DoD Common Access Card
Convergence of Technology
Access/E-Commerce/Biometrics

IDENTITY

Mary Dixon

February 12, 2003

A Short Review and Update

DoD is issuing 4 million smart cards to:

- Active Duty Military
- Selected Reserve/National Guard
- DoD civilian employees
- DoD contractors inside the firewall

To provide the ENABLERS to support:

- E-Commerce (non-repudiation via PKI)
- Improve and Re-engineer Business Processes
- Improve and Re-engineer Physical Security
- Reengineer Logical and Network Access

Common Access Card (CAC)

Initial (1999) Requirement Converged Three Separate Initiatives

Smart Card
- Pilot Studies
- Business Process Re-engineering
- No $

E-Business
- Non-repudiation for digital signatures

PKI
- Hardware token
- Secure network log-on

Common Access Card (CAC)

Common Access Card (CAC)

Status of Convergence Today

- 1.75 Million Cards Issued
- 9-12 thousand cards being issued per day
- Piloting Contactless Technologies (14443A)

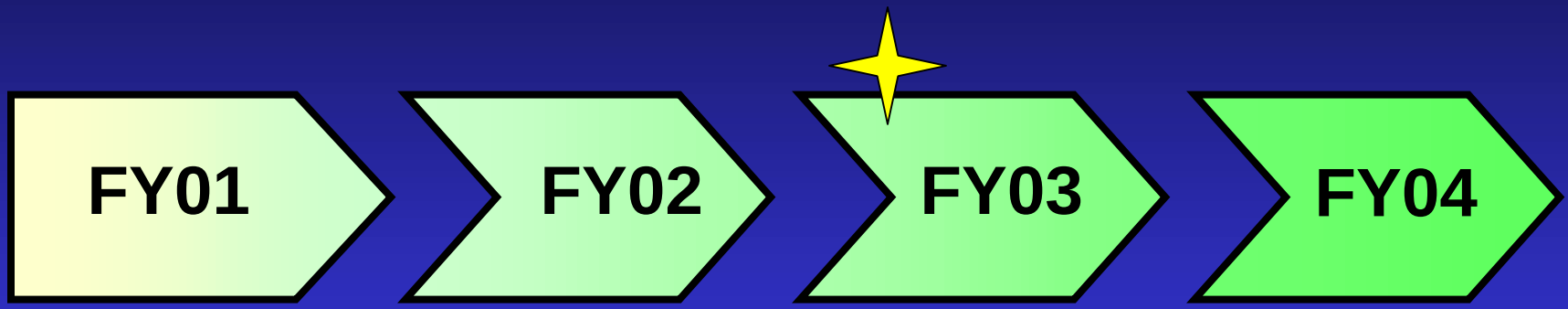
- 150,000+ workstations with logical access/log-on
- 1300 issuance workstations
Issuing in 15+ countries worldwide

Applications:
Food Service
Manifesting
PKI Signing
PKI Encrypt

BETA Testing:
Remote Update
&
Card Maintenance
via Web

Smart Card Standards
GSA
NIST
ISO/ANSI
FEDERAL

CAC Implementation Timeline



- Planning /Development
- Upgrade existing issuing Infrastructure
- Issue cards
- Field readers / middleware
- Add biometrics to card
- Contactless Pilots and Decisions

New Developments

The Real Issue

Shifting Paradigms

Identity NOT Technology

Case for a New Paradigm

The world has changed -

- **Identity theft is an emerging problem - identified as fastest growing white collar crime**
- **Credentialing has not recognized new realities - fakes are everywhere with both "wholesale" and "retail" options**
- **Political as well as financial motivations - no longer benign rite of passage**
- **What's at stake is huge - identity is key to financial systems and logical and physical access to corporate/government assets**

Case for a New Paradigm

How much progress have we made?
Credentials in DoD have not kept pace

More similarities than differences
New card computer generated -
only an advantage if that power is used
to authenticate the individual

Issuance: Strong Identity Proofing

Paper credentials w/1-2 picture
NOT SUFFICIENT

Check presence in PDR

Verify biometric

Person Data Repository
PDR

12 personnel databases

What do I know:

- All civilians go through National Agency Check (NAC) before hiring
- All military go through NAC/background checks before being sworn in
- All contractors on our networks go through NAC before given access

Usage

Token binds the *confirmed* identity to the digital credentials

Authenticate and sign

Biometrics on the Token can raise the bar

Optional methods

Store on:	Matched on:
A. Server	Server
B. Workstation	Workstation
C. CAC	Server
D. CAC	CAC

Evaluating multiple options and uses

- Biometric in lieu of PIN (probably not)
- Biometric with contactless chip
- Potential CAC applications using biometric

Case for a New Paradigm

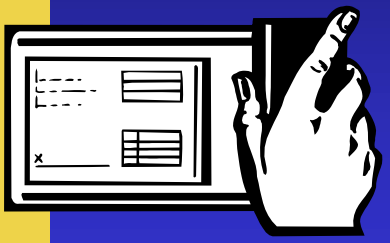
Biometrics have an important role ...

Early recognition of the importance of biometrics

- but how easy is it to use as identity authentication?
- many biometric solutions today are not much more accessible

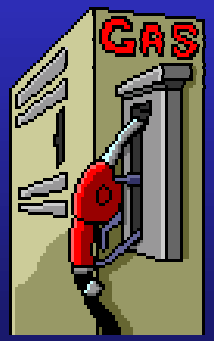
Case for a New Paradigm

Credit card industry has long recognized the issue:



1960's - The card looks good - use the embosser

1970's - I need to get authorization for this purchase - central system verification

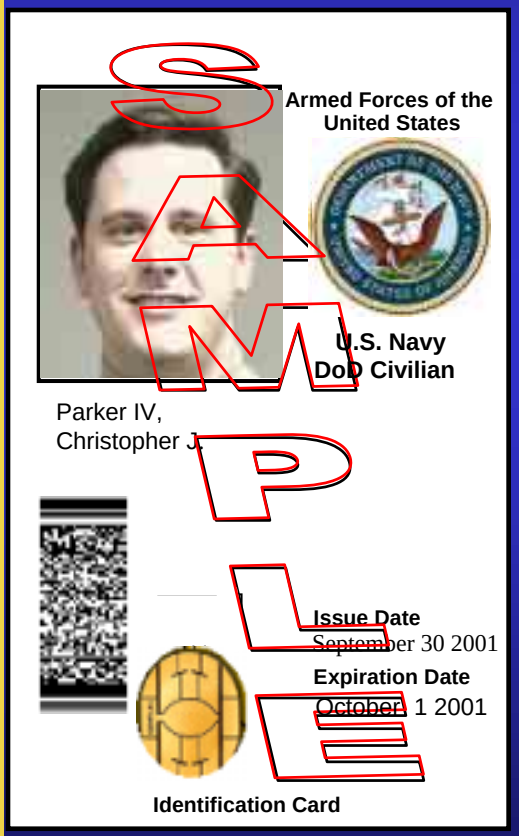


Present - all transactions authenticated - network based always on connection to central system

Physical Access is at the 1960's stage - *it looks like a good card*

Case for a New Paradigm

Summary



- Fakes are a big problem
- DoD has high risk assets
- Existing technology not used
- Physical Security solutions have not kept pace with technology
- Biometrics are collected enterprise wide but not used for physical access

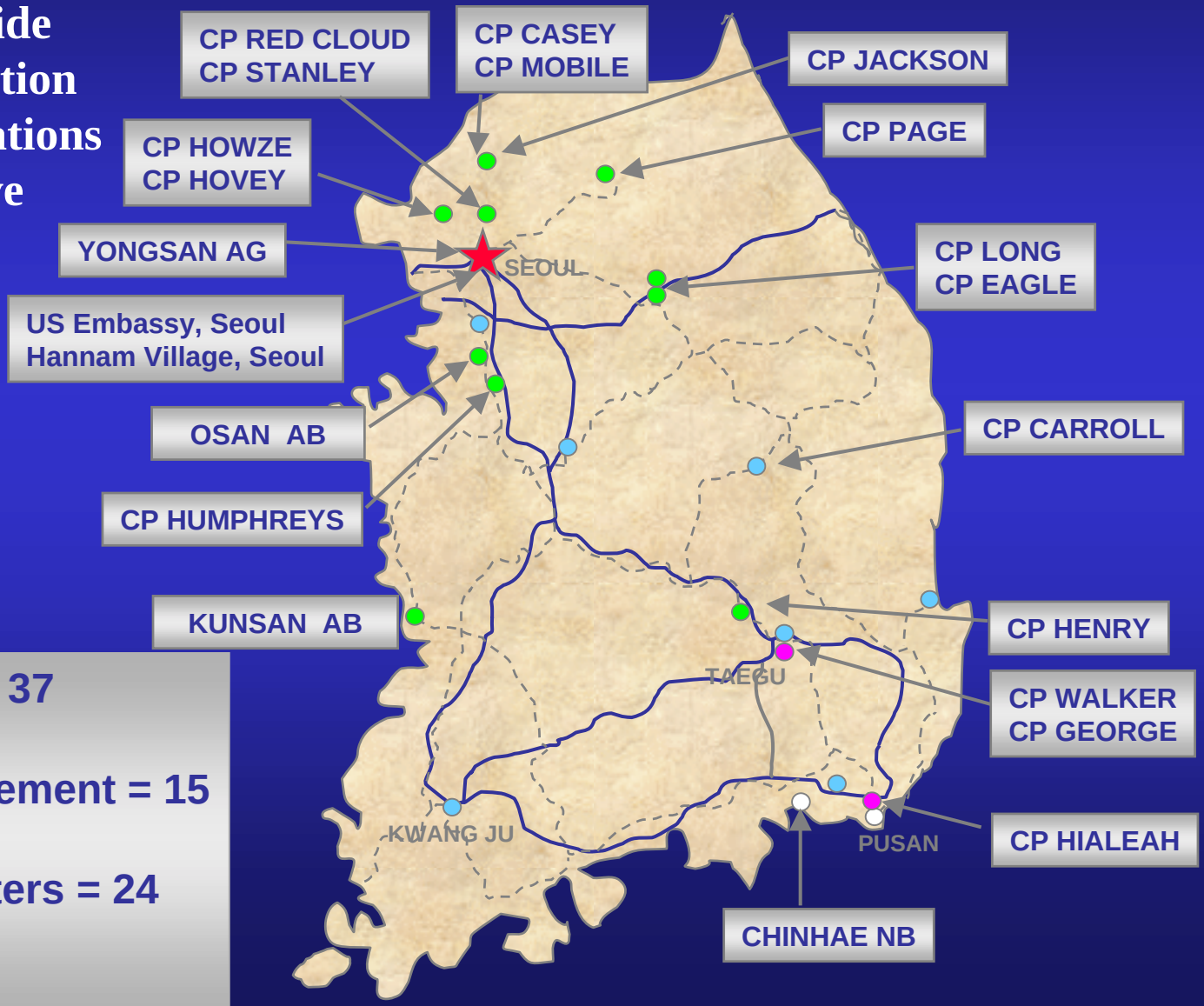
These are the issues BIDS addresses

Biometric Identification System (BIDS) Application of the Paradigm

- **Identity management and force protection system:**
  - **Uses Existing DoD Issued Identification Credentials**
  - **Issues badges for other individuals (visitors/vendors)**
  - **Covers a building, an installation, or an entire theater of operations**
  - **Contains person information, digital photo, digital fingerprint, motor vehicle info, and privately owned weapons info**
  - **Configurable by force protection level and local business rules**

BIDS, Fully Deployed and Operational in Korea

Theater-wide Implementation
150K registrations
90K active



Pass & ID = 37

Law Enforcement = 15

Visitor Centers = 24

Gates = 48

BIDS, Other Locations

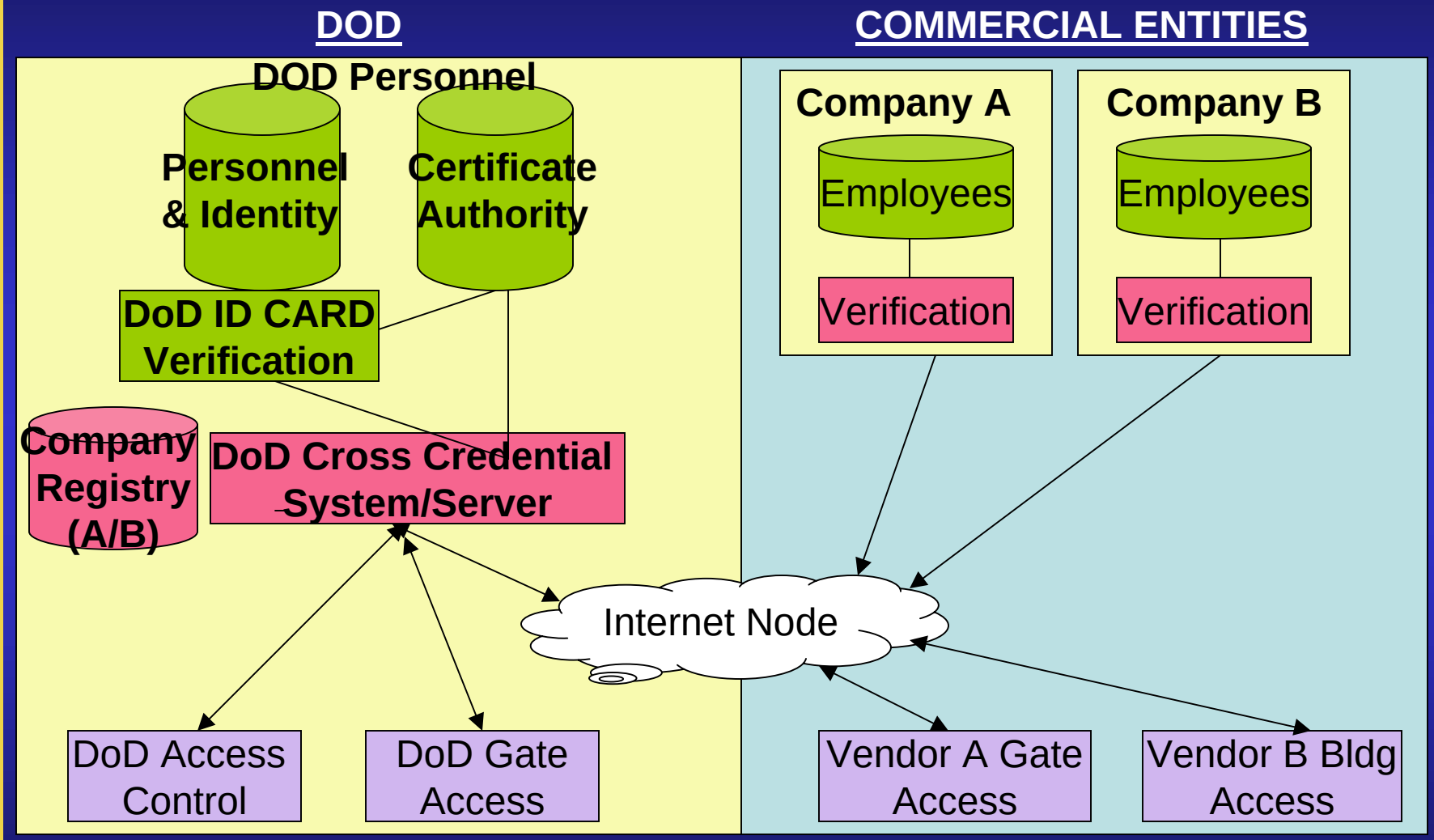
- US Army Europe
- Defense Language Institute (Monterey, CA)
- US Forces Japan
- Biometrics Fusion Center (Bridgeport, WV)

DCIS Pilot

Defense Cross-credential Identification System

- **DoD can strongly identify it's core members via the DoD Personnel Data Repository (ID+Biometric)**
- **DoD does not have a chain of trust for 'outside' members**
  - **EX: Contractors or Delivery and Repair Personnel**
- **Need for a 'federated system' to identify and assign privilege to personnel but maintain privacy**
- **Raise the bar on security while making access easier for companies and employees**

DCIS CONCEPT



If Internet Access is available, any access point can receive a digitally signed (by the US Govt), certificate containing identity, status, photo, privilege, etc

Common Access Card (CAC)

Future Convergence-Beyond DoD?

- Other Federal Agencies considering Smart Card issuance

- Federal Contactless (14443A) Standard Proposal Via NIST

- Emphasis on IDENTITY SECURE TOKENS BIOMETRICS MACHINE READABLE

- Federal Agencies Working Common Standards

- CHANGING PARADIGMS What is ENTERPRISE? Department or the Federal Government?

- Smart Card Standards GSA NIST ISO/ANSI FEDERAL

- "WE ARE A FEDERAL COMMUNITY" What common processes can we share?

What are the Weak Links?

- **Standards**
  - **Smart Cards**
  - **Physical Access**
- **Interoperability**
  - **Standards**
  - **Policies for reciprocity of credentials**

Emphasis on Identity = Bridge

Standards

DoD Strategy

- Embrace standards where they exist and stretch requirements so that standards work for the application
- Adopt industry best practices as defacto standards – ex: Global Platform & Javacard
- Publish specifications and distribute freely – ex: the card edge specifications for our applets
- Develop interfaces that are provided to anyone interested in developing or adapting applications to work with our card system – ex: Basic Services Interface (BSI)

Interoperability

- Most interoperable solution in industry
- Requires commercial involvement
- Good partner relationships a necessity
- ***CAC Goal***: any operating system, any card, any reader

Physical Access

- Dept. of Interior (DOI) is taking the lead
- Agencies learning from/working with each other with interoperability as the focus across the entire government enterprise
- Reviewing contactless technologies

Summary: Where Are We Going?

DoD

- Complete rollout of cards and infrastructure
- Continue to improve w/technology
- Shift focus to usage
  - Physical access
  - Logical access
  - e-business initiatives

Federal Govt

- Common policy on identity proofing
- Interoperability
- Physical access

Questions?

Mary Dixon
(703) 696-7396
dixonmm@osd.pentagon.mil