E-Authentication & HSPD 12

Jeanette Thornton

April 10, 2006

What is the relationship between E-Authentication and HSPD 12?

- Purpose and objectives
- Policy drivers and requirements
- Technical Infrastructure
- Areas of shared interest and responsibility

Identity Management Initiatives

- HSPD-12: Common Identification Standard for Federal Employees and Contractors
  - Improve the security of facilities and IT systems
  - Integrate physical security, information security, and human resources
  - Create a minimum level of trust across the Federal government because of minimum background check
- U.S. E-Authentication E-Government Initiative
  - Support e-gov using Federated Identity Management
  - Accept non-Federally issued online credentials from members of E-Auth Federation

HSPD-12 Credentials will be issued by agencies to:

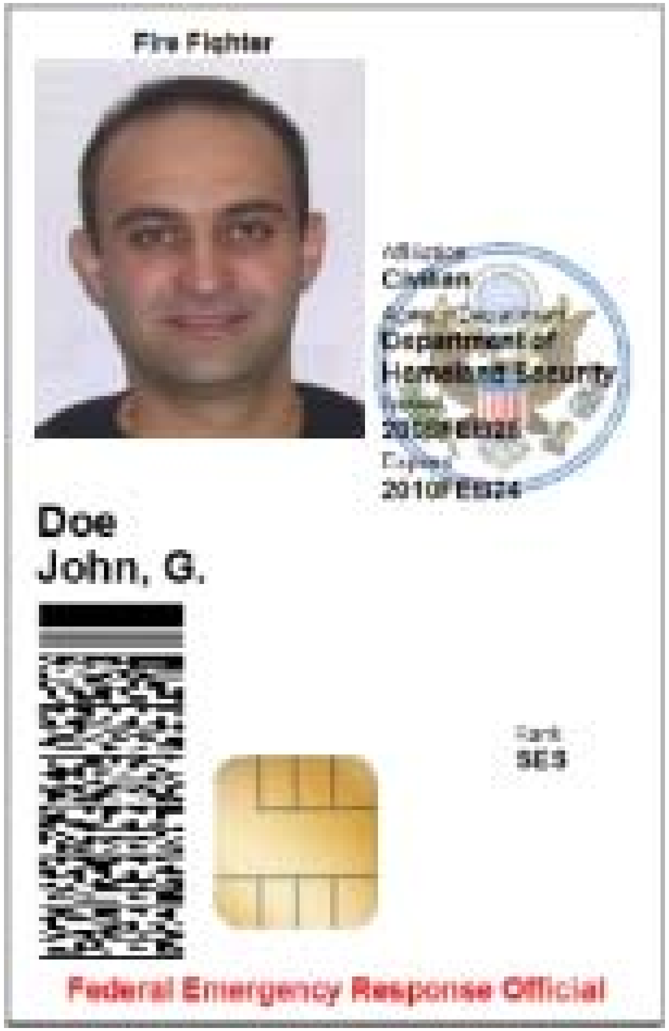
- Federal Employees
- Contractors who require access to federally controlled facilities/information systems
- Other categories based on agency risk (e.g. guest researchers, volunteers, temporary employees under 6 mths)

Based on standard background investigation conducted by OPM

First Deadline to Issue Cards: October 2006

What does it mean?

- Standard ID for all Federal Employees and Contractors
  - Same look
  - Technically Interoperable
  - Standard data storage requirements
  - Used to access IT systems and facilities
- Contact/Contactless Smart ID card



Implications

- Reaffirms the existing “background Checks” required by EO, but new requirement for some government contractors.
- Controls in place to limit use to Federal Government (Facilities/systems)
- Designed to provide routine access to employees and contractors
- Pushing the limits of industry for interoperability (e.g. biometrics)

E☆Authentication: Purpose

- Enable millions of safe, secure, trusted online transactions between Government and the citizens and businesses that it serves
- Reduce online identity management / credentialing burden for government agency application owners and system administrators
- Provide **citizens and businesses** with a choice of credentials when accessing online government agency applications

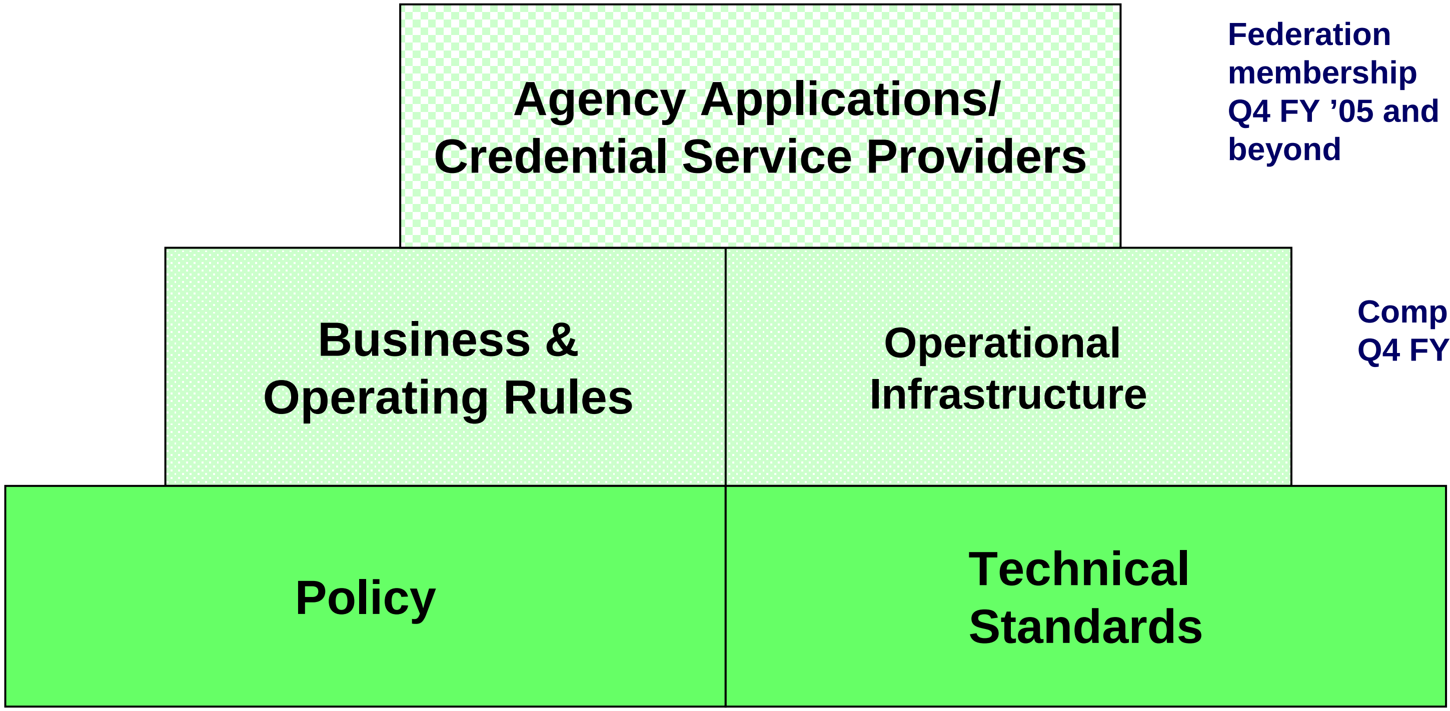
E-Auth uses private sector Credential Service Providers

- Technology Providers/Certificate Authorities
- Financial institutions
- For a limited time ONLY, government credential providers

Future Credential Service Providers

- Credit Card Companies
- Internet Service Providers
- E-Commerce Providers
- State & local government
- Healthcare
- Universities

E-Auth: Pieces



Agency Applications/ Credential Service Providers

Federation membership Q4 FY ’05 and beyond

Business & Operating Rules

Operational Infrastructure

Completed Q4 FY ‘05

Policy

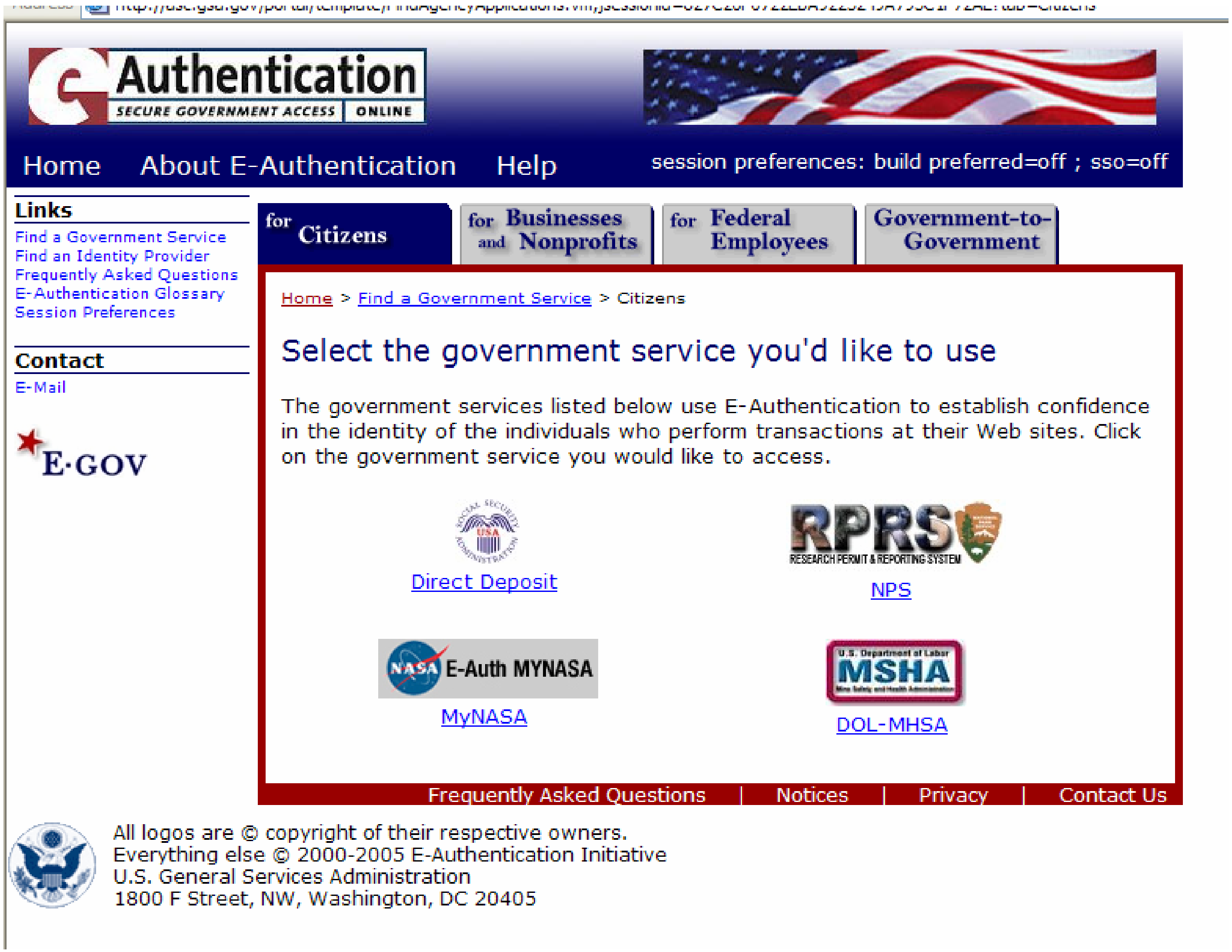
Technical Standards

Completed FY 2004

E-Auth: Technical Standards

- The architecture is based on industry best-practices
  - Open standards-based, federated identity management
  - Security Assertion Markup Language (SAML) 1.0 in place now, SAML 2.0 support planned
  - Liberty Alliance and WS-Federation support is also planned
- First-of-its-kind Interoperability Lab supports
  - Product testing
  - Technical support
  - Private Industry and Agency Application testing
- Architecture supported by interoperable products
  - 9 products on Approved E-Authentication Technology Providers List – meaning all have demonstrated interoperability using SAML 1.0 artifact profile

E-Authentication Metrics



Authentication
SECURE GOVERNMENT ACCESS ONLINE

Home | About E-Authentication | Help | session preferences: build preferred=off ; sso=off

Links

- Find a Government Service
- Find an Identity Provider
- Frequently Asked Questions
- E-Authentication Glossary
- Session Preferences

Contact

- E-Mail

E·GOV

for Citizens | for Businesses and Nonprofits | for Federal Employees | Government-to-Government

Home > Find a Government Service > Citizens

Select the government service you'd like to use

The government services listed below use E-Authentication to establish confidence in the identity of the individuals who perform transactions at their Web sites. Click on the government service you would like to access.

Direct Deposit

RPRS RESEARCH PERMIT & REPORTING SYSTEM
NPS

E-Auth MYNASA
MyNASA

U.S. Department of Labor MSHA
DOL-MHSA

Frequently Asked Questions | Notices | Privacy | Contact Us

All logos are © copyright of their respective owners.
Everything else © 2000-2005 E-Authentication Initiative
U.S. General Services Administration
1800 F Street, NW, Washington, DC 20405

Implications

- Standardization of Federal E-Auth requirements
- Agency Consolidation of Identity Management infrastructure
- Adoption of Standard E-Auth Federation business and operating rules
- Furtherance of privacy goals and citizen choice

Technical Infrastructure

- For Level 3 and 4 credentials govt-wide infrastructure is shared.
  - Leverages Federal PKI infrastructure
  - ACES certificates
- Agencies can use the same infrastructure for identity management/logical access
  - Use approved e-authentication products
  - e.g. USDA’s level 2 applications can be used by both employees and outside parties.

Technical Infrastructure: Cont'd

- Step Down Translator
  - Infrastructure being developed to convert digital certificates to SAML assertions
  - Will allow FIPS 201 card holders to use their credential for E-Authentication's Level 1 and 2 applications
- Path Discovery and Validation

Other Possibilities

- Industry Adoption of FIPS 201
  - – Transportation Credentials
  - – State and local government
  - – Legislative Branch
  - – Other industries/employee credentials
- Health Care
  - – Adoption of Federated Identity

Resources

- E-Authentication
  - – www.cio.gov/eauthentication (PMO site)
  - – http://asc.gsa.gov (portal)

- HSPD-12
  - – http://csrc.nist.gov/piv-project
  - – http://www.smart.gov/fips201apl