



## HELPING AGENCIES MEET IDENTITY MANAGEMENT MANDATES

### EDS ASSURED IDENTITY™ SOLUTION

The Homeland Security Presidential Directive 12 (HSPD-12) sets policy for a common identification standard for federal employees and contractors, requiring agencies to be fully compliant by October 2008. EDS, an HP company, can leverage its extensive identity management experience, including smart cards and biometrics, to help government organizations meet HSPD-12 and other government mandates.

#### **Business challenges**

In recent years, the federal government has enacted laws, regulations and directives that require agencies to secure information systems and data privacy. HSPD-12, Federal Information Processing Standards (FIPS) 201 and corresponding Personal Identity Verification (PIV) standards and guidance outline an overall protection of privacy with which agencies are directed to comply. Government agencies need an identity management solution that provides secure and reliable identification of its employees. The solution must converge logical and physical access control systems. And it must meet the newly created FIPS 201 standard, associated special publications and Office of Management and Budget guidance even as those requirements are being defined.

#### **How we can help**

The EDS Assured Identity™ solution helps government agencies address HSPD-12, FIPS 201 and corresponding standards. It is a wholly integrated secure and scalable system that allows agencies the capability to efficiently implement a compliant system with minimal cost. Built on our robust identity management capabilities, EDS Assured Identity™ is a one-stop shop for agencies needing to meet the deadline for HSPD-12 compliance. The EDS Assured Identity™ solution has been approved by the U.S. General Services Administration (GSA) and is available on GSA Schedule 70. EDS is ready to help government agencies meet these requirements – now.



## WHAT YOU CAN ACHIEVE

### Identity and Access Management Capabilities

- Role-based identity lifecycle management - Provides centralized administration of employee identities and facilitates mapping them to client-defined user groups and roles.
- Identity provisioning - Propagates, from a central location, identities and assigned privileges to resources distributed throughout the enterprise in support of logical and physical access control.
- Federation - Allows an agency the ability to share identity information with other agencies and authorized organizations.
- Logging, auditing and reporting - Maintains a record of activity that allows the agency to enhance non-repudiation capabilities, identify responsible parties for all activities, and analyze processes and procedures in order to increase productivity or implement changes.
- User authorization based on PIV roles - Separation of duties as specified in FIPS 201 are satisfied and enforced by making operators authenticate with their card prior to accessing various systems.
- Fully integrated common user interface for PIV front-end systems - Provides a single common user interface across PIV functional systems. Eliminates need to toggle between various COTS products to complete process. Reduces training initiative and improves usability for the end user.
- Data sharing and automation environment - Promotes consistent data across PIV functional systems and reduces amount of data entry for the operator.
- Layered security framework - Creates secure environment by implementing various technologies to verify the identity of an employee prior to entry into the system.
- End-to-end identity management solution - Provides an overall solution that integrates existing agency systems with new PIV systems including both logical and physical access control systems.
- Easily integrates different vendor technologies as needed - Allows the agency flexibility to choose the best-of-breed technology, swap out products as a result of technology enhancements, end-of-life product life-cycle events, or vendor relation and/or company solvency issues without having to change the user environment.
- Secure communication and data storage - Provides a secure mechanism for communicating and storing sensitive data including biometrics.

- Interface designed as PIV specific - User interface is designed for PIV and does not have extraneous features found in many COTS products.

### Pre-Enrollment, Identity Proofing and Registration

- Pre-enrollment Web portal with event notification feature - Provides sponsor ability to create new employees, import existing employees and notify the employees via e-mail or other specified methods. Provides online capability for the generation of the SF 85 allowing the data entry to be performed over a span of time.
- Dynamic electronic data collection and population of employment forms such as SF 85 - Allows employees the capability to enter data required by agency employment forms. The data is collected electronically over a span of time, verified and imported into an employment form for submission to the Registrar.
- Batch import capability for existing employees - Allows the sponsor the ability to import existing users from an HR database or other data repository.
- Ten fingerprint capture, segmentation and generation of EFTS file for submission to FBI - Electronic capture of the 10 fingerprints allows the agency an expedited means for identity verification. Fingerprint capture is completely integrated into common user interface creating easy capture process for the operator.
- Electronic identity source document authentication and data capture - Electronically interrogates documents to ensure required security features are present and to validate the authenticity of the presented identity source documents. Data is captured during the authentication limiting the amount of data that has to be entered by the operator.
- Electronic identity source document storage - Enhances the paperless environment and provides a secure electronic storage of the identity source documents for comparison during issuance.
- Simplified photo capture with auto optimization for ANSI/INCITS 385-2004 - Captures optimized image while limiting the amount of effort for the operator.

### Biometric Management

- Biometric duplicate enrollment check - Layered security approach enables the agency to check existing users in the database to make sure the new user is not already enrolled.
- Ten fingerprint secure storage in standard WSQ format - Securely stores biometric data in an industry standard format allowing interoperability and future compatibility.



## Credential Management

- Fully integrated interface to back-end card management system - Integration into common user interface limits the amount of functionality that may be available through the COTS user interface. Tasks that are needed to be completed for identity verification are accomplished in an easy and intuitive manner.
- Fingerprint biometric verification prior to card issuance - Layered security approach allowing the agency to ensure the person issued the card is the same person that was present during the identity proofing and registration process.
- Dynamic creation of card topology based on PIV applicant designation - Allows the agency the flexibility to issue cards to various employees and contractors with print preview capability.
- Applicant acknowledgement and electronic signature capture - Provides the employee with directions for use and process for when a card is lost stolen or left at home. Also provides privacy information addressing the use and storage of biometric data.

## Logical and Physical Access Control

- Convergence of logical and physical access control systems - Creates a homogeneous solution with information sharing across IT networks and physical access control systems controlling agency facilities. EDS understands the complexities and existing issues in migrating existing PACS systems to fully compliant target state PACS.
- Single sign on - Provides an efficient authentication mechanism for agencies and enhances the user experience with the overall system.
- Authentication and authorization - Provides mechanism for authentication of the credential and the identity associated with the credential as well as the authorization associated with the identity.

## WE'RE READY TO HELP YOU MEET HSPD-12 REQUIREMENTS NOW

After all, establishing secure credentials is something we've done more than 17 million times. Our proven, end-to-end authentication solutions are already helping government clients address critical security and privacy issues every day.

- EDS has more than 10 years' experience in federal biometric, card-based and access control systems.
- The EDS Assured Identity™ solution, built on field-proven components and processes, is specifically designed to meet the needs of HSPD-12. EDS Assured Identity™ is an integrated,

modular and scalable solution for enrollment, registration, issuance and management services. GSA has qualified EDS as an end-to-end HSPD-12 service provider and EDS Assured Identity™ has been approved by GSA as a bundled product. In fact, in April 2007 GSA selected EDS to provide the HSPD-12 shared services solution, including infrastructure and registrars, providing credentials to an estimated 420,000 federal government employees and contractors at 40-plus agencies.

- EDS is the only IT services integrator to have implemented a massive-scale smart card solution for the U.S. government, serving as the prime integrator for the largest advanced smart card program for the U.S. Department of Defense's Defense Manpower Data Center (DMDC). EDS has delivered more than 16 million common access cards to DMDC to date.
- In support of DMDC, EDS also helped develop and deploy the Defense Biometric Identification System (DBIDS), the DoD's broadest physical access system, which includes biometric authentication. Currently, more than 1.2 million U.S. military personnel, family members and contractors globally are registered in the system.
- EDS developed ExpressEntry<sup>SM</sup>, a biometric automated inspection system, for passport control at Israel's Ben Gurion Airport near Tel Aviv for Israeli frequent international travelers. Since the pilot was started in 1998, 340,000 Israeli citizens have enrolled.
- The Ben Gurion ExpressEntry<sup>SM</sup> system won the AFCEA Inaugural Golden Link Award for Excellence and Innovation in Government Operations.
- The ExpressEntry<sup>SM</sup> framework enabled a three-month or less turnaround on similar projects such as the U.S. Transportation Security Administration's (TSA) Registered Traveler program.
- EDS supported the TSA in implementing the Registered Traveler program at Boston's Logan and Washington's Reagan National airports. Registered Traveler used smart cards and biometrics - iris images and electronic fingerprints - to confirm identities and expedite travel without compromising security. Many processes necessary for HSPD-12 compliance were implemented for Registered Traveler, including identity proofing, registration and card issuance. EDS successfully enrolled nearly 4,000 passengers and facilitated more than 25,000 passenger authentications during the pilot.
- In 1995, EDS helped the U.S. Immigration and Naturalization Service implement INSPASS, an automated inspection system designed to shorten the inspection process for low-risk travelers entering the United States by airplane. INSPASS used hand geometry to verify



## About EDS

EDS, an HP company, is a leading global technology services provider, delivering business solutions to its customers. EDS founded the information technology outsourcing industry more than 46 years ago. Today, EDS delivers a broad portfolio of information technology and business process outsourcing services to customers in the manufacturing, financial services, healthcare, communications, energy, transportation, and consumer and retail industries, and to governments around the world.

the identity of travelers at automated inspection stations. More than 90,000 travelers enrolled in the program.

- EDS served the Israeli Ministry of Defense and the Israeli National Police by developing and installing an innovative biometric fusion-based border control system. The system was designed to monitor the entrance and exit of more than 50,000 daily workers to the Israeli territories. It provided improved security and efficiency of automatic inspection of passengers by applying innovative integrated biometric technologies of hand geometry and facial recognition, as well as contactless smart cards.
- EDS serves as Europe's largest provider of non-financial smart cards, with the rollout of 4 million cards for the UK Card Account at the Post Office.
- EDS is a founding member of the Federation for Identity and Cross-credentialing Systems (FiXs), an industry consortium supporting the DoD in building and maintaining an interoperable identity cross-credentialing network focused on protection, trust, standard operating rules, policies and technical standards.
- EDS partners with world-class, industry-leading biometric and identity technology companies, integrating production proven security solutions and institutional knowledge to deliver high-quality solutions to support critical business processes and needs.

## Contact

David Troy  
Director of Identity  
Management Solutions  
EDS, an HP company  
phone: 703.742.1887  
e-mail: david.troy@eds.com  
visit: www.eds.com