Smart Cards & Credentialing in the Federal Government

Smart Card Alliance
13 Feb 2003
Salt Lake City

Bill Holcombe
GSA – Office of Governmentwide Policy

New Urgency for Credentialing Solutions

- Post 9/11 need for better security
- Better identification of
  - Govt employees, contractors, and agents
  - Citizens, business, others doing business with Govt
  - Visitors & travelers to U.S.
- For what purpose . . .
  - Physical access
  - Cyber / systems access
  - Security threat analysis

Some Government “Drivers”

- Fear of al Qaeda & terrorist attacks
- War looming with Iraq
- DHS National Strategy for Homeland Security
- Aviation Transportation Safety Act
- Enhanced Border Security & Visa Entry Reform Act
- The Patriot Act
- Government Paperwork Elimination Act
- Government Information Security Reform Act
- Privacy Act and Electronic Signatures Act
- OMB A-130: Mgt of Federal Information Resources

Technologies of High Interest for Identification and Credentialing

- Smart Cards
- Biometrics
  - Fingerprint -- Facial -- Iris
- PKI
- Central and distributed data bases
- Other

Major Players in Credentialing and Identification

- Department of Homeland Security
- Office of Management and Budget
- General Services Administration
- DOD, State, Treasury, Justice, FEMA, DOT
- Participants in air & sea travel business
- Agencies/bureaus dealing with border crossings
- States - DMVs - driver's license (AAMVA)

Governmentwide Initiatives & Groups

- Established smart card buying contract for agencies
- Coordinated development of North American smart card interoperability standard – going global
- Set up groups for coordination of Federal smart card education and projects
  - Executive Interagency Advisory Board
    - Coordinates across Federal agencies
  - Smart Card Project Managers Group
    - Info-sharing, joint forum with industry
  - Identification Policy Group
    - Helps formulate policy
  - Contactless Interoperability Group
    - Led by Dept of Interior

What's Happening Around the Government in Smart Cards, PKI, and E-Gov?

www.smart.gov

Click on "What's New"

Also visit

www.estrategy.gov

Federal Agencies Already Deploying Smart Cards

- DOD - CAC (common access card), a PKI-enabled smart card
- More than a dozen DOD legacy systems in Hawaii and around the world
- State Dept –Diplomatic Security in WashDC
- DOT- Federal Transit
- VA – Veterans Express card
- GSA – HQs
- GSA – Fairfax Willow Wood facility
- SSA at Woodlawn
- Commerce – Bureau of Census
- Interior – Fish & Wildlife Serv
- Bureau of Land Mgt
- FDIC
- IRS
- Justice Dept
  - Immigration (currently laser cards)
  - Justice Mgt Div, Civil Division, OIG

More Just Coming . . .

- DHS wide implementation
- FAA
- TSA
- State
- GSA Regions
- NSF
- Treasury
  - PTO
  - USSS
  - BPD
  - Other Treasury bureaus
- BLM
- FBI
- DOL-BLS.

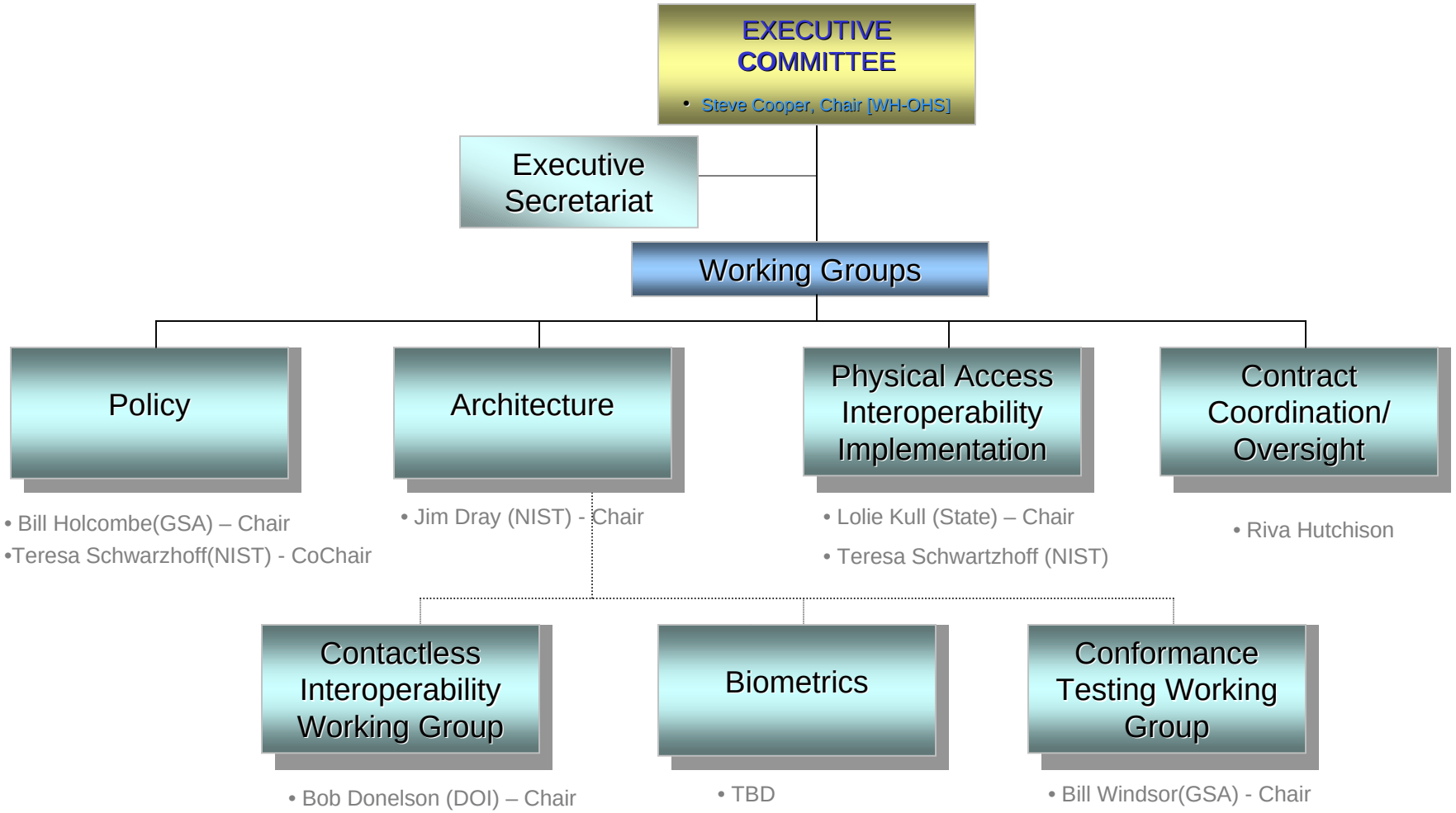
Smart Card Project Managers Group

- Meets bi-monthly with prominent speakers
- Open to all interested
- Shares info, policy, best practices
- Next meeting is Mar 13 in Washington DC

EIAB
Smart Card Executive Interagency Advisory Board

- Established to provide coordination of Federal smart card efforts
- Recently refocused to look at identification and credentialing more broadly
- New Policy Group established to recommend smart card and credentialing policy to OMB and DHS

SC-IAB MANAGEMENT STRUCTURE



Policy Direction

- Use of interoperable credentialing token as platform of choice across organizations
- Raise floor for credentialing platform to be secure and used for both physical and logical access
- Encourage all agencies to think “enterprise-wide” for identification and credentialing
- Use same or similar trust levels for physical and cyber access
- Provide govt framework which is “vendor and technology agnostic”
- Deal with privacy concerns

Policy Direction

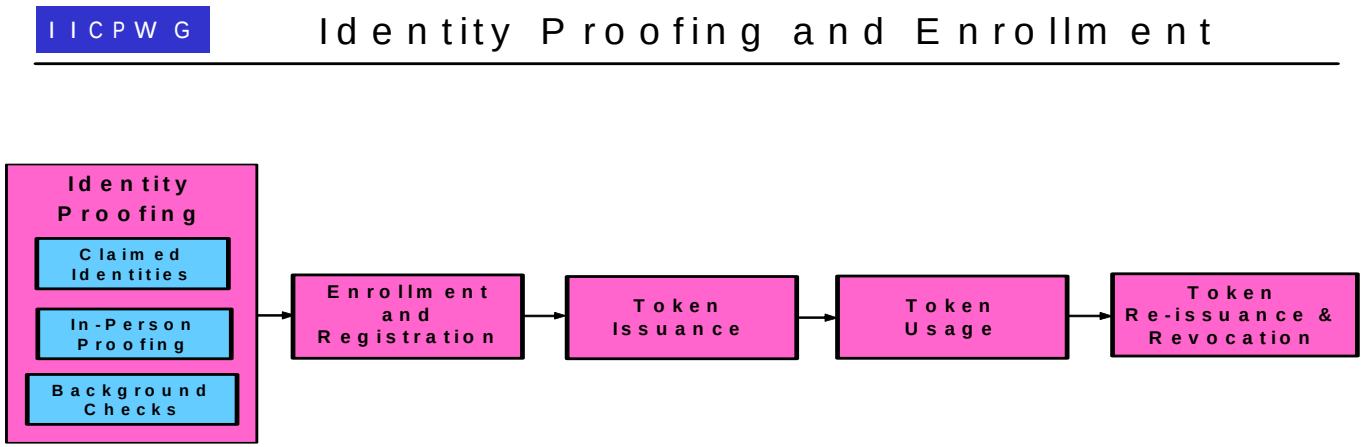
- Merging of physical and cyber domains
- Increasing impetus for smart cards as token for certificates
- Need for 3 certificates and multiple biometrics pushing to high memory cards
- DHS to model all employee smart card for civilian agencies

Strategy

- Interoperability of systems needed
  - To come up with ID's that are effective
  - So Govt agencies can recognize each other's credentials
  - To save Govt $$ and avoid reinventing the wheel
  - Establish a platform on which physical and e-authentication can be added

Weaknesses of Current System

- **Agencies and components keep building proprietary systems**
- **I.D.s easily falsified, counterfeited with old technology**
- **Proofing process is often Achilles' heel of ID systems**



Obstacles and Issues

- The sheer complexity of the problem & varying definitions of the problem to be solved
- Privacy Concerns
  - Data carried on card
  - Info in data bases on individuals
  - Use of biometrics
- Diversity of ID needs, to identify
  - Foreigners crossing borders
  - All travelers, and those accessing airports & sea ports
  - Gov employees
  - Those transacting business with Govt

Obstacles and Issues -continued-

- Immaturity of supporting technologies
- Competing proprietary approaches
- Needed cooperation among Federal, foreign, state & local govt, airports, etc.

Outcomes

- Urgency related to security
- Interoperability & integration of e-authentication technologies
- Governmentwide single ID platform?
- Funding?

For More Information

Bill Holcombe
GSA – Office of Governmentwide Policy

www.smart.gov Click on “What’s New”

Also visit www.estrategy.gov

Bill.holcombe@gsa.gov
202 208-7657