BearingPoint

Roadmap to FIPS 201 Implementation: Managing the Project

Smart Card Alliance – Washington, DC

May 1, 2006

Agenda

- HSPD-12 / TWIC Overview
- Managing the Project
- PIV Business Practices
- Case Study: Transportation Worker Identification Credential
- Summary

BearingPoint

HSPD 12 / TWIC Overview

HSPD-12/FIPS 201 / TWIC Purpose

- **Nationwide implementation of a secure identification credential for government employees and contractors / transportation workers.**
  - Strong, distributed, and authenticated physical and logical access facilitated by a uniform credential.
  - Creating a chain of trust that ensures cardholders' identities
- **Overarching Goals and Specific Objectives**
  - Goals include protecting and enhancing Privacy, Security and Commerce
- **Obeying and Fulfilling Laws and Directives**

FIPS 201 / TWIC Interconnection

The development of FIPS 201 was closely monitored and supported by TSA. Likewise, the development of the TWIC Prototype system was closely monitored by a number of those authoring FIPS 201. As a result, the majority of the components of the TWIC system were designed and implemented in alignment with FIPS 201.

In fact, there were many strategic reasons for which implementing officials created a TWIC process to be closely aligned with the PIV standards. Some of these include:

- Demonstrate the functionality of PIV, providing a template and lessons learned for other government agencies;
- Secure critical facilities using the same secure process as the Federal government;
- Cutting edge technology and process;
- Interoperability during a disaster.

FIPS 201: PIV 1 and PIV 2

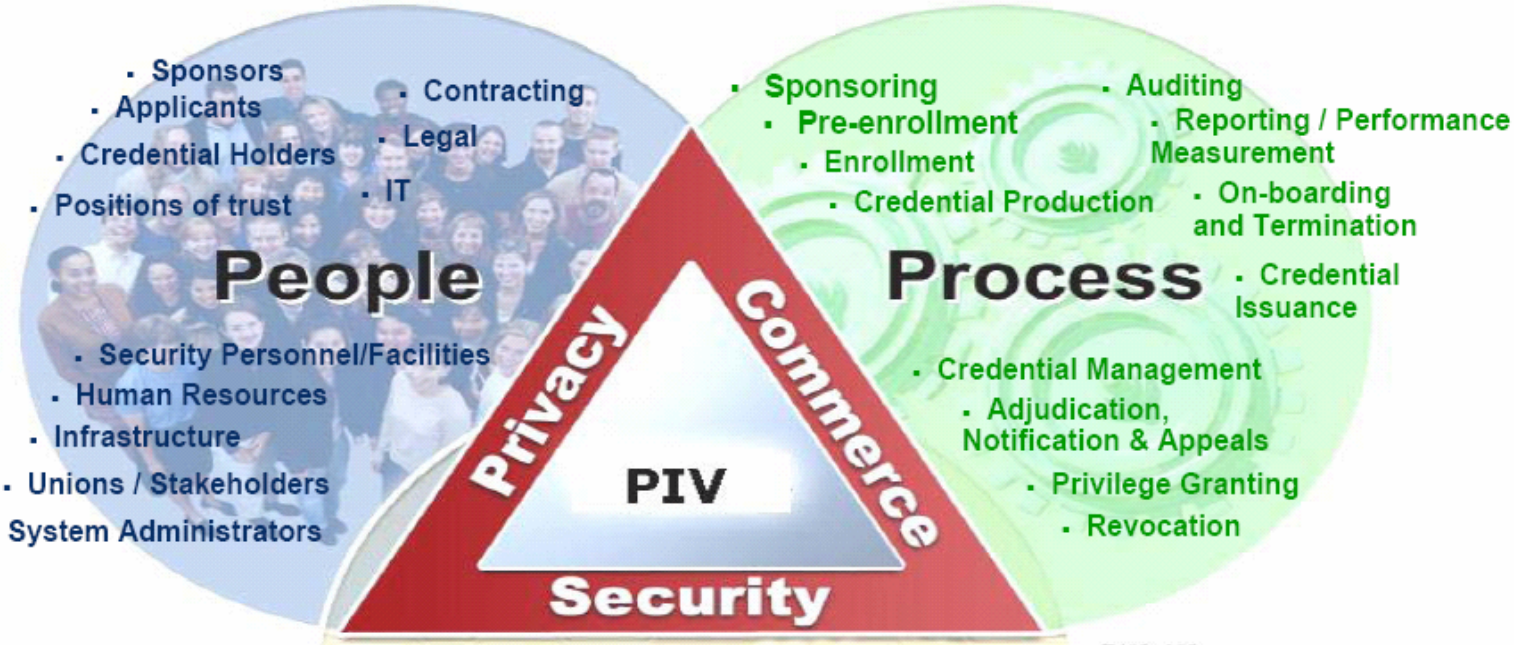
- Procedural alignment with PIV I – No single person involved in the TWIC lifecycle can issue, revoke, or produce a TWIC.
- Pre-enrollment Interfaces – FIPS 201 compliant solutions must deal with interfaces to legacy systems as part of the formation of a full identification record. TWIC standardizes this behavior in its legacy conversion import functions (Extensions of the pre-enrollment/sponsorship processes)
- Separation of access and identity – FIPS 201 makes identity proofing the first part of the process; access privileges are granted only once an identity has been validated and associated with a strong credential through a reference biometric. TWIC takes the same approach.

BearingPoint

Managing the Project

Focus on People, Process & Technology

PIV goes beyond just Technology.



Technology

- Enrollment workstations
- Applications and hosting
- Physical Access Infrastructure
- Databases / reference systems
- System Administration
- Interface tools for background checks
- Card Personalization and Inventory Management System
- Public Key Infrastructure
- Card Management System
- Notification and Reporting Tools
- Web-based portal
- Work flow
- Smart Cards, readers, printers, related consumables

Programmatic / Technical Challenges

Many items in implementing these systems are long lead items and must be addressed in planning; these include:

- Card topology
- Card data model
- Public Key Infrastructure
- Biometric infrastructure
- Hosting set-up, configuration and testing
- Training and certification of key users
- Security assessments
- Privacy assessments
- Help desk
- Communications / Awareness
- FIPS 201 Process Validation
- FIPS 201 Product Validation
- Legacy System Integration
- Automation
- Standard Operating Procedures
- Adjudication
- Application testing and fielding
- Card Personalization

BearingPoint

PIV Business Practices

PIV Business Practices

Practices are groups of Business Processes that are governed by overarching policies; these processes provide the foundation for Standard Operating Procedures and should govern the technical requirements and supporting implementation

Credentialing Practices

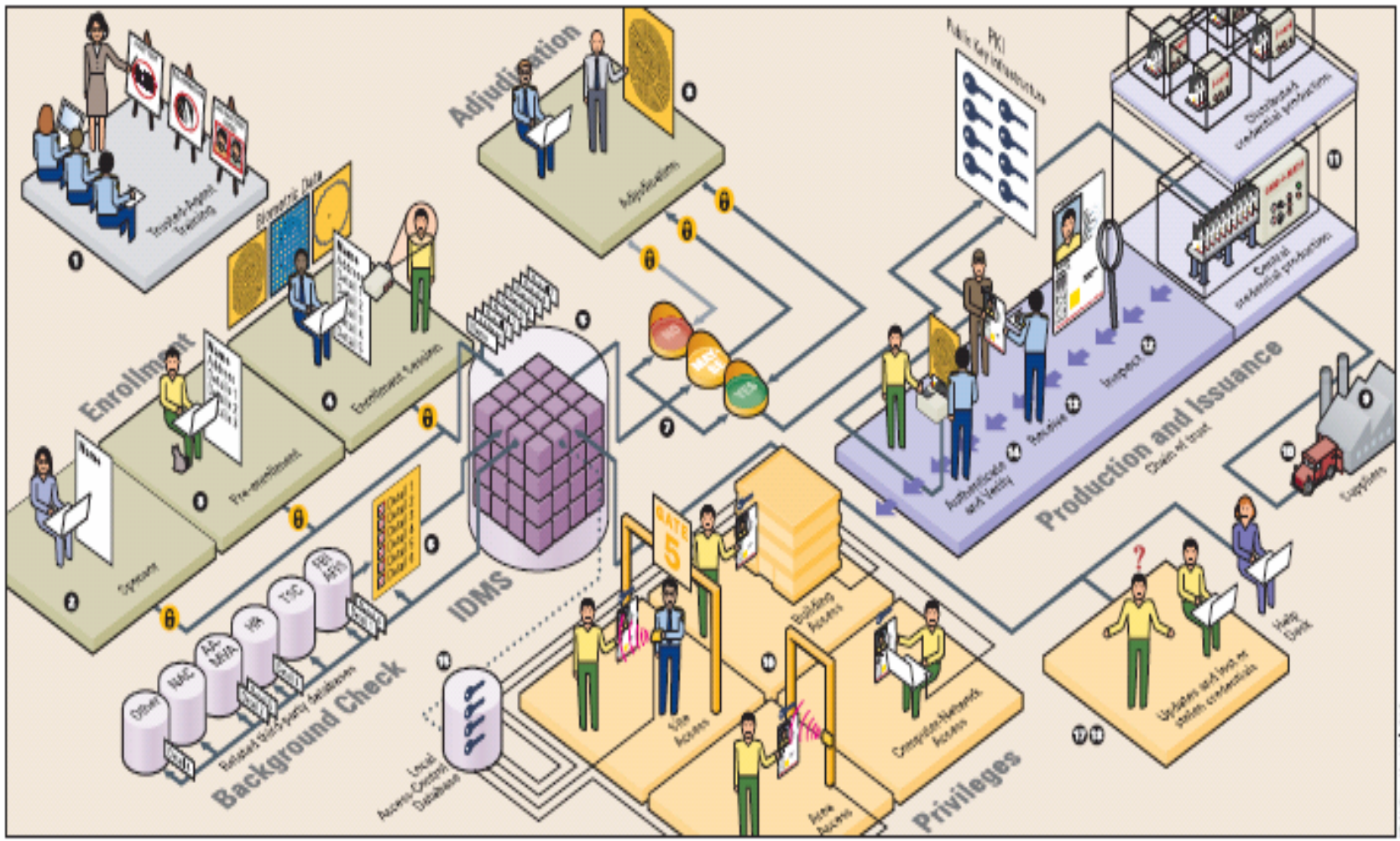
- Sponsoring
- Identity Proofing
- Identity Vetting
- Credential Issuance
- Revocation of Credential

Integration of physical and logical access to common business model

- Directories
- User Provisioning
- Privilege Granting

Other Practices

Credentialing Processes



PIV Practice: Physical / Logical Access Integration, Process – Authentication

Business issues:

- **Directory and Group structure: e.g., single forest, multiple forests, etc.**
- **User Provisioning**
- **Access control conditions: e.g., Times of Day (only permitted to access areas specific times of day, not on weekends, not after hours), Permission issues**
- **Distributed applications: requires that card status, link between card and individual and issuer / data should be verified**

PIV Practice: Other Best Practices

- **Privacy Protection at every step**
- **Using Performance Metrics to measure system and performance; important to align metrics with program goals**
- **Stakeholder involvement (e.g., communication planning)**
- **Re-Use of existing systems**

BearingPoint

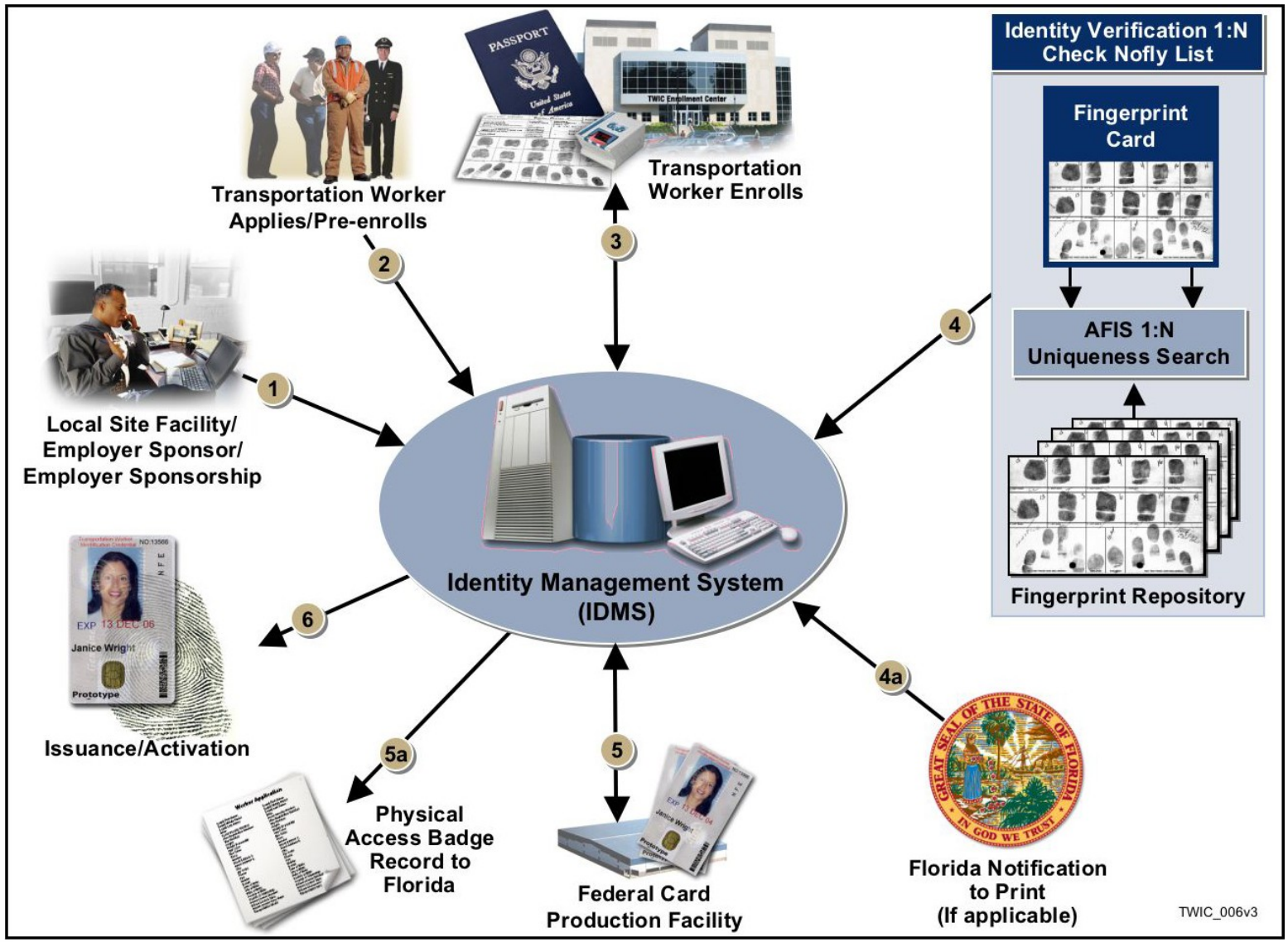
Case Study: TWIC Business Practices

End-to-end credentialing with physical and logical access

Case Study: TWIC Phase III Business Practices

- End-to-End Credentialing, Identity Proofing, and Identity Vetting
- Standards-based – Maximum compliance with HSPD 12 before specifications finalized
- Strong Supporting Elements
- User Guides for every subsystem
- Standardized and well-documented standard operating procedures
- Trained and certified Trusted Agents issuing credentials

Case Study: TWIC Phase III Process



BearingPoint

Summary

Managing the project with an initial focus on people and process

Lesson: Developing the TWIC system on the bleeding edge of FIPS provided the foundation for a standardized credentialing system and offered the following lessons:

- Credentialing practices must be founded firmly in PIV processes
- Integration of physical and logical access to common business model, including Directories, User Provisioning, and Privilege Granting promote interoperability
- Interactive design sessions are key to a successful system development and implementation

- Business process and policy are intimately inter-related to technical functionality

Benefits:

- Well founded processes and policies will drive technology, preventing technologies from driving poor business processes.
- Awareness of policies and procedures drives customer satisfaction and efficiency

Contact Information

BearingPoint
Business and Systems Aligned. Business Empowered.

Gordon Hannah
Managing Director
Security & Identity Management Practice

6564 Loisdale Ct.
Springfield, VA 22150
www.bearingpoint.com

Tel: +1.703.253.2517
Mobile: +1.
E-mail: gordon.hannah@bearingpoint.com

BearingPoint®

Global Management & Technology Consulting