Federal e-Government Agenda: Authentication and Identity Management

David Temoshok
Director, e-Government Strategic Development
GSA Office of Governmentwide Policy
June 5, 2002
President’s Management Agenda

• 1st Priority: Make Government citizen-centered.
• 5 Key Government-wide Initiatives:
  1. Strategic Management of Human Capital
  2. Competitive Sourcing
  3. Improved Financial performance
  4. Expanded Electronic Government
  5. Budget and Performance Integration
## President’s Mgmt. Council E-Gov Agenda

### Government to Citizen

1. USA Service  
   - Managing Partner: GSA
2. EZ Tax Filing  
   - Managing Partner: Treasury
3. Online Access for Loans  
   - Managing Partner: DoEd
4. Recreation One Stop  
   - Managing Partner: DOI
5. Eligibility Assistance Online

### Government to Business

1. Federal Asset Sales  
   - Managing Partner: GSA
2. Online Rulemaking Management
3. Simplified and Unified Tax and Wage Reporting  
   - Managing Partner: Treasury
4. Consolidated Health Informatics (business case)  
   - Managing Partner: HHS
5. Business Compliance 1 Stop  
   - Managing Partner: SBA
6. Int’l Trade Process Streamlining  
   - Managing Partner: DOC

### Cross-cutting Infrastructure: e-Authentication GSA, Enterprise Architecture OMB

### Government to Govt.

1. e-Vital (business case)  
   - Managing Partner: SSA
2. e-Grants  
   - Managing Partner: HHS
3. Disaster Assistance and Crisis Response  
   - Managing Partner: FEMA
4. Geospatial Information One Stop
5. Wireless Networks

### Internal Effectiveness and Efficiency

1. e-Training  
   - Managing Partner: OPM
2. Recruitment One Stop  
   - Managing Partner: OPM
3. Enterprise HR Integration  
   - Managing Partner: OPM
4. e-Travel  
   - Managing Partner: GSA
5. e-Clearance  
   - Managing Partner: OPM
6. e-Payroll  
   - Managing Partner: OPM
7. Integrated Acquisition  
   - Managing Partner: GSA
8. e-Records Management  
   - Managing Partner: NARA
E-Authentication Activities
3 Big Buckets

- Determine e-Authentication (Application) Requirements for all e-Gov Initiatives
- Provide multiple Government-Wide solution sets to meet Requirements (Gateway)
- Provide Government-wide Acquisition and Deployment for The Secure Government ID
The Authentication Gateway

Direct Access Capability Preserved

Citizen

Business

Identity Verification Required

Credential Validation Process

eAuthentication Gateway

Federal Agency Relying Parties

Credential Providers

State or Federal Government

Health Care

Acadia
U.S. Identity Credentials - How do we know who you are?

**Personal Information**
- Address - Home, Business
- Telephone - Home, Business
- Mobile
- Genealogy - Parents, Relatives
- References - Friends, Associates
- Employment - past/present

**Out of Wallet Information**
- User ID, Passwords
- Recent Transactions

**Public ID**
- Commercial Digital Certificate
- Loyalty Cards
- Civic, Community - Library

**Government ID/Credentials**
- Birth Certificate
- Social Security Number
- Passport
- Drivers License/ID
- Taxpayer/employer ID
- Immigration Identification
- Military Service Number

**Material Relationships**
- Financial Services
  - Bank accounts
  - Credit card accounts
  - Loan accounts
  - Insurance
- Tax Authorities
  - Federal, State, local
- Asset Ownership
  - Vehicles
  - Real estate
  - Other
  - Utilities
  - Education, Civic groups
Identity Management Communities - Who do you Trust?

Governments
DMV, AAMVA
Illinois PKI
Washington State PKI
EBT
Government of Canada and U.K.

Higher Education
CREN PKI
Higher Education PKI Bridge

Healthcare
California Medical Association
Med e-Pass
WGA Health Passport

Financial Services Industry
Identrust/DST
VISA/Mastercard

Trust Network

Federal Government
Social Security Admin.
GSA/DOD - Common Access Card
GSA - ACES
DoD, NASA, NFC - PKI
Transportation Security Administration - TWIC
INS
State Department
Veterans Affairs
Dept. Education

Transportation Industry
TWIC
Aviation
Maritime
Railroad
Trucking
Identification Technologies

- User ID/Passwords
- Knowledge-based authentication

Secure Identification Technologies

- Smart Cards - Card-Based identification
- Public Key Encryption - digital certificates
- Biometric Profiles

Policy-Based Identification Technologies

- Public Key Encryption - digital certificates
Identification Technologies and Smart Cards

• Securely store, protect, and transport cryptographic keys (public/private keys) and digital certificates.
• Capacity to hold multiple keys/certificates.
• Provide secure computational and processing facility without exposing sensitive information to risk.
• Provides security for: generation of digital signature, use of private key for personal authentication, portable permissions/logical access control.
• Convenience for end user.
• PKI can be one set of functions on a multi-application smart card.

Should result in trust and confidence in E-Gov applications.
Government Secure ID Applications

• Secure identification for physical/building access.
• Authentication for logical access (e.g., secure sign-on to networks).
• Authentication for application, data or service access within a system.
• Support for applications requiring secure electronic/digital signature, data encryption/decryption, data storage.
• Authorization and privilege management.
• Storage and access to common demographic information.
• Storage and access to critical health care information.
• Management of licenses and credentials.
• Tamper-proof security for digital credentials.
Federal Secure ID Credential Platform

Card management system and deployment through GSA Common Access Card contract, DoD CAC, and Transportation Security Agency TWIC systems.

Card, data, and architecture specifications consistent with GSA Smart Card Interoperability specification.
Government Secure ID Credentials Concept

1. Form Inter-agency partnership to build common ID requirements.

2. Consolidate requirements to define a common Secure ID specification standard.

3. Deploy Government Secure ID cards through GSA Smart Access Common ID Card Contract to all participating Federal agencies

   **Prime Suppliers:**
   - KPMG
   - EDS
   - Northrup-Grumman
   - Maximus

4. Potential Secure ID Users Interacting with Non-Federal Entities
   - DOD/DOC (Import/Export Licenses)
   - DOT (FAA, etc)
   - INS (Citizens & Foreign)
   - VA Medical (Veterans)
   - Customs (Businesses)
   - FDIC (Banks)
   - States (IL, WA, NJ)
   - AAMVA (Drivers’ licenses)

For More Information

Phone
David Temoshok
202-208-7655

E-mail
david.temoshok@gsa.gov

Websites
http://cio.gov/fpkisc
http://cio.gov/pkipa
http://egov.gov