

DIGITAL ID WORLD

Strong Authentication

&

User Experience

Date: September 12, 2006

Bill Boggess
CIO of the Defense Manpower Data Center

STRONG AUTHENTICATION

Identity Challenge

- World has changed – cyber transactions and identity theft
- Fake credentials are prevalent and increasingly easy to make
- DoD has high risk assets that require protection – threat has increased
- Existing physical security solutions lag behind technology – flash pass
- Digital authentication rare
- Biometrics (fingerprints) collected enterprise-wide but not extensively used for physical access



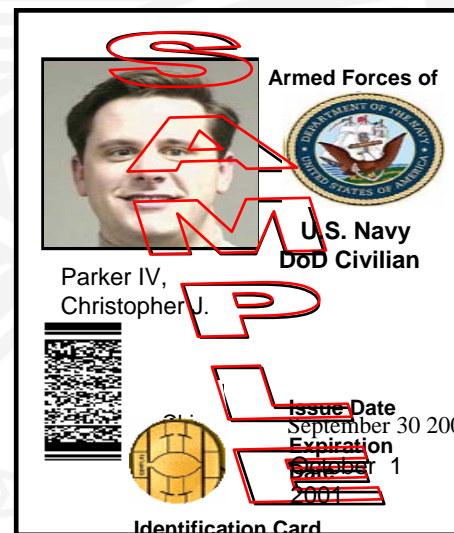
Major Issues that Need a DoD Enterprise Solution

Identity Challenge

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



Not much if you don't use the power of the new card – digital authentication and biometrics



What has been done?

Identity is all about the Chain of Trust.

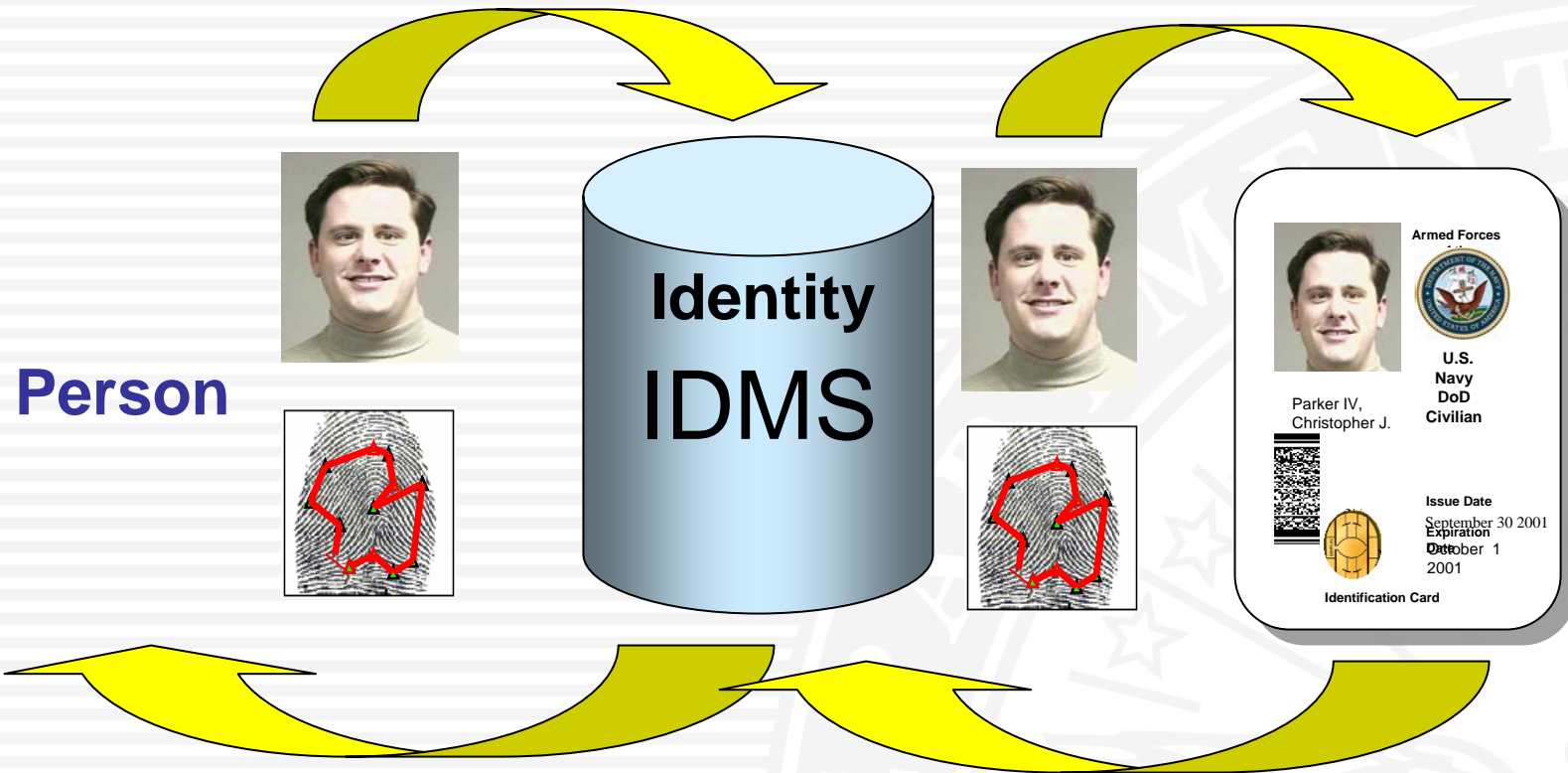
What is Contextual Identity Information?

- I am Bill.
- I am married to Connie.
- I have two children.
- I graduated from the University of California.
- I work of DMDC.
- I drive a Saturn.
- I like beer.

DoD Enterprise Identity Process

- **Identity Vetting** – Process of insuring that people are who they claim to be
- **Identity Management** – Process of tying vetted identity to a management system and a DoD affiliation using biometrics and card issuance and then tracking the identity. PKI keys and certificates are issued.
- **Authentication** – Insuring digitally and with great fidelity that a credential is authentic and the person presenting the credential is the person to whom it was issued.
- **Authorization** – Assigning access privileges based on an identity and affiliation and conditioned on threat.
- **Access** – Physical Access and Logical: the hardware and process of allowing access based on the above four processes

Biometric Identity Binding



- Biometrics can be use effectively to bind a person to an identity store in an IDMS.
- Biometrics can be use effectively to bind a card to an identity store in an IDMS.

What has been done?

We are talking about Electronic Identity.

It is made up of some of the following:

- A Photograph
- Biometrics
- Demographic Data
 - Name
 - Numbers: EDI/PI, CHUID, SSN
- Public key Infrastructure

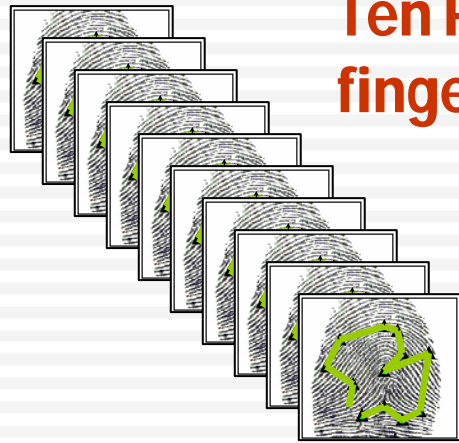
And is stored in a database or on an Id card.

Critical Issues or Challenges

- Recognizing Individual Uniqueness
 - Use of Numbers to doomed to population size
 - Use of Biometrics comes with
 - False Matches
 - False No-Matches
 - Matching – References- Names are not unique
- Vetting vs. Suitability

What has been done?

What is Biometrics Identity Information?



**Ten Prints
fingerprints**



**Iris
images**



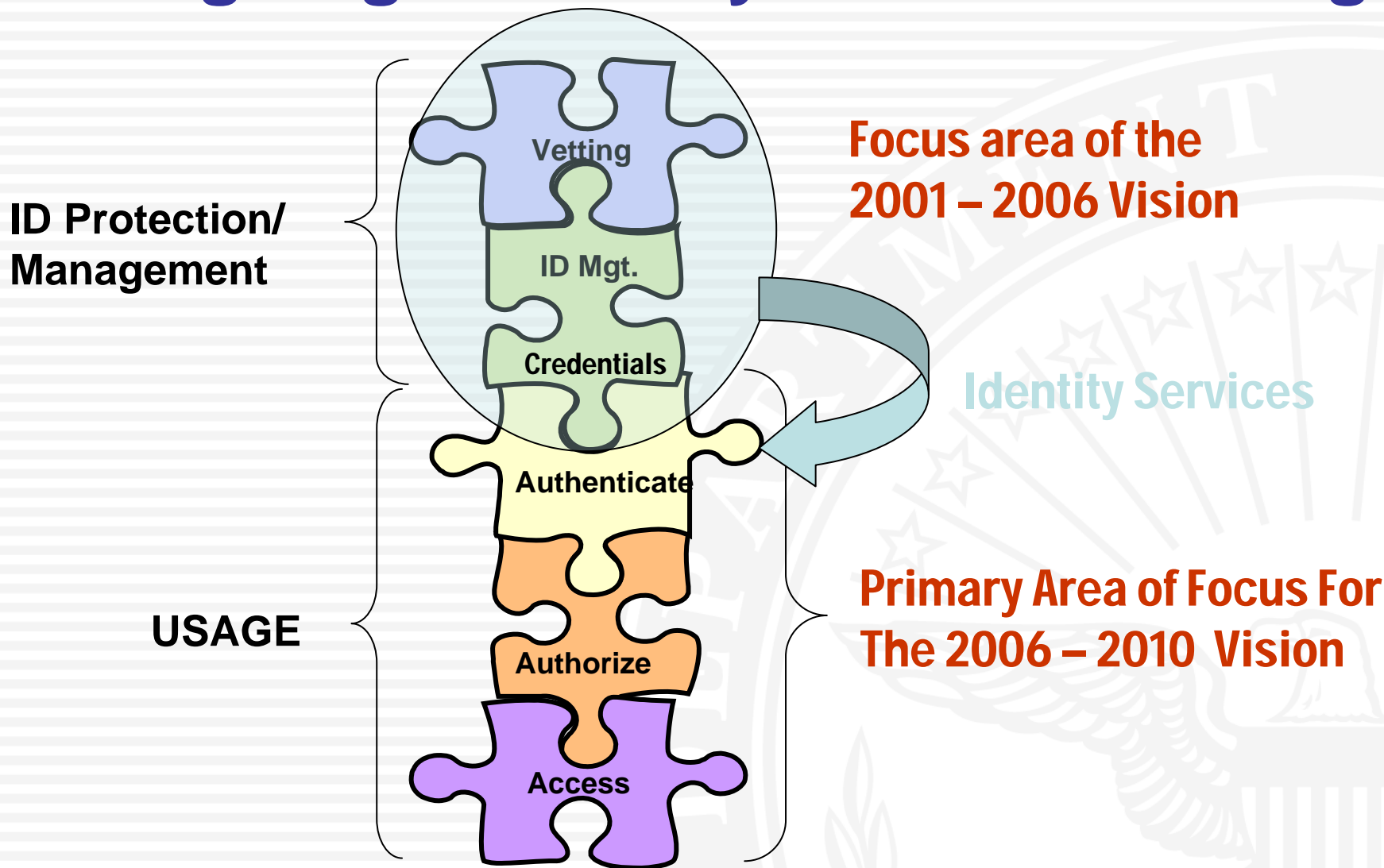
Photographs



What is PKI Identity Information?

- Public and Private Keys
- PKI Certificates

Doing Logical & Physical Access Right



Cheap Technologies?

Front **Back**

Front Side:
Armed Forces of the United States
DEPARTMENT OF THE ARMY
Army
Active Duty
Parker IV, Christopher J.
Grade: E5
Rank: SP5
Issue Date: 2000SEP19
Expiration Date: 2003SEP18
Geneva Conventions Identification Card

Back Side:
Medical Blood Type: O+
Organ Donor: Yes
Date of Birth: 1969JAN09
Social Security Number: 742-76-0064
Service Category: IV
DCIO/OUSD(P&R) OCT 2000 Property of the U.S. Government

- Bar codes are write once
- Bar codes and Magnetic stripe are read always.

USER EXPERIENCE



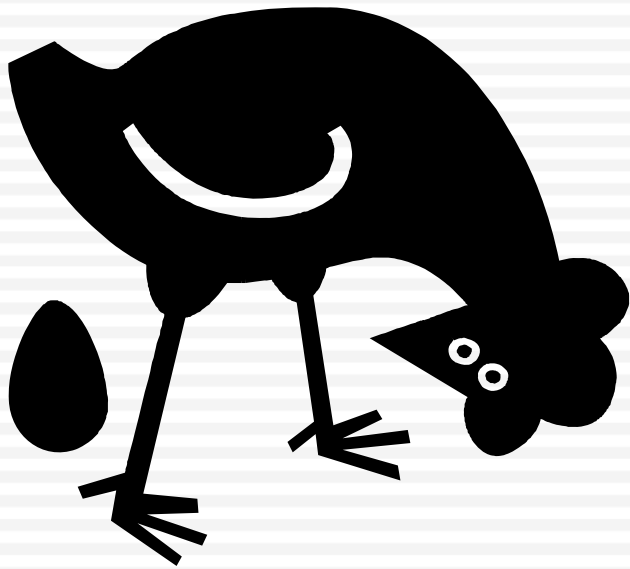
Early Days

- I can open my door with my card
- Can I be electrocuted by my card?
- Will lightning strike me if carry a card?

Later

- Will the enemy get all of my information from the card?
- Will lightning strike me if carry a card?
- What do I do if I forget my card?

Create the Card or Install Applications



Chicken or the Egg

Lessons Learned

Common Access Card/Public Key Infrastructure 2001-2004

The Army

- Fielded 818,584 card readers
- Fielded 900,000 middleware licenses
- Fielded 2,000 Public Key Enabling Development kits
- Trained 6,016 personnel to install readers & middleware, set up user certificates, and establish CAC logon procedures
- Provided on site fielding and training to 103 separate locations
- Answered 2500 Help Desk calls

Lessons Learned

	2001	2002	2003	2004	2005
CAC not Accepted	✓				
Users forgot their PIN	✓	✓	✓	✓	✓
Left their card in the Reader	✓	✓	✓	✓	✓
Issuance time	Too Slow	Too Slow	Too Slow	Shorter	Good
Issuance infrastructure	Up & down	Up & down	Up & down	Reliable	Very Reliable
New features added	N/A	N/A	Late	delivered	delivered

Lessons Learned

CAC PIN Reset (CPR) - Allows a trusted operator reset the CAC for the CAC holder to change the pin.

DIGITAL ID WORLD

QUESTIONS?

Date: September 12, 2006

Bill Boggess
CIO of the Defense Manpower Data Center