DMDC

*Information and Technology for Better Decision Making*

# Department of Defense Approach to PIV

*Prepared for:*

## PIV Workshop

*Presented by*


## Mike Butler

**Deputy Director**
**Smart Card Programs and Operations**


*October 2004*

# CAC Topology


- **Important**
  - Provide standardization of ID card
  - Meet Geneva Convention Card requirements
  - Prevent counterfeits
    - ID theft – fastest white collar crime

## INS Security Alerts

- Notify change in CAC topology
- Prevent fraudulent use of CAC

# CAC Technology

- Migrating to 64K Card (Approved) – Estimated March 2005
  - Space: accommodate emerging space requirements
  - Scalability: cost effective and provide solution for growing range of technologies
  - Flexibility: changeable access controls, remain vendor neutral
  - Security: CAC certification FIPS 140-2 level 2 or 3
  - Standards: work with NIST, biometrics, and Global Platform
- PKI Applet
  - Identification Certificate
  - E-mail Signing Certificate
  - E-mail Encryption Certificate
- PIN Management Applet
- Demographic Data Applet
  - Uses General Container Applet
  - Data Grouped in 5 Instances

# DoD Approach to CAC

- CAC is the identity token
  - Minimal data on card
  - Card is key to network (PKI)
  - PKI is basis for authentication
- Why this approach?
  - Synchronization of card data to database record is key to protecting data

**Not a data storage device**

# It's Not Technology – It's BUSINESS

- Issuance process
- Identity proofing and vetting
  - Most important part of issuance process
- Policy for who receives credential
  - Outliers
    - Volunteers
    - Non-appropriated fund civilians

**Technology + Policy = BUSINESS**

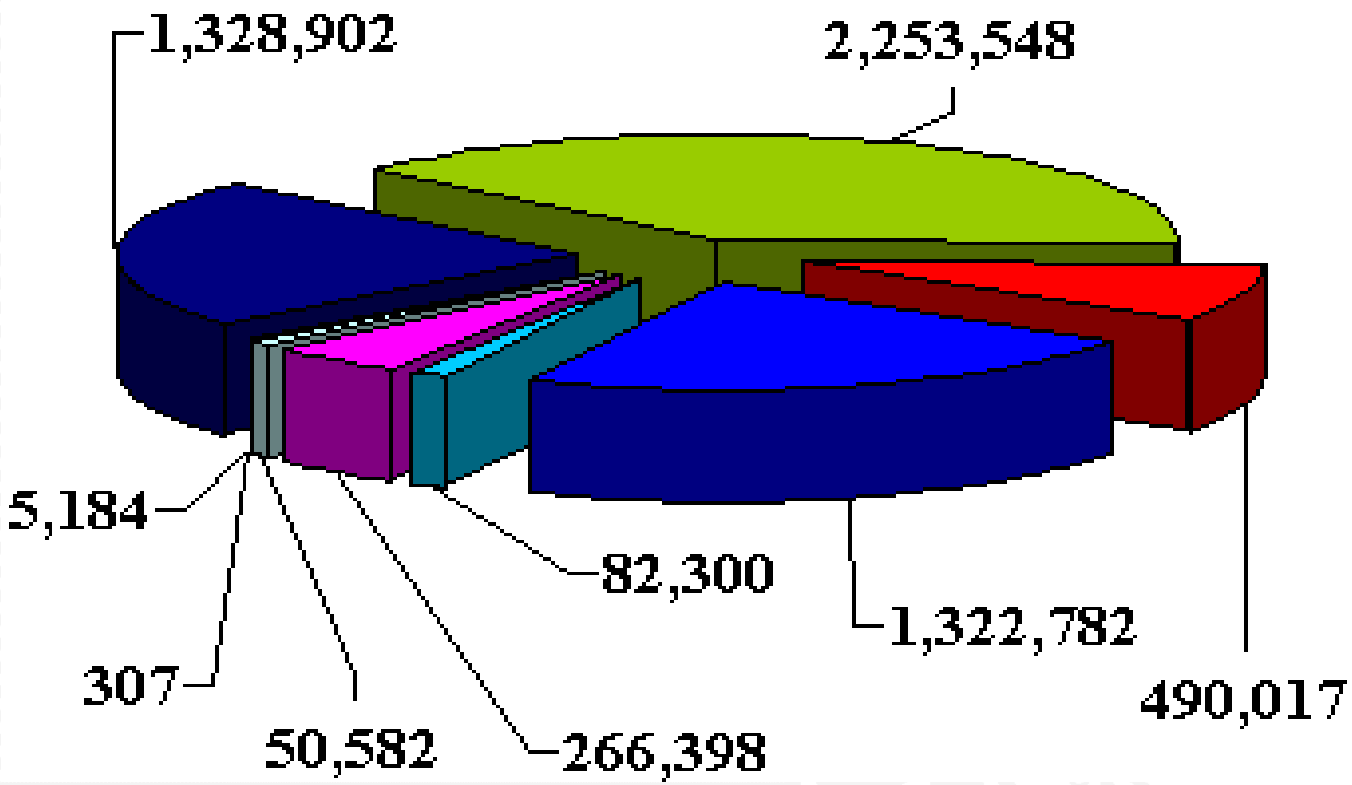
# CAC Status

- Initial operating capability CY 2000
- Issued to 91% of target population
- Web-Based CAC tools
- NEXGEN CAC
- Personnel Identity Protection (PIP) Program Directive: DoDD 1000.25

# CAC Issuance Statistics

## 5,800,020 CACs Issued as of 30 August

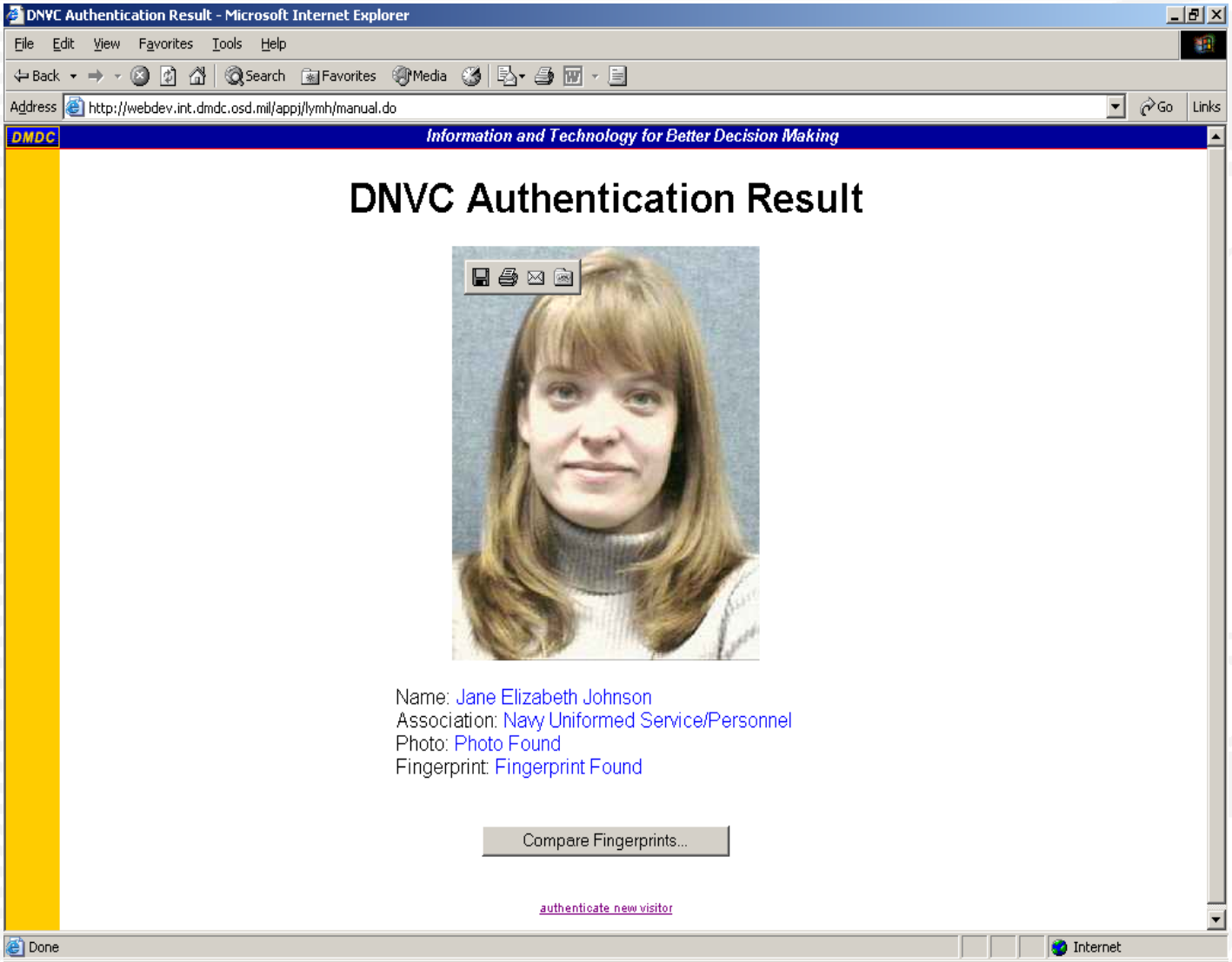
(Unterminated issued 3,135,670 of approx. end strength of 3.45M)



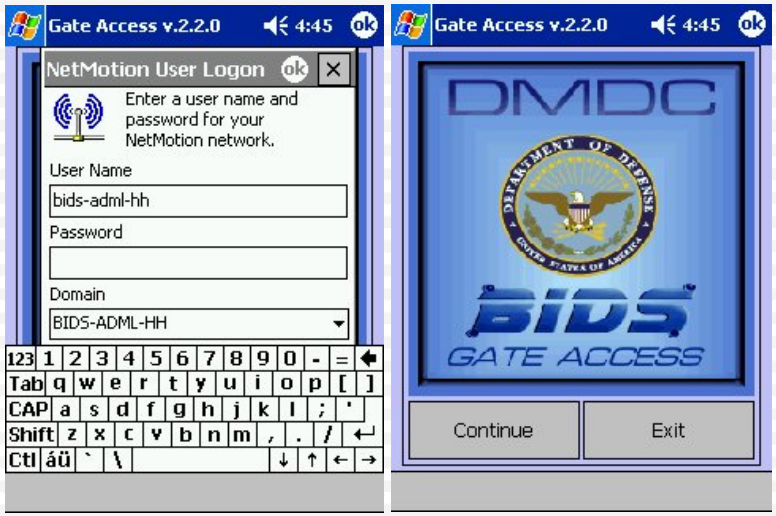
# CAC Tools

- **Web-Based Systems**
  - **Contractor Verification System (CVS)**
  - **Defense National Visitor's System (DNVS)**
  - **Defense Cross-Credentialing Identification System (DCCIS)**
  - **Defense Biometric Identification System (DBIDS)**
  - **User Maintenance Portal (UMP) / Post Issuance Portal (PIP)**
  - **CAC PIN Reset (CPR)**
  - **Central Issuance Facility (CIF)**

# DNVS


DNVC Authentication Result - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://webdev.int.dmdc.osd.mil/appj/lymh/manual.do
Go Links
DMDC
Information and Technology for Better Decision Making
DNVC Authentication Result
Name: Jane Elizabeth Johnson
Association: Navy Uniformed Service/Personnel
Photo: Photo Found
Fingerprint: Fingerprint Found
Compare Fingerprints...
authenticate new visitor
Done
Internet

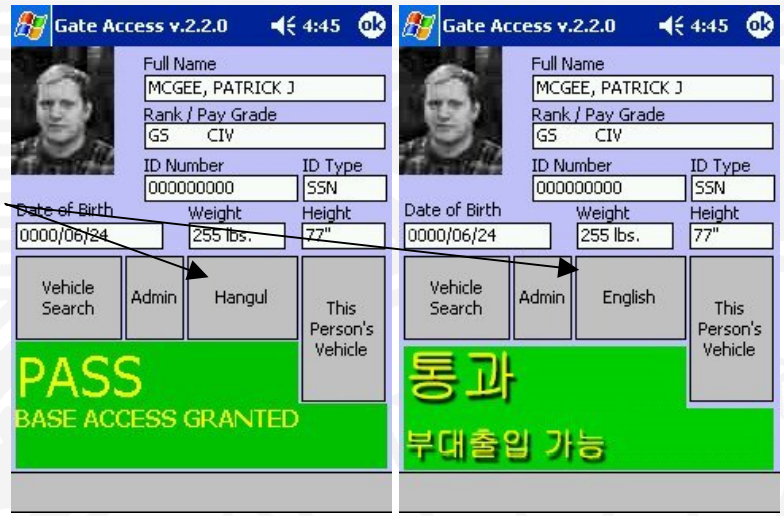
# DBIDS Handheld Sample Screens




**Logon Screens= Click 'OK' and 'Continue'**

**Switch languages @ click of button**

**Default set by Admin/SSM**




**ID Scan = Pass**

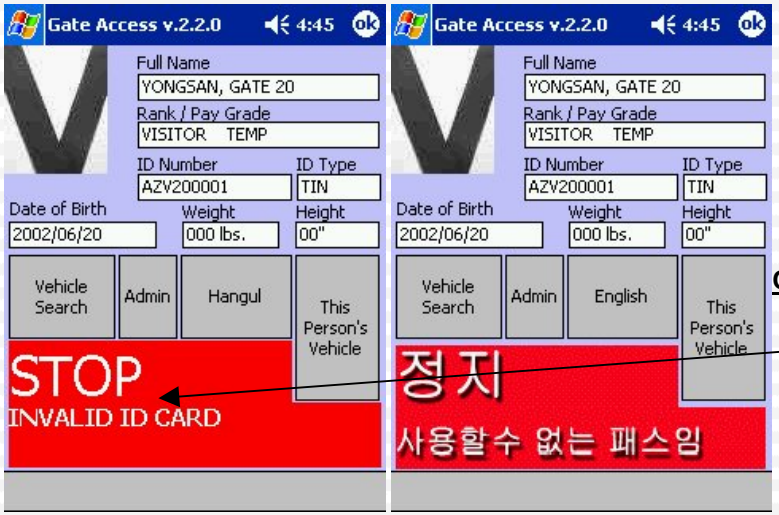
**Safety Sticker Barcode Scanning Ready to go! Just need stickers**


**Safety Sticker Scan = Driving Status**

**May view multiple owned vehicles If applicable**


**This Persons Vehicle = Driving Status**

# DBIDS Handheld Sample Screen #2

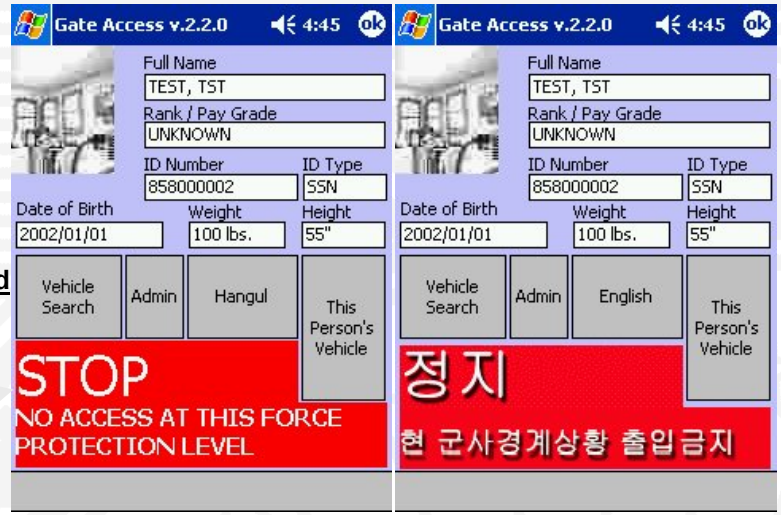



ID Scan = Invalid Card (replaced by newer one)

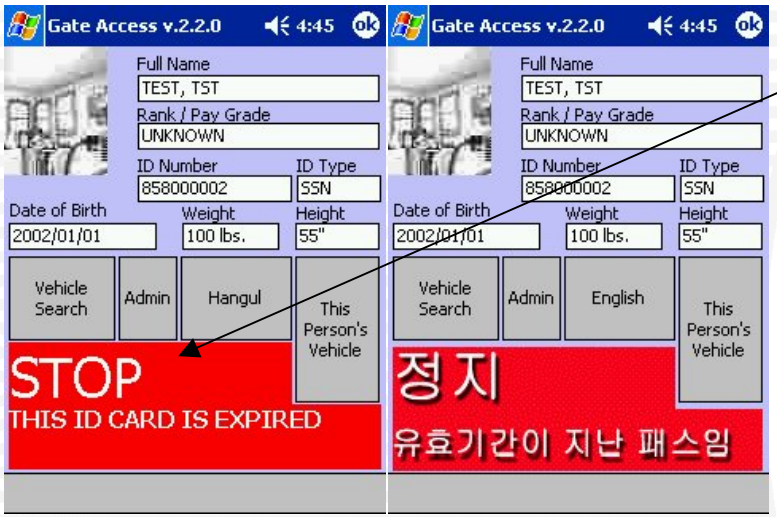
**Checked & Validated**

** Valid ID's

** FPCON Access



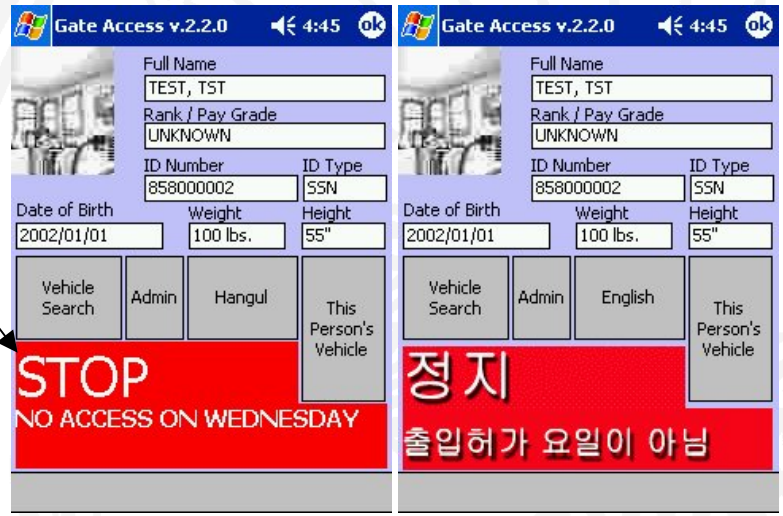

ID Scan = Access Denied FPCON Level




ID Scan = Expired ID Card

** Expirations

** Days/Times Allowed




ID Scan = DBIDS ID was for Sat, Sun Only

# Program Successes and Shortfalls

- **Overall success**
  - **Logical access process**
  - **Standards for technical implementations**
  - **Network capable tools**
- **Shortfalls**
  - **Physical security**
    - **Standard processes**
  - **Technical guidance (HSPD-12)**
  - **DoD supports PACS 2.2**

**Technology + Policy = BUSINESS**

# The FiXs Federation

## A DCCIS Identity protection and management partner

## A Cross Certification and Interoperability Pilot of Credentialing, Identity Management and Protection

**Ron Parsons**
**Co-Chair: FEGC**
**Co-Chair: FiXs Federation**

# New Concept Requirements

- One credential vs. many for any individual
- Multiple characteristics vs. one for access (system/organization)
- Interoperability for cross-credentialing
- Maintenance of data privacy
- Satisfies new policies for Personnel Identity Protection
- Build, test and deploy new system components on a continual basis

# Satisfying the "Missing Piece" for a Cross-credentialing Identification System

- DoD can strongly identify it's core members via the DoD Person Data Repository (ID + Biometric)
- DoD does not have a chain of trust for 'outside' members
  - Example: Contractors, other government agencies or delivery and repair personnel
- Need for a 'federated system' to identify and assign privileges to personnel but maintain privacy
- Need for an inter-operable trust model with Industry and other Agencies

# The FiXs Federation & DCCIS OBJECTIVES

1) **Satisfy current policies, standards and processes with a standard automated access control system (To include compatible trust policies for both physical and network access).**

2) **Produce the Proof of Concept (PoC) and Pilot for a target "Defense Cross-Credentialing Identification System (DCCIS)"**

3) **Create a Federated credentialing system between government and Industry where the information on individuals remains with, and under the control of, their parent organizations.**

4) **Develop interoperable system concepts for accessing and validating contractor(s) and government credentials at U.S facilities and temporary overseas duty stations.**

5) **Produce metrics evaluating the objectives.**

# FiXs Federation & DCCIS MOU Documents

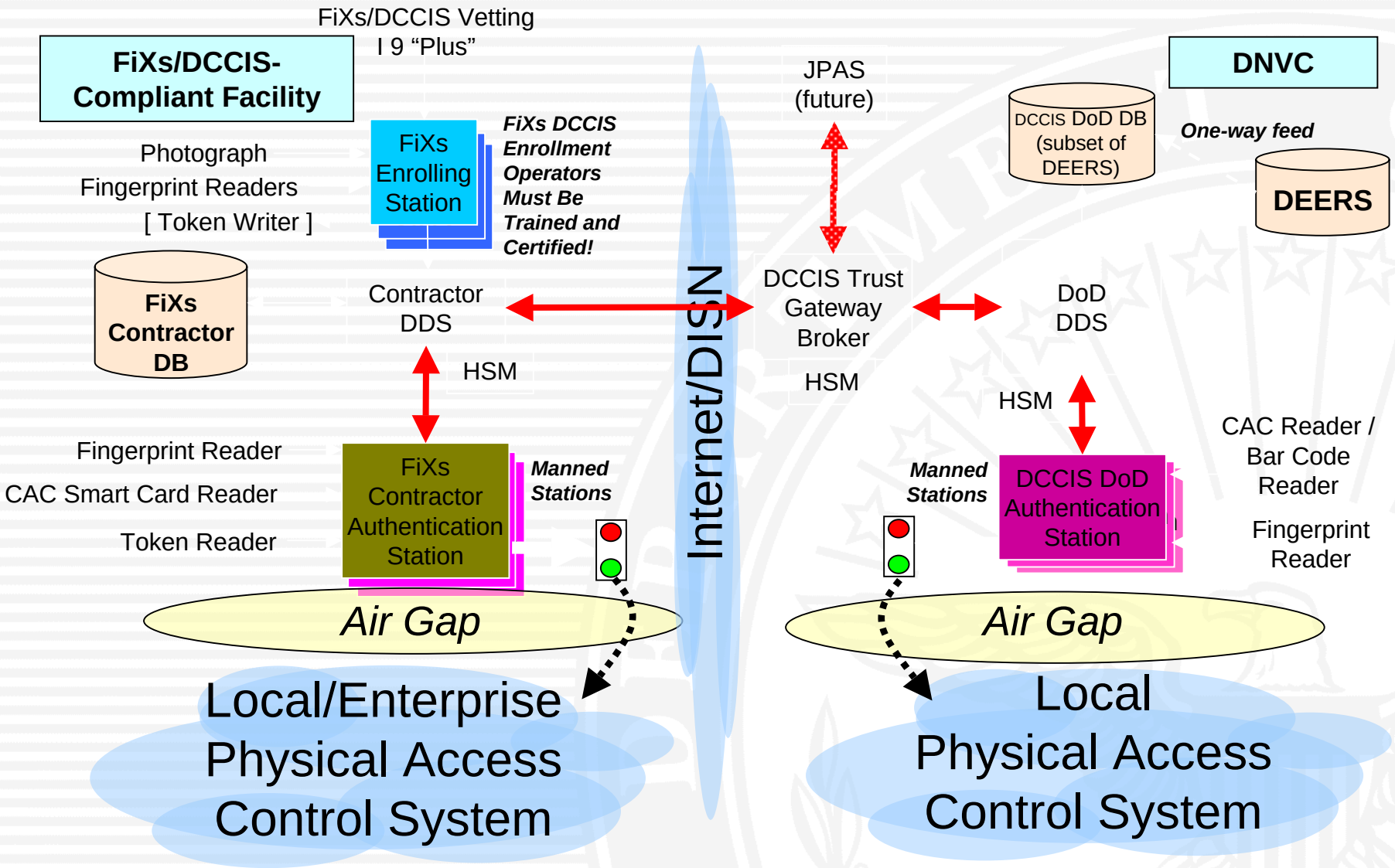
- Trust Statement
- Policy Document
- Operating Rules
- Technical Specifications

Memo of Understanding (signed by senior executives of Government and Industry organizations participating)

# Concept of Operations

- **DoD: Uses existing Common Access Card (CAC) and reconciles trust models with Industry trust models.**
- **Industry: Authorized Company Security Official issues FiXs Federation token (or reference ID based on company issued credentials) for purposes of identity authentication only using DCCIS requirements.**
  - **Strongly-bound biometrics (2 fingerprints)**
  - **Hi-resolution facial photo**
  - **Is responsible for revocation of credential and notification to the "network"**
- **Base Security: Uses FiXs Federation DCCIS token (or reference ID) to authenticate identity and then uses local policies to grant privileges.**
  - **Accepts Company data and revocation; adds/deletes authorized base accesses**
  - **Validates biometrics, local privileges, revocation status**
  - **Allows or denies access**
  - **Local policies and procedures remain enforced**
- **DoD Components: Utilize the National Visitor Center and DBIDS infrastructure to facilitate the FiXs/DCCIS enterprise deployment.**

# FiXs Federation & DCCIS Architecture



# FiXs Federation & DCCIS Design (Continued)

- **Web-Based interfaces between all organizations.**
  - **Each web-site uses strong authentication**
  - **Hardware Security Modules (HSM) ensure secure server-to-server communications**
- **Four types of web-based access, served from FiXs/DCCIS Domain Server (DDS).**
  - **Enrollment website issues basic identity, binds biometrics and photograph; submits record to DCCIS database**
  - **Authentication website collects initial data (name, "home" company, FiXs/DCCIS token – if available), checks with "home" DDS, compares biometrics**
  - **Accepts requests for data from FiXs/DCCIS Trust Broker; Sends biometrics**
  - **Administrative interface allows local site management**
- **Authentication workstation (kiosk): Displays stored photograph, compares biometrics, sends Match/No-Match determination to local site security officer – data remains under control of parent organization.**

# Participating FiXs Federation Organizations (As of Fall 2004)

- Anteon
- BearingPoint
- DSA, Inc
- EDS
- Intelli-Check
- Northrop Grumman Corporation
- SRA International, Inc.
- Lockheed Martin

- NACHA
- FEGC
- Liberty Alliance
- American Logistics Assoc
- WaveSystems
- SAIC
- ActivCard
- BIO-key
- Corestreet
- ChoicePoint
- Identix
- Neustar
- Verisign

# Participating Government Organizations

- ASD(NII) -- Directorate of Information Assurance
- USD(I) -- Physical Security and Force Protection
- DMDC
- Access Card Office
- PKI PMO
- DIAP
- BMO
- Army PEO-EIS
- NSA
- GSA -- AIWG
- OMB -- e-Authentication Portfolio Manager
- Department of Interior
- United States Postal Service

# Initial Fielding Sites

- DMDC -- East Coast and West Coast
- Wright Patterson AFB (Office Complex)
- Kirkland AFB (Office Complex)
- Northrop Grumman Corporation -- McLean, VA & Reston, VA
- SRA International, Inc. -- Fair Lakes, VA
- Bearing Point -- Alexandria, VA
- EDS -- Alexandria, VA
- Anteon – TBD (Navy site?)
- Lockheed Martin
- Ft. Monmouth (Myer Center)
- US Dept of Interior (?)
- Other Federal Agencies (?)

# DoD Reference Guides

- DoD has:
  - Policy
    - Dr. Hamre Memo, November 10, 1999
    - Smart Card Technology Directive 8190.3
    - DoD Personnel Identity Protection Directive 1000.25
  - Technical Specifications
    - Middleware Specification
    - Pre-Issuance Specification
  - Guidance and Legal Decisions
    - April 2002 CAC Policy Memorandum
    - Foreign Nationals

# Summary

- For each technology on the card exists a single point of failure,
  - The fewer the technologies = the less points of failure
  - Minimize the technologies to address current and anticipated future requirements
- Technology will evolve and change will happen - remain flexible and open-minded
- As a successful program meeting business needs, we continue to support initiatives to use credentialing as DoD business processes

# Questions?

**Mike Butler**

**cacsupport@osd.pentagon.mil**

**(703)696-7396**