PIV Workshop

Department of Homeland Security

Joe Broghamer

October 7, 2004

Authentication

Good Guys

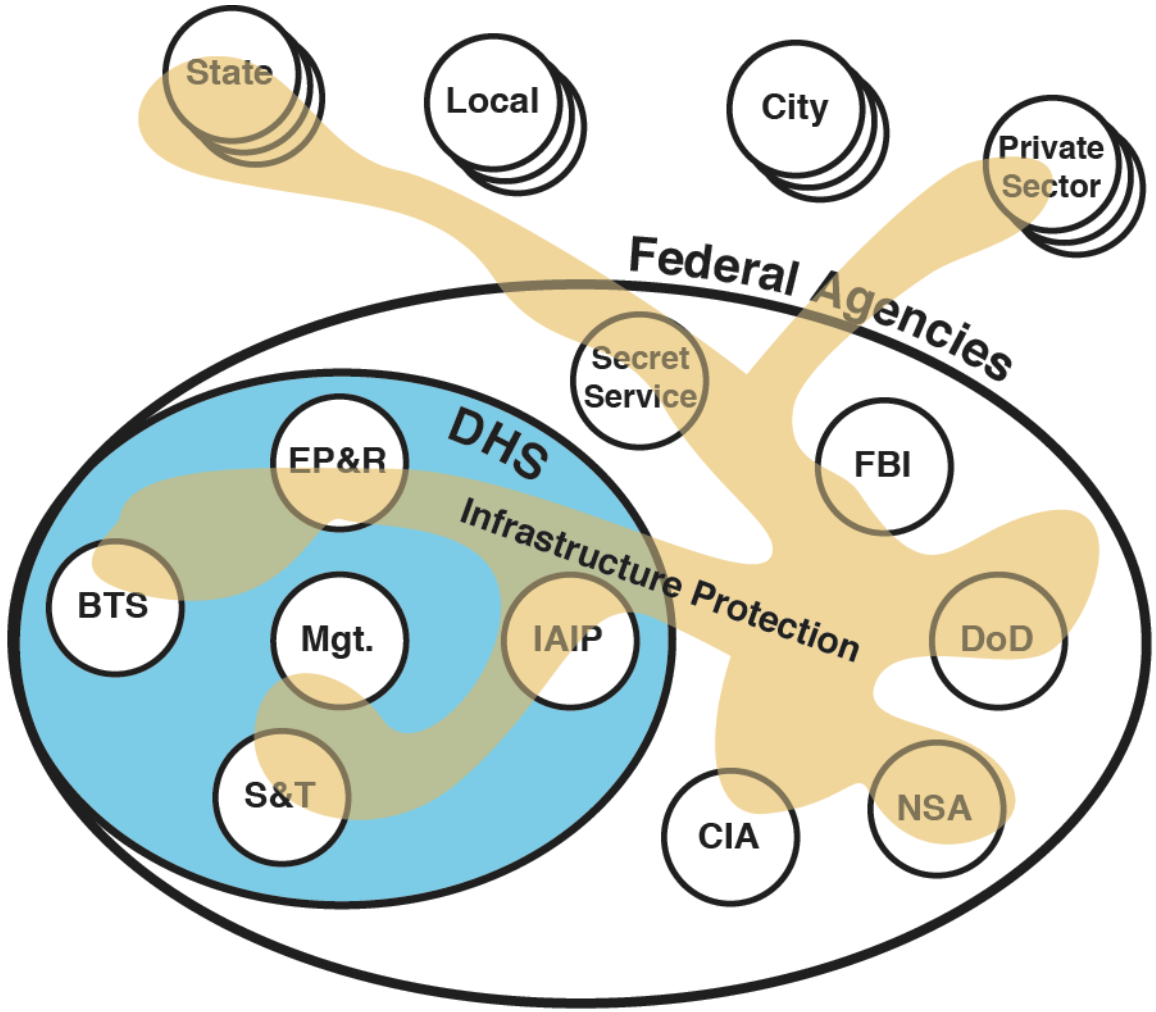
vs.

Bad Guys

Paradigm Shift

> Security = Less Functionality

Communities of Interests



Problem (Multi-tokens)

Vision

- **One Card**
  - **Same token (smartcard) used to enter facilities, log on to desktop computer, and access appropriate services and data stores no matter where they exist**

Improved

– Functionality

– Security

Objectives

- Single Log-on
- Client authorization to secure web-sites (SSL)
- Digital Signature and encryption for e-mail (S/MIME)
- Workstation protection & Local File Encryption
- Support E-commerce
  - Document Signing
  - Certified Document Routing
  - Certified Time Stamping
- VPNs (remote access)
- Wireless Protection (ex: Blackberry)
- Multi-function token (Java-based)
  - Applications can be added in the field (after issue)
- Facility Access
  - Card only (single factor identification)
  - Card and PIN/Biometrics (two and three factor identification)

DHS Access Card (DAC)

Multi-purpose
- Physical Identification
- Cyber Identification
- Building Access (proximity)

Java (add applications in field)

Storage of biometrics

Vendor Neutral

Standards Based

Accomplishments

- **Card Issuance System Implemented**
  - **Single credential Issuing Process**
    - Modified Commercial Product (problems)
    - Custom Developed Application (solution)
  - **Interfaces with cyber and physical systems**
- **Support for Standards**
  - **Government Smart Card Interoperability Specification, version 2.1**
  - **Government developed applets and middleware**
- **Secure Web site**
  - **Client-side Authentication**
  - **Multi-level of access**
  - **Used for “First Responders” to issue Class 1 Certificates**
- **Token for Homeland Secure Data Network (HSDN)**
- **Documentation**
  - **User handouts & Verifying Official (VO) Manual**
  - **Certification and Accreditation**

Smart Card Specification

- ISO 7816, 1,2,3 compliant
- FIPS 140-2, level 3
- Java Applications
  - PKI Applet
  - ID PIN Verification and Management Applet
  - GCA Applet
  - Authentication Applet
  - Biometric Authentication Applet
  - Stake Holder applets (future)
- JavaCard 2.1
- Global Platform 2 Compliant
- 64 K RAM (42K available for applets)
- DES/3DES/AES(when available)
- RSA asymmetric 1024 / 2048
- PTS speed in access of 9600 bps
- EEPROM endurance > 250,000 r/w cycles
- MIFARE Proximity (contactless) chip
  - DESFire (ISO 14443-A)
  - 4 k NV memory

DHS Initial Implementation

- 50 Participants
- Start June, 2004
- Physical Access (3th and 4th Floor, 7th and D Street, SW)
- Cyber Access (Cryptographic logo on)
- Sign and Encrypt E-mail (S/MIME)
- Client-side Secure Access to DHS On-Line Web site
- Certified Time Stamping
- Remote Access
- Secure Wireless Support
- Multi-signed Document Routing

PKI Functions

Public Key Infrastructure

Servers

Software

Clients (End Users)

Database Structure

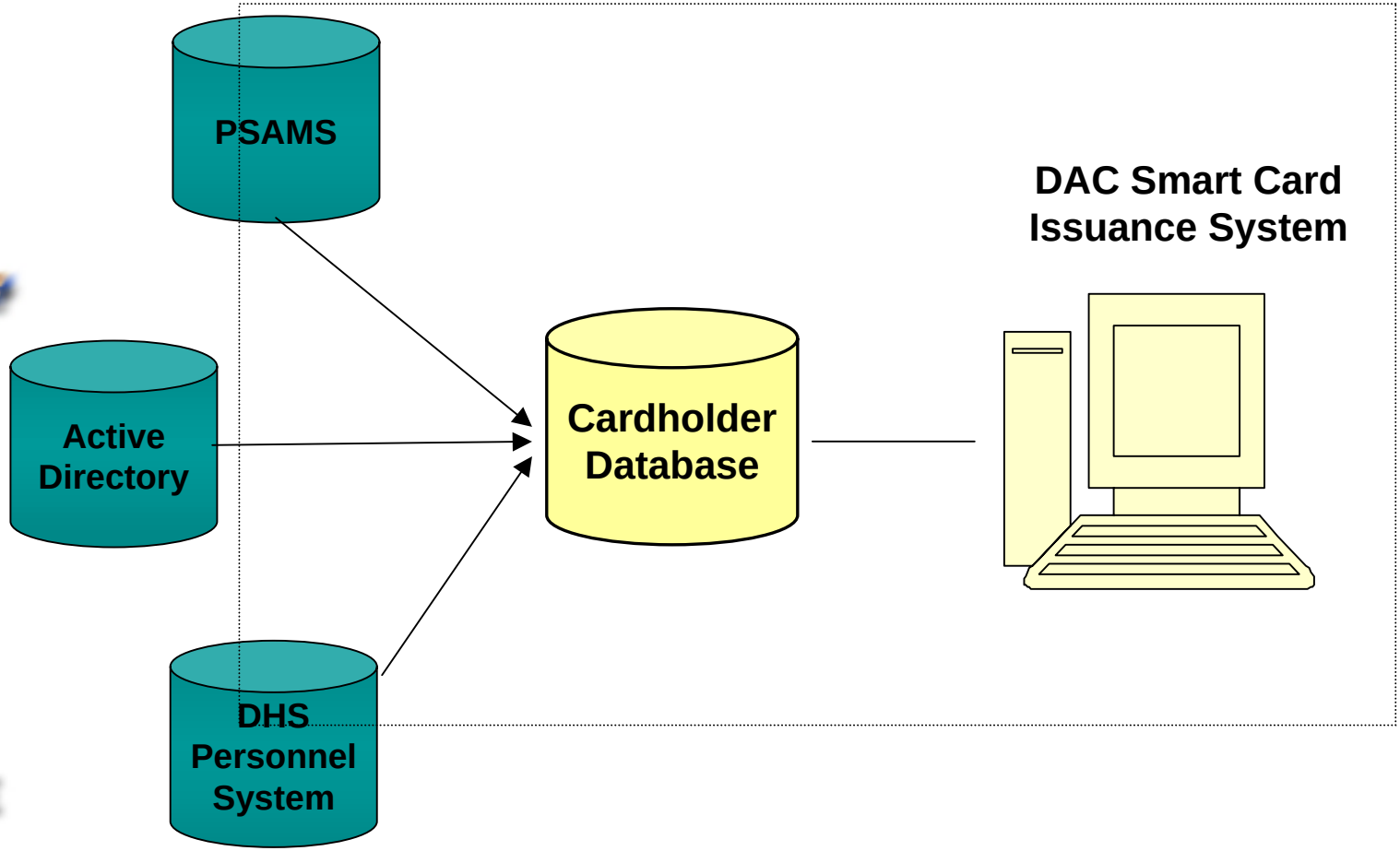


Image Capture System

- **Ease of Installation**
- **Simple Implementation**
- **Low Maintenance**
- **Durability**

Image Capture Procedure

Image Capture Procedure

Image Capture Procedure

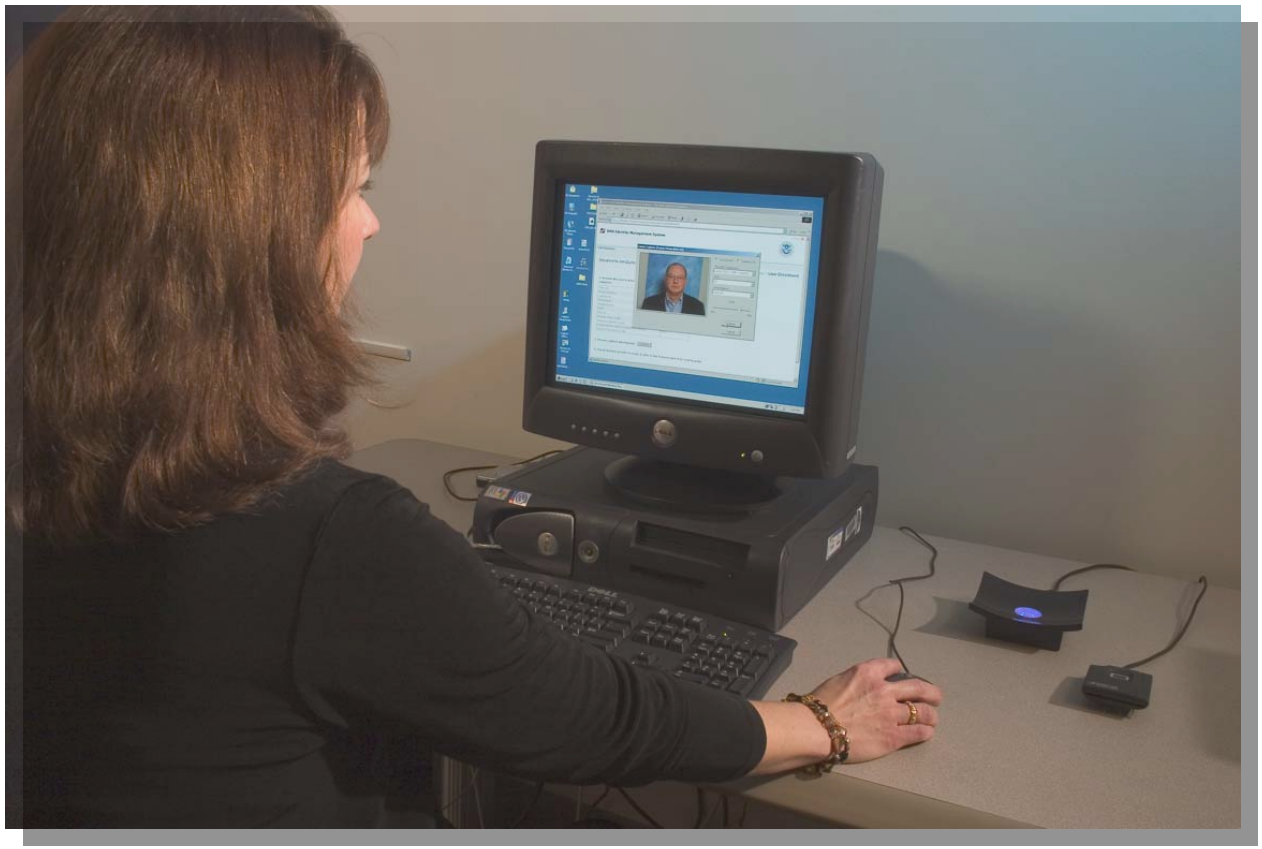


Image Capture Procedure

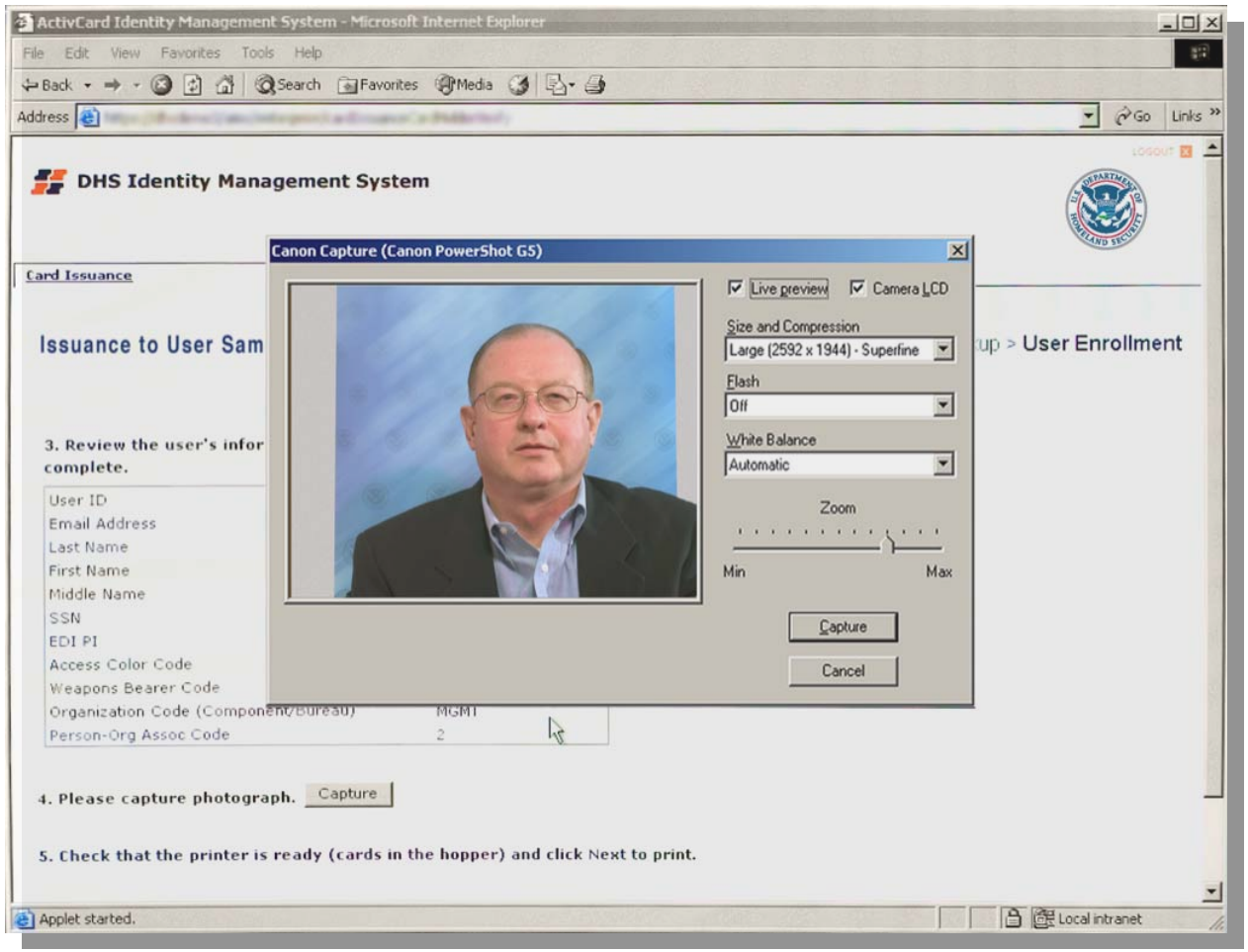
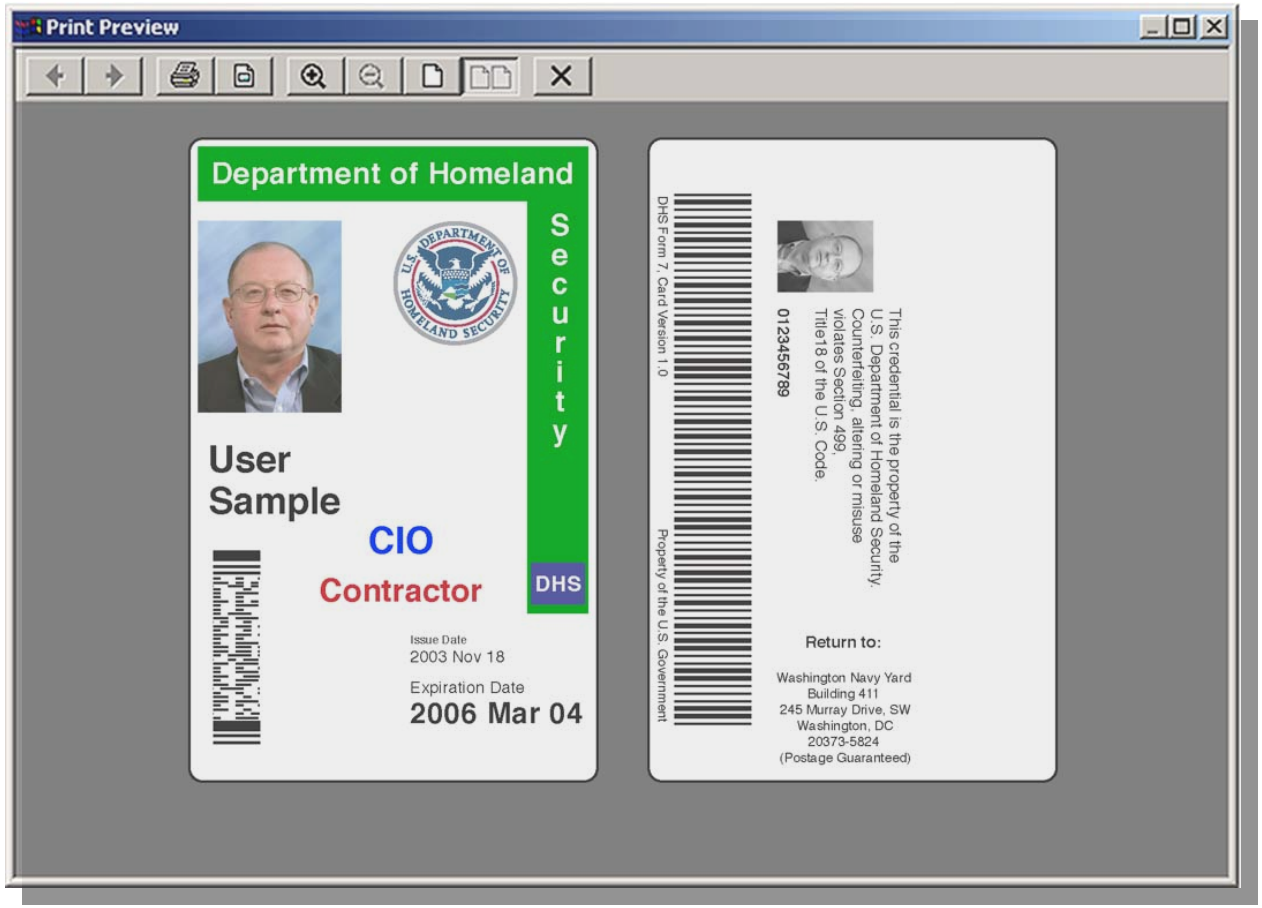
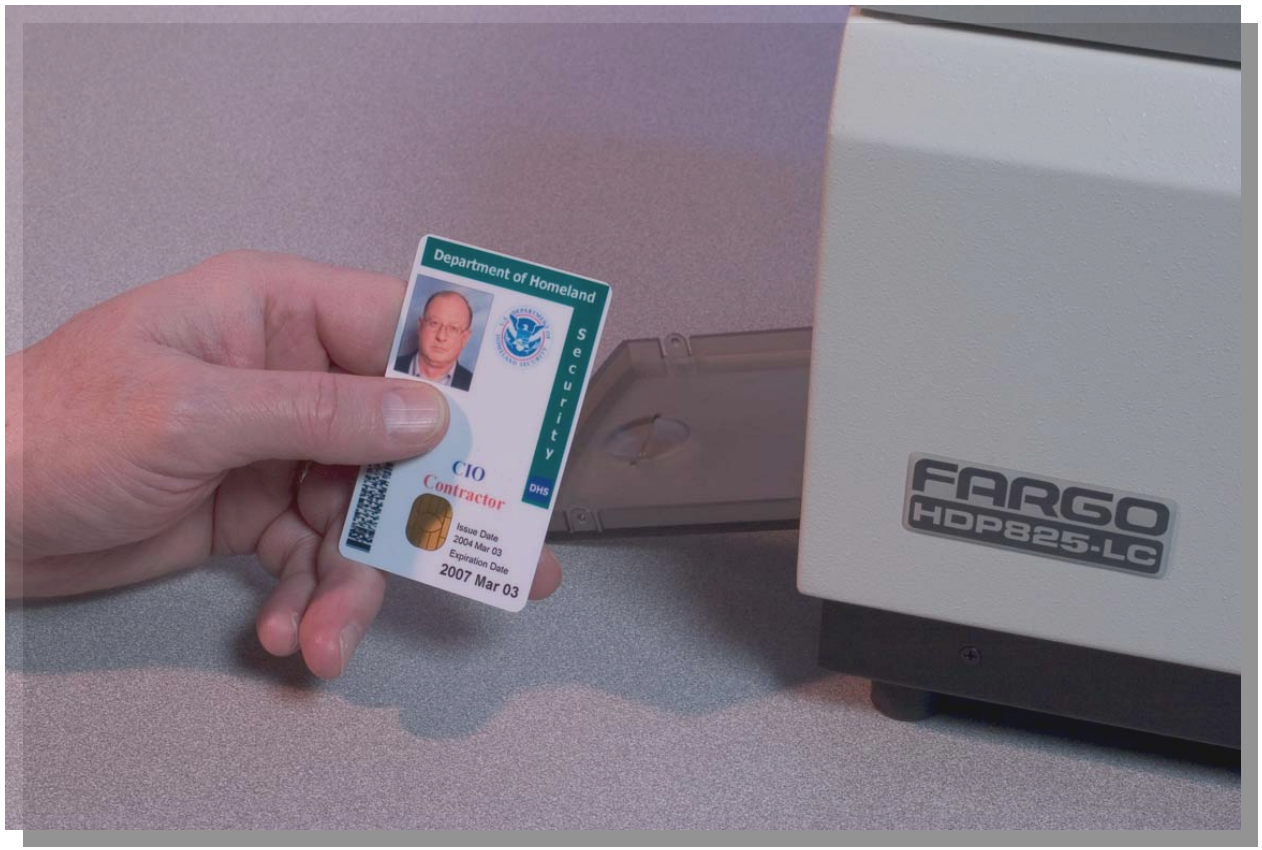


Image Capture Procedure



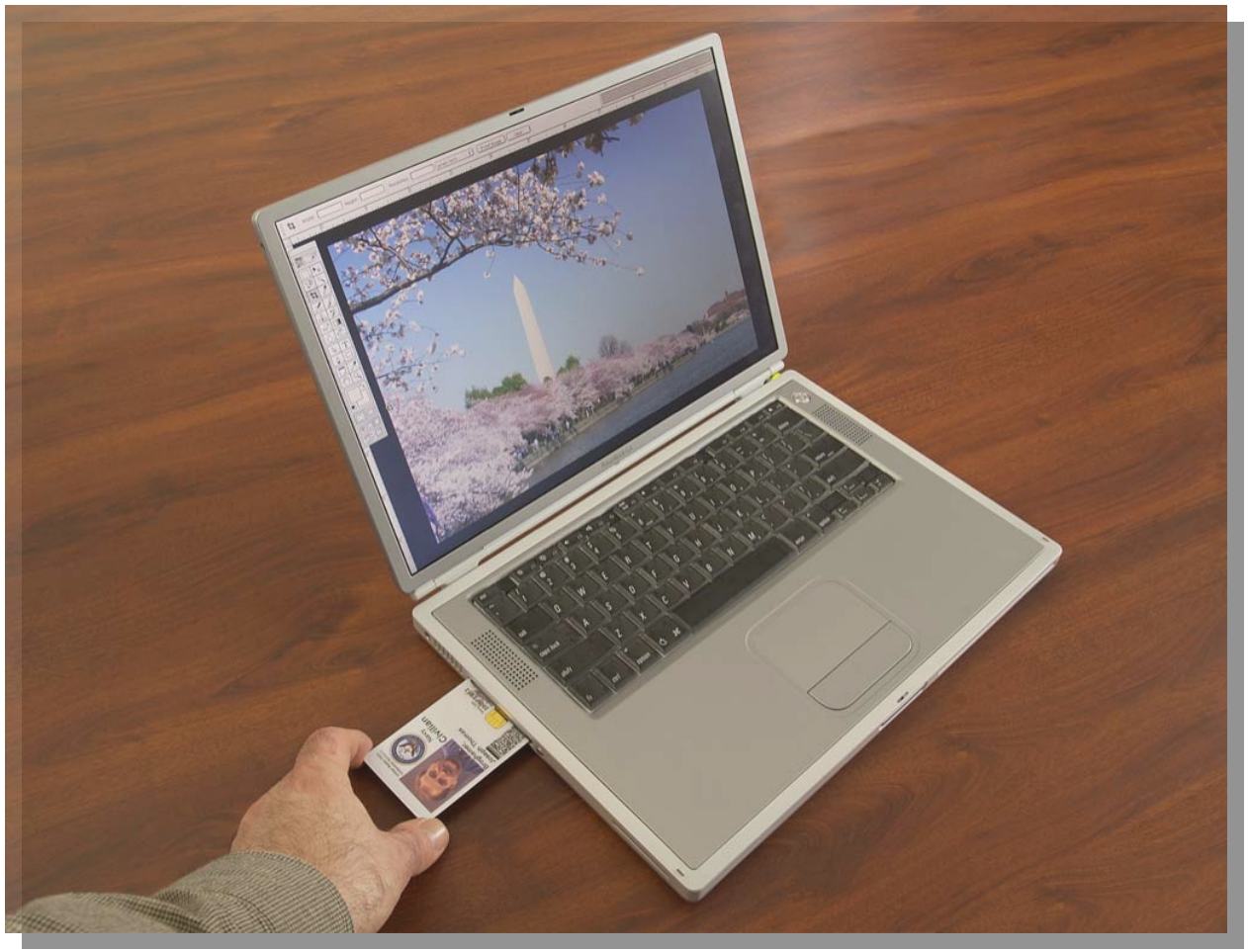
Printed Smart Card



Encoding The Biometric Template

Encoding The Unique Identifier

Computer Access Control



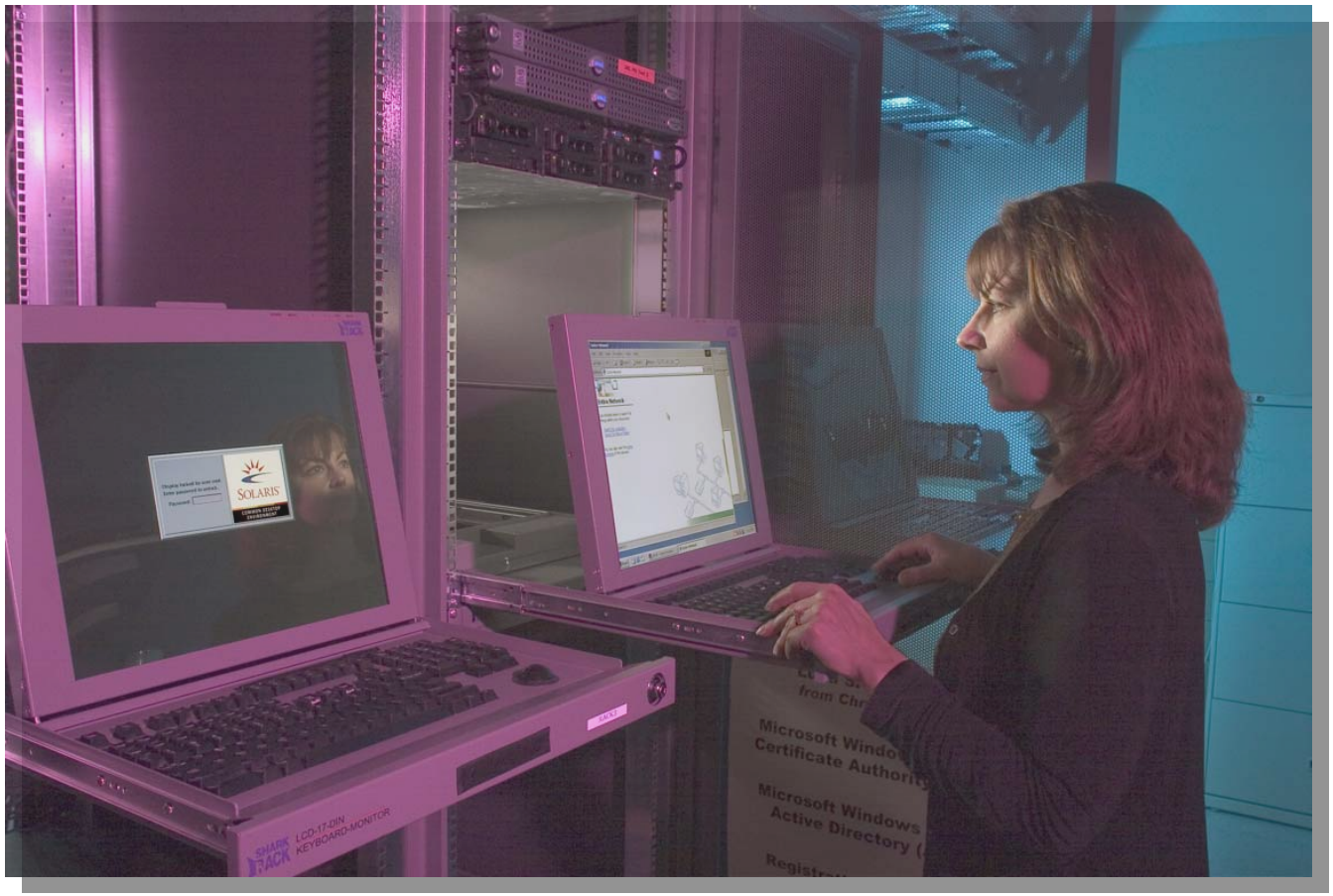
Biometric Enabled Keyboard

Physical Access Control Failure

Physical Access Control Success

Physical Access Control
Biometric Validation

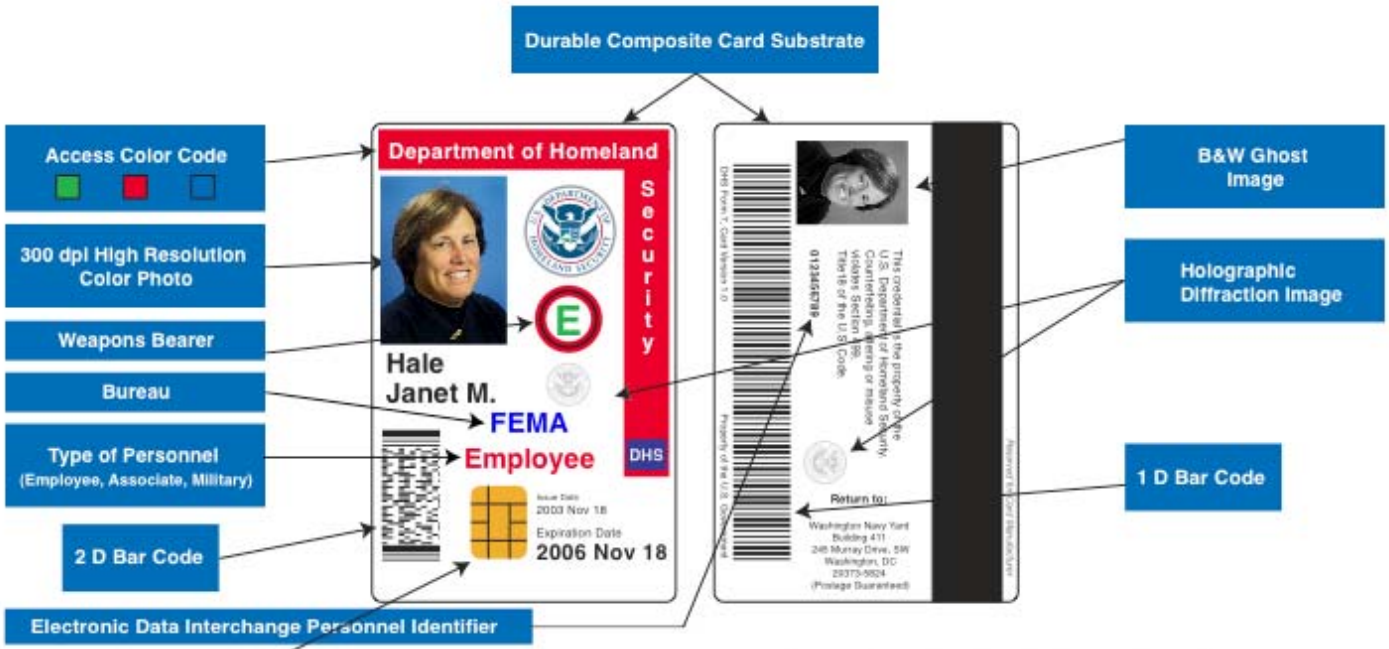
Secure Web Servers



Secure Web Site

Card Layout

DHS Identification Smartcard



Contact Chip:

- Java Card 2.1 w/cryptographic co-processor
- 64 K EEPROM
- 3 Certificates (Identification, Signing, Encryption)
- FIPS 140-2, level 3 Certified
- Symmetric Algorithms (DES, 3DES, AES)
- Asymmetric Algorithm (RSA 1024/2048)
- GSC IS 2.1 Compliant
- Global Platform 2 Compliant
- 50% Available for Future Applets

Proximity Chip (embedded/not shown)

- ISO 14443-A/B
- DESFire-g (card/reader authentication)
- GSC IS 2.1 Compliant
- Read Range: 10 cm

Standards

- Java
- PKCS
- FIPS-140-2
- Microsoft API
- Global Platform
- Common Criteria
- Public Key Infrastructure X (PKIX)
- International Telegraph Union (ITU)
- Internet Engineering Task Force (IETF)
- Government Smartcard Interoperability Standard (NIST)

Project Management

- **Three Approaches for Project Management**
  - **Contract Out PM and Technical Solution**
    - GSA approach (provides contracting and acquisition assistance)
    - No Requirement for Government Functional Experts
    - No Incentive for Standards or Interoperability
    - Reduce Government Control over Approach or Results
  - **Government Project Management, Contractor Technical Solution**
    - More Government Oversight
    - Improved Interoperability
  - **Government Retains Project Management Government Chooses Technical Solution (Components)**
    - Maximum Adherence to Requirements
    - Maximum Support for Standards and Interoperability
    - Solution Maximized for Government Benefit
    - Source Code and Libraries owned by Government

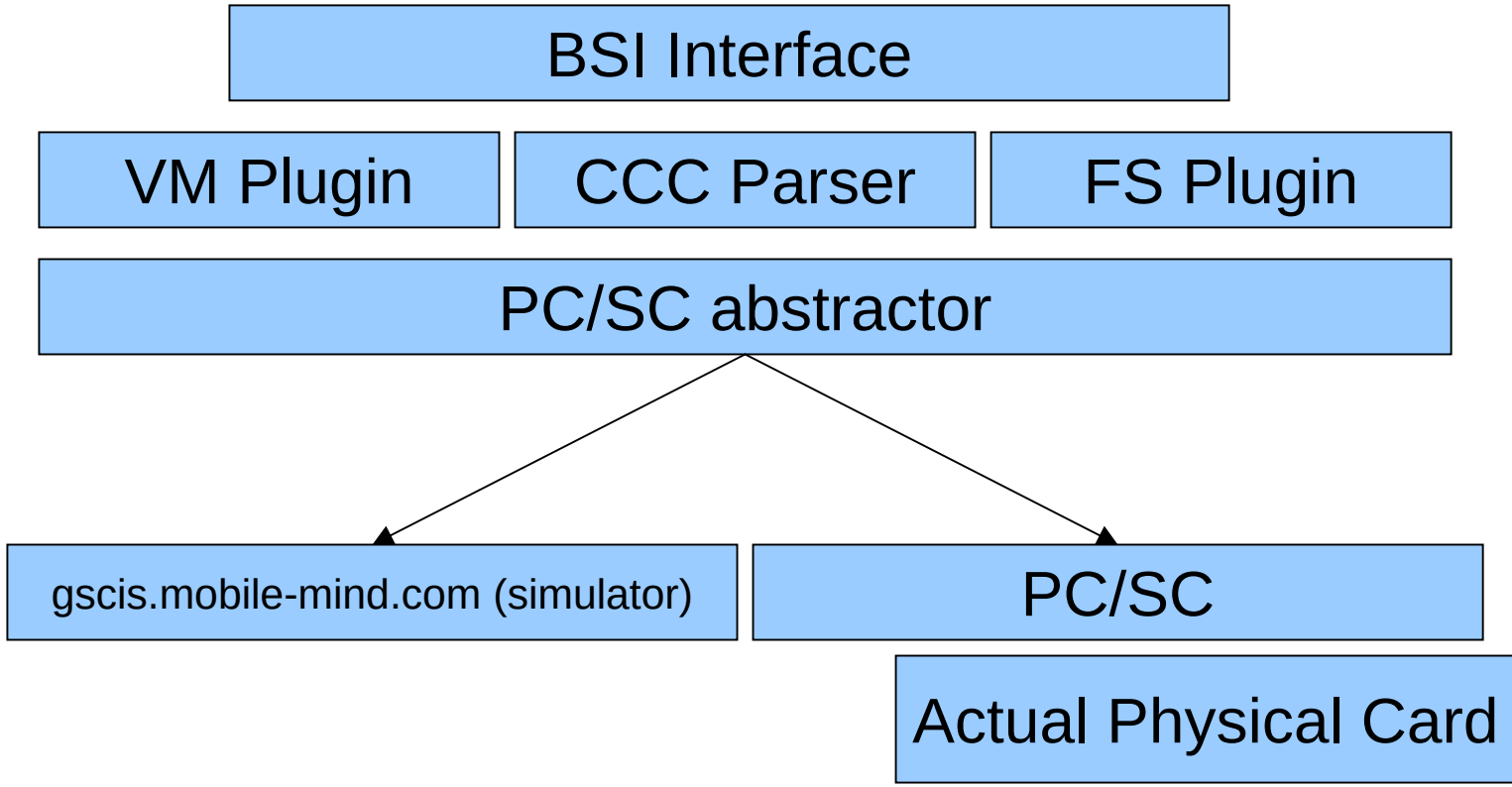
Implementation Strategies

- **DHS**
  - **Card Management (CM) System**
    - "Long Pole in the Tent"
    - Requires Customization of Commercial Application
    - Integration (physical & cyber)
    - Web vs. Client application
  - **Our Solution: Develop CM Front End**
  - **Linkage with Enterprise Database**
    - Human Resource (HR)
    - Security (clearance information)
  - **Linkage with IP-based Physical Access Systems**
    - Single initial credential issuance
      - Who you are?
      - Have you been revoked?
    - Relying party access control
      - Granularity of access control
      - Post-issuance modification to SEIWG string
  - **Digital Imaging**
    - Primary reason for Smart Card form factor

Reference Implementation Goal

- **NIST has undergone the development of a reference implementation of GSC-IS 2.1**
  - **To provide a reference BSI that can communicate with both native GSC-IS 2.1 VM and File System cards**
  - **To provide a reference GSC-IS 2.1 simulator for VM and File System like card edges.**
  - **To surface ambiguities in the current GSC-IS 2.1 specification and provide guidance for implementers**

Architecture



Card-Edge Simulators

- **Progress**
  - **VM “usage” simulator completes GSC-IS 2.1 specification as it is today**
    - Need to address personalization (card management)
    - Potential to test reference applets on actual cards instead of a simulator
  - **File system “usage” simulator completes GSC-IS 2.1 specification as is**
    - Some personalization already addressed using ISO standards
  - **Simulators provide native GSC-IS 2.1 implementation so no APDU translation is needed**

Q&A