.

SIN 132-62, HSPD-12 Product and Service Components

Products and services for agencies to implement the requirements of HSPD-12, FIPS-201 and associated NIST special publications. IDTP received GSA Certification for "Pure Integration Services".



Identification Technology Partners, Inc. (IDTP)
12208 Pueblo Road
North Potomac, MD 20878-2064
Office: 301-990-9404
Fax: 301-990-9405
www.idtp.com

Contract Number: GS-35F-0211T

Contract Period: January 15, 2007 – January 14, 2012

IDTP is a small business

Point of Contact:

Stephen M. Hunt

shunt@idtp.com

Office: 703-430-2037

Fax: 703-430-3077

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Supply Service's home page via the Internet at <http://www.fss.gsa.gov/>

Table of Contents

<i>Section 1 – IDTP</i>	3
Qualifications	3
<i>Standards</i>	4
Project Summaries	6
<i>Section 2. Customer Information</i>	9
<i>Section 3. SIN 132-51/62 Position Descriptions</i>	10
Senior IT Principal:	10
Senior IT Consultant:	10
IT Principal:	10
IT Subject Matter Expert I:	11
<i>Section 4. Pricing</i>	12

Section 1 – IDTP

Qualifications

Identification Technology Partners, Inc. (IDTP) was formed in October 2000, as a Washington D.C. area based consulting firm focused on the advanced identification technology industry. IDTP has experience in advanced systems integration and design to support the application of biometric, smart card, PKI and secure identification technologies in large-scale credentialing, Automated Fingerprint Identification Systems, and physical & logical access applications. IDTP provides clients with a broad range of program and technology-centric services that support the optimization of business value and operational impact. IDTP provides services throughout the life of a program that ensure well-defined goals and requirements, program planning, effective risk management, system design alternatives and assessment, tailored installation and testing services (consistent with client requirements), performance analyses, and post-implementation support.

Our approach to program management is benefited by an unequalled depth and breadth of experience in identification programs for government and the private sector. IDTP's program management attitude emphasizes Business Value through effective management of all aspects of the client program and clear communication with the client. IDTP's reputation for unequalled expertise in identity related technology disciplines and standards development is well known and respected in government and industry. Our ability to provide our clients with the industry's finest technology consulting and program management services has been proven through many successful client programs. We have supported national-level programs of large scale and considerable complexity, and have developed proven methodologies through practical experience. Our past successes fuse commercial best practices and intellectual capital with a client's requirements for proven experience and performance to realize programs of diverse requirements and complexity.

Through its industry and technical partnerships, IDTP has become a leading authority regarding biometric standards and biometric technology applications. IDTP experience and expertise in advanced identification technologies has been instrumental in the development of system design concepts for identity credentialing including the creation of key industry standards like the NIST Federal Information Processing Standard (FIPS) -201.

IDTP provides support services in the areas of:

- Technology integration
- Biometric technology analysis, assessment, and selection
- Smart card technology analysis, assessment, and selection
- Requirements analysis
- Technology standards definition and application
- Identification document implementation
- Strategy development and implementation
- Business need definition
- Technology assessment
- IT architecture development

IDTP has assembled a professional staff who have been providing information technology and security solutions to industry and government for over 30 years.

IDTP provides comprehensive systems knowledge to our clients enabling the assessment, application and design of systems and processes that employ advanced security and identity credentialing technologies. IDTP has recognized experience and competency in the following areas:

- Border Entry and Exit
- Secure Credentialing
- Biometric Authentication
- Technology Standards
- Software Application Profiles
- Smart Card Solutions & Analysis
- Hardware and Software Development
- Information Security
- Smart Card & Security IC Controllers
- Physical & Logical Access
- Identification card programs
- Large-scale civil ID
- “Chain of Trust” management
- Technology Integration
- Market Research & Analysis
- Information Assurance
- Public Key Infrastructure (PKI)
- Encryption Technologies

Standards

Identification Technology Partners have been involved with the development and application technology standards since the mid 1990’s. IDTP volunteer staff has been proactive in the development of biometric and related standards. IDTP serves as a “standards incubator” to INCITS / M1, the American National Standards Institute (ANSI) standards group for biometrics.

IDTP participates in a number of standards initiatives, including:

- BioAPI Consortium
- Common Biometric Exchange Formats Framework (CBEFF)
- Biometric Consortium Working Group
- ANSI/NCITS B10
- INCITS / M1 and related AD HOC technical working groups
- ISO/IEC JTC 1 / SC 37 International Biometric Technical Standards Sub-committee

Further, IDTP provides key personnel support for:

- M1 - Border Management Application Profile (technical editor)
- M1 – Transportation Workers Identification Card Application Profile (tech. co-editor)
- SC37 – Common Biometric Exchange Framework Format (technical editor)
- Government Smart Card- Interagency Advisory Board (GSC-IAB) Federal Information Processing Standard (FIPS) 201 & Special Publication (SP) 800-73, SP 800-76 and SP 800-78 initiatives.
- The Smart Card Alliance – Physical Access Control Advisory Council

Identification Technology Partners have worked toward development and acceptance of:

The **BioAPI**, an Application Program Interface designed specifically for the biometric industry. IDTP supported the National Institute of Standards and Technology (NIST) with the development of BioAPI assertions for use in the development of biometric conformance assurance testing tools.

The Common Biometric Exchange File Framework (CBEFF)

An IDTP Associate served as the technical editor for standards under development in ISO/IEC JTC 1 SC 37, IDTP and managed the release of the “Common Biometric Exchange Formats Framework — Part 1: Data Element Specification”.

The INCITS M1, Biometrics Technical Committee

An IDTP Partner is an officer and technical editor for standards under development in INCITS M1. IDTP staff members managed the completion and release of the “Application Profile for Interoperability - Data Interchange and Data Integrity of Biometric Based Personal Identification for Border Management” and prepared and released the preliminary “Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification”.

The **Smart Card Alliance** a not-for profit, multi-industry association works toward accelerating the widespread acceptance of multiple application smart card technology. IDTP Partners have been actively involved in the alliance over the course of the last eight years, providing guidance and editing on several work products. Most recent activities include work on GSC-IS, physical access control and Windows File Structure working groups.

The IDTP role in Standards Management is a continuing activity that encompasses both serving as officers of standards organizations (for example, the chair of ANSI/INCITS M1 Task Group M1.2) as well as performing support tasks for such officers (for example, transformation of documents that are used in standards meetings into more convenient formats for dissemination to attendees). IDTP holds memberships in and contributes expertise to standards bodies including the BioAPI Consortium, the Biometric Consortium Working Group, INCITS Biometrics Technical Committee M1 and several of its Task Groups, ANSI/NCITS B10, and ISO/IEC JTC 1 Subcommittee 37-Biometrics. IDTP staff members have held various full time and part time positions within these organizations from chairmanships to technical writing and editing roles.

IDTP has contributed directly to the development, revision and approval of several American and international standards including BioAPI (ANSI 358-2002 and ISO/IEC 19784), CBEFF (NISTIR 6529-A and ISO/IEC 19785), the M1 transportation workers application profile (INCITS 383), the M1 border management application profile (INCITS 394), the M1 Government Smartcard application profile, as well as related ad hoc working groups.

IDTP work in the area of Technical Interfaces directly supports ISO/IEC SC 37 Working Group 2 and Task Group M1.2 within INCITS M1. It is expected that this effort will finalize all remaining technical interface requirements pertaining to BioAPI, CBEFF, the Javacard API and related template protection and usage guidelines.

IDTP staff members are performing work on another project which will parallel and supplement a corresponding ISO/IEC project to build a standard that defines conformance test methods and procedures for BioAPI, as well as specifying the test assertions that document the test case requirements. This standards project applies to the ANSI version of BioAPI and has a scope that covers less than 100 percent of the BioAPI specification. The project recognizes that the ISO/IEC standard (providing 100% coverage) will take longer to complete; the objective is to develop a partial solution that covers the most commonly used functions.

IDTP completed development of Application profiles in the areas of Border Management and Transportation Worker Identification. IDTP plans involvement in application profile development in Point of Sale and various Department of Defense applications. Each application profile specifies how to apply base standards to the functional requirements defined in an application. For example, the Border Management profile specifies what content from the biometric data interchange format standards, BioAPI, CBEFF, X9.84 and ICAO document 9303 should be called out in any Statement of Work related to the use of biometrics in border management systems.

IDTP is involved with development of the NISTIR-CBEFF Implementation Guidelines. This project will develop tutorial information in support of the adoption of NISTIR 6529-A (USA CBEFF) by vendors and application developers. This effort will produce a stand-alone document as well as presentation materials that can be adapted to the requirements of various audiences (technical, management overview, public information).

Data format efforts will be finalized in a number of areas including fingerprint minutia, pattern, finger image, face, iris, hand and signature. Conformance testing support for these data format standards will be integrated into the conformance test suite as they become available.

Finally, IDTP work efforts include the preparation of support documentation which supports APIs, conformance test methodologies, CBEFF development, template protection, and GSC interoperability.

Project Summaries

Identification Technology Partners have been involved with numerous projects that have utilized biometric and smart card technology to insure positive identification of individuals. Recent IDTP projects include:

- **Transportation Security Agency – Transportation Worker ID Credential (TWIC)**
TWIC is a pioneering, civilian focused high assurance ID system designed to improve security at our nation's ports and air transportation facilities. Its mission is to provide a high assurance ID credential serving two principal purposes: strong identity assurance and a credential that works with automated physical access control systems throughout the transportation system. The system uses fingerprint biometrics to assure identification of workers in either an online or offline model.

The core capabilities of the TWIC credential enable it to:

- Confirm the bearer of the card as the rightful card holder using PIN and/or biometric verification.
- Register the rightful cardholder into PKI based applications and physical access control systems (PACS)
- Enable the cardholder to use systems and network resources using PKI facilities, such as single sign-on, email access and encryption
- Assure the credential is valid and has not been tampered with and is compatible with the FIPS-201 PIV credentialing standard.
- Access buildings and facilities using the same smart credential

IDTP task efforts included project planning & technical management, functional requirement analysis, implementation planning, biometric technology selection and integration, Statement of Work development, technical and functional requirements definition, gap analysis, site survey and facility assessment, RFP preparation and editing, and evaluation planning. IDTP deliverables included design documentation supporting a unified smart credential approach that provides Identity, PKI and PACS services to the TWIC cardholder. IDTP was strategic in the design of all biometric processes and the identity management processes that provide strong assurance that the bearer of the credential is the rightful cardholder, that the credential is valid and has not been revoked, and that this can be electronically verified by all relying parties.

- **Registered Traveler (RT)**

IDTP provides the TSA's Registered Traveler program with program management expertise, engineering, technical and strategic system analysis support. The TSA's Registered Traveler program provides expedited security screening for passengers who provide biometric and biographic information that is vetted through a security screening process. The Registered Traveler credential is a secure smart card containing biometric and biographical information, expediting the passenger screening process through identity verification. IDTP's support to the RT program includes defining the RT credential functional, security, business case and technology requirements and standards, screening system interface analysis, large-scale automated fingerprint information system analysis & requirements, support Certification & Accreditation testing and provide oversight of the contractor design and development process. Through its depth of experience in identification, credentialing and security programs, IDTP provides the TSA RT program with strategic program guidance and monitoring, risk identification and impact analysis and standards and specification compliance oversight in the areas of biometrics, smart cards and PKI. IDTP provides TSA with extensive technical experience and insight - as well as strong program planning and management expertise to ensure the RT program's success.

- **GSC-IAB Support**

IDTP provided the Government Smart Card – Interagency Advisory Board (GSC-IAB) support services which produced a new logical data model for submission and review by the GSC-IAB. IDTP task efforts established minimum acceptable data elements for a common data model, established pluggable data model options (biometrics, legacy applications), provided mandatory and optional element definitions, conducted data module refinement, and reconciled inconsistencies between national and international standards. Additionally, IDTP provided smart card, biometric, identity management, and card and credential lifecycle management Subject Matter Experts for review of FIPS PUB 201 Personal Identity Verification (PIV) for Federal Employees and Contractors PUBLIC DRAFT and NIST Special Publication 800-73 Integrated Circuit Card for Personal Identity Verification.

- **Biometrics for National Security (BiNS)**

Identification Technology Partners, Inc. has been retained as a subject matter expert in the area of biometric and smart card technology. *IDTP prepared and delivered a Database Design Document that defined the functional requirements of a national biometric database. IDTP supported the National Institute of Standards and Technology (NIST) by managing the completion and release of a.) The Application Profile for Interoperability - Data Interchange and Data Integrity of Biometric Based Personal Identification for Border Management, b.) Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification, and c.) Common Biometric Exchange Formats Framework — Part 1: Data Element Specification. IDTP is providing ongoing support to NIST regarding the development of BioAPI and CBEFF biometric conformance assurance test tools.*

- **PANYNJ Aviation Access Control Biometric Authentication Project**

IDTP provided system engineering and technical expertise to the Port Authority of New York and New Jersey's Biometric Authentication Project, under a subcontractor to the Louis Berger Group. The project integrated biometric authentication and contactless smart card credentials for physical access security at all airport facilities operated by PANYNJ, including LaGuardia, JFK and Newark. This project serves as a Stage I implementation toward an interoperable Transportation Worker Identification Credential (TWIC) capability within the Port Authority's physical access control systems. *IDTP performed site surveys to document existing physical access control systems, infrastructure, head-end configuration and access control business practices. Working in conjunction with PANYNJ staff, IDTP identified and documented complete requirements for the project including functional, technical, performance, physical, environmental, interface and interoperability needs. IDTP developed a detailed requirements specification that provided the PANYNJ with a document that could be used in procurement actions to ensure full compliance with the agency's needs. IDTP developed system designs for system biometric and smart card readers that were interoperable with legacy magstripe cards during the transition period. IDTP also developed recommendations for interfaces with door and gate controllers as well as designs for enrollment systems changes to issue smart cards with PKI encryption and biometric templates. IDTP was responsible for profiling the industry products that could meet the Port Authority's complex and challenging set of requirements and in recommending solutions and options when no product could meet the full requirements set. IDTP was responsible for developing detailed specifications for: the contactless smart card, the credential printer, PKI encryption and the biometric capture device. IDTP developed an Application Data Model for the PANYNJ consistent with relevant US and international standards. IDTP's support to the Port Authority was a key element in the security enhancement at very large airport installations.*

Section 2. Customer Information

1. a. SIN 132-51, Information Technology Services,
SIN 132-62, HSPD-12 Product and Service Components – See Section 3
- b. Government price based on a unit of one; exclusive of any quantity/dollar volume or prompt payment discount. – See Section 4.
2. Maximum order:
 - a. SIN 132-51: \$500,000
 - b. SIN 132.62 \$1,000,000
3. Minimum order, SIN 132-51 and SIN 132-62; \$100
4. Geographic coverage: Domestic, 50 states, Washington D.C., Puerto Rico, US Territories
5. Points of Production: Not Applicable
6. Discount from list prices: Prices shown are Net prices; basic discounts have been deducted
7. Quantity Discounts: 1% on orders exceeding \$350,000
8. Prompt payment terms: 3% – Net 10
9. a. Government purchase cards are accepted for payment at or below the micro-purchase threshold
- b. Government purchase cards are accepted for payment above the micro-purchase threshold
10. Foreign items: None
11. a. Time of Delivery: 30 days ARO or per Statement of Work
- b. Expedited Delivery: Per Statement of Work
- c. Overnight & Two day delivery: None
- d. Urgent Requirements: Agencies can contact Contractor's representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.
12. FOB Point: Not Applicable
13. Ordering Address: IDTP, Inc., 12208 Pueblo Road, North Potomac MD 20878-2064.
14. Payment Address: Same as Contractor
15. Warranty Provisions: Per Statement of Work
16. Export Packing Charges: Not Applicable
17. Terms and Conditions of Government Purchase Card Acceptance: Any thresholds above the micro-purchase level
18. Terms and Conditions of Rental, Maintenance and Repair: Not Applicable
19. Terms and Conditions of Installation: Not Applicable
20. Terms and Conditions of repair parts, indicating date of parts, price lists and any discounts from list prices: Not Applicable
 - a. Terms and Conditions for any other services: Not Applicable
21. List of Service and Distribution points: Not Applicable
22. List of Participating Dealers; Not Applicable
23. Preventative Maintenance: Not Applicable
24. a. Special Attributes such as Environmental Attributes: Not Applicable
- b. Section 508 Compliance for EIT: Not Applicable
25. DUNS Number: 101520364
26. Notification regarding registration in Central Contractor Registration (CCR) Database: Registration valid

Section 3. SIN 132-51/62 Position Descriptions

Senior IT Principal:

Experience: Has a minimum of 20 years experience in the corporate/business environment with at least five years in a senior management position responsible for day-to-day operations of a major business operating unit, or equivalent experience in a corporate senior staff role. Possesses the ability to work with clients at the senior manager level to assess and evaluate the total impact of changes to business and/or operating policy, processes, business rules, products, technology and their integration into overall business plans to meet organizational objectives.

Functional Responsibility: The Senior IT Principal plans, directs, and coordinates all phases of multiple client projects, and/or leads projects. The Senior IT Principal is a member of a senior management team that assesses a client's business and information technology organization to in order to determine and meet business or mission objectives. A Senior IT Principal develops strategic and tactical business/mission objectives, plans and the supporting infrastructure. This individual develops any necessary reports, documentation, solicitations, or other support materials to support client short and long term objectives.

Education: Bachelor's Degree and/or 20 years in progressive middle and/or senior management positions.

Senior IT Consultant:

Experience: A nationally recognized expert evidenced by past performance, publications, or patents, and fifteen years of progressive experience in the design, development and implementation of applicable systems. The specialty may relate to a variety of development, operational or support functions that require special expertise, due to degree of complexity, impact on mission, or novelty of approach.

Functional Responsibility: The Senior IT Consultant is responsible for advising clients on the proper approach to a unique functional problem regarding a hardware/software system, or the design and development of a major new system, or total redesign of an existing system.

Education: A Master's degree and/or 15 years of experience in a field appropriate to the area of consultation is required.

IT Principal:

Experience: Has 10 to 15 years experience in a business environment with demonstrated ability to effectively manage a broad spectrum of management activities to include, but not limited to operations, planning, requirements analysis, process design and development, procurement, logistics, financial analysis, strategic and tactical planning, business case development, risk analysis, and other business and/or information technology activity. Has the ability to understand common and distinct business and/or information technology elements and how they can be enabled to meet the business objectives of the client.

Functional Responsibility: The IT Principal has demonstrated expertise in a functional, information technology, and/or industry-specific business practices. Demonstrates thought leadership and fluency in issue analyses in the business and/or information technology field. The IT Principal assesses the scope and complexity of a client's issues and leads the development and execution of strategic programs. He or She serves as a functional or industry

specialist within the areas of strategic planning, process analysis, benchmarking, organizational alignment, and other operational areas.

Education: Bachelor's Degree or equivalent of 12 to 15 years experience in increasingly responsible positions.

IT Subject Matter Expert I:

Experience: The IT SME has 5 to 12 years experience in a specific area of expertise related to information technology, automated identification, biometrics, image processing, operations, standardization, failure analysis, encryption, PKI, and Integrated Circuit Chip (ICC) definition and application.

Functional Responsibility: The IT Subject Matter Expert provides expert advice and guidance to clients based on their expertise and evaluation of assigned problem areas. Prepare written and oral presentations.

Education: A Bachelor's degree in engineering, technical or management discipline. Ten or more years of specific related experience can substitute for a degree.

Section 4. Pricing

<u>Position Title</u>	<u>Rate/Hour</u>
Senior IT Principal	\$243.06
Senior IT Consultant	\$199.10
IT Principal	\$165.52
IT Subject Matter Expert	\$135.76