


Smart Card Business Roundtable


*Sponsored by
Systems Engineering Inc
Femtosecond Inc
Organizational Change Future Workplace, LLC*



Business Roundtable Agenda

- ▶ *Logistics*
- ▶ *Speaker Introductions*
- ▶ *Guest Introductions*
- ▶ *Business Case and Change Leveraging PIV*
 - *Robert Donelson, OCFW, LLC*
- ▶ *Enabling Physical Access using PIV*
 - *Roy Hayes, Systems Engineering Inc*
- ▶ *Enabling Logical Access using PIV*
 - *Russell Davis, Femtosecond Inc*
- ▶ *Guest Challenges*
- ▶ *Questions and Answers*
- ▶ *Wrap-Up and Next Steps*

Business Roundtable Speaker and Guest Introductions

- ▶ *Robert Donelson, OCFW, LLC*
 - ▶ *Roy Hayes, Systems Engineering, Inc*
 - ▶ *Russell Davis, Femtosecond Inc*
 - ▶ *Guest Introductions*
- 

Change is a Challenge

- ▶ *Change is a Challenge*
- ▶ *Outside Change Factors*
 - *This is an election year a new Administration will soon be upon us!*
 - *Budget – Congress, Administration, World Events*
- ▶ *Competition for Change*
- ▶ *Competition for Who is Going to Bring About Change Exists*
- ▶ *Organizational Culture Exists*
 - *Law of Physics: A Body at rests tends to stay at rest*
- ▶ *What are the Challenges of Change in Your Organization?*

Change Leveraging Opportunities and PIV

- ▶ *Budget Justifications Enable Change*
 - *2009 and 2010 Budget Justifications*
 - *Departmental and Office Annual Budget Directives*
- ▶ *Education and Awareness as a Change Agent*
- ▶ *Clear Vision is a Change Agent*
- ▶ *New Administration is a Change Opportunity*
- ▶ *Increased issuance of PIV provides an Asset, PIV Credential as a Change Agent*
- ▶ *The Economy provides incentive for Change*
 - *Smart Cards were Economical in 1999 with Some Standardization. The Economics are Optimal Today!*

Business Case, Opportunities and Leveraging PIV

- ▶ *PIV Credentials are being issued in FY 2008 to Every Federal Employee and Contractor, 75% of The Investment is being made.*
- ▶ *Strong Secure tamperproof PIV Credentials bound by background Checks are growing in the Federal Sector, Private Sector Comparable Credentials are beginning to follow*
- ▶ *Standards are in place via FIPS-201 and accompanying Special Publications minimizing risks of Private Sector and Federal Sector investments*
- ▶ *Costs and benefits are predictable*
- ▶ *What are your agency Business Challenges?*
 - *We are all already paying for HSPD-12 Functionality in Stovepipe, Duplicative non-standard less secure methodologies*

SYSTEMS ENGINEERING, INC.



Providing Security Solutions

Systems Engineering & Design

**Meeting Today's
Security Requirements
and Tomorrow's Challenges**

Secure Facilities Design, Construction & Accreditation

HSPD-12/FIPS-201 CREDENTIALING

21351 GENTRY DRIVE, SUITE 100
DULLES, VIRGINIA 20166
TELEPHONE (571) 434-6943
FAX (571) 434-7554
POC: ROY HAYES
E-MAIL: ROYHAYES@EARTHLINK.NET
WWW.SYSTEMSENGINEERINGINC.COM

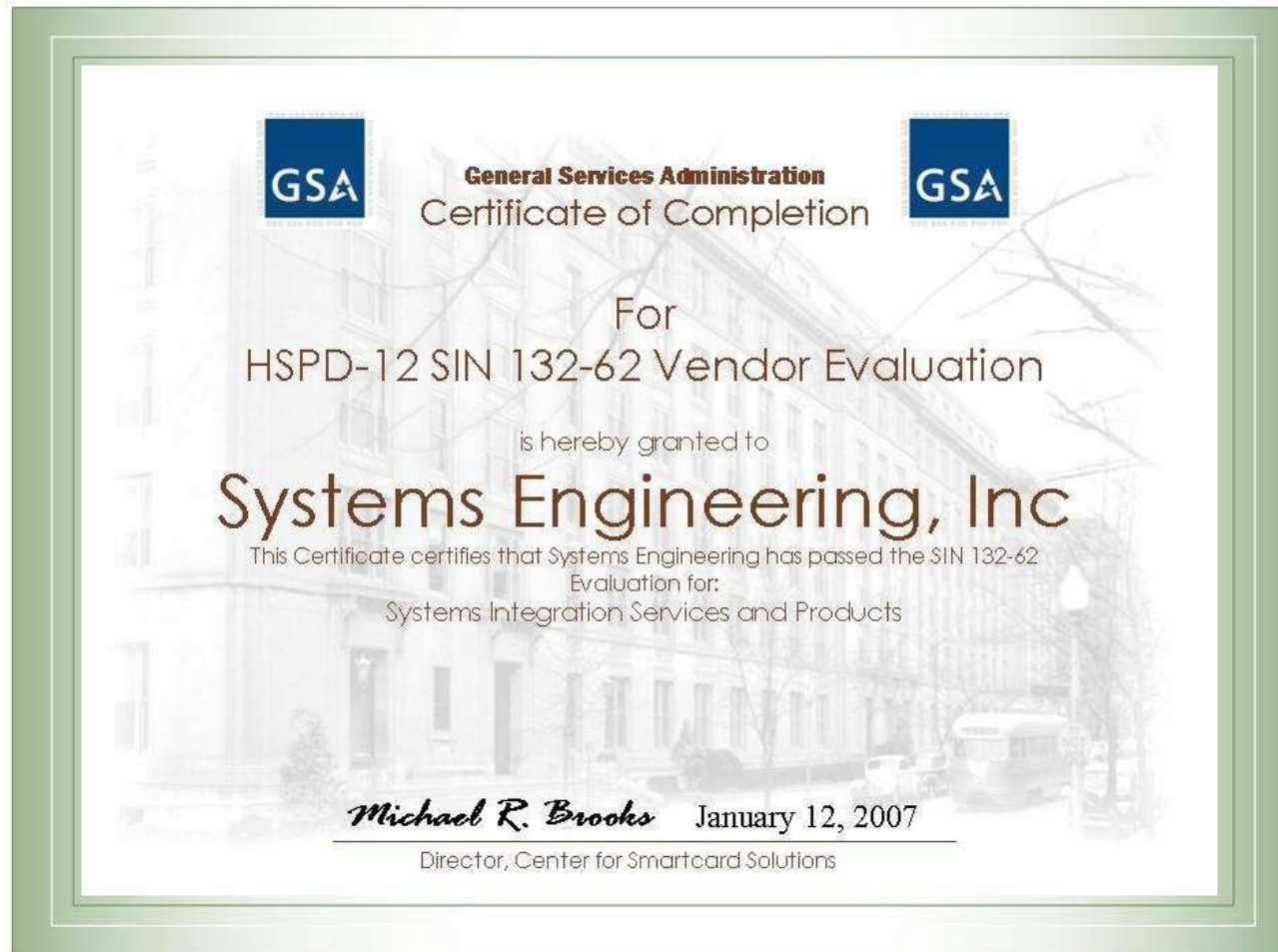


AGENDA

- ▶ Certification
- ▶ HSPD-12 Defined
- ▶ FIPS-201 Defined
- ▶ Proposed Approach
 - Role-Based Model
- ▶ THE Card IS THE ENABLER



GSA Certified PIV Integrator



General Services Administration
Certificate of Completion



For
HSPD-12 SIN 132-62 Vendor Evaluation

is hereby granted to

Systems Engineering, Inc

This Certificate certifies that Systems Engineering has passed the SIN 132-62
Evaluation for:
Systems Integration Services and Products

Michael R. Brooks January 12, 2007

Director, Center for Smartcard Solutions



HSPD-12

- Homeland Security Presidential Directive-12 (HSPD-12) is the policy enacted on August 27, 2004, by President Bush for a Common Identification Standard for Federal Employees & Contractors
- HSPD-12 requires each Federal government agency and department use the same standards when issuing identification badges for employees and non-Federal workers



FIPS-201

- Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005

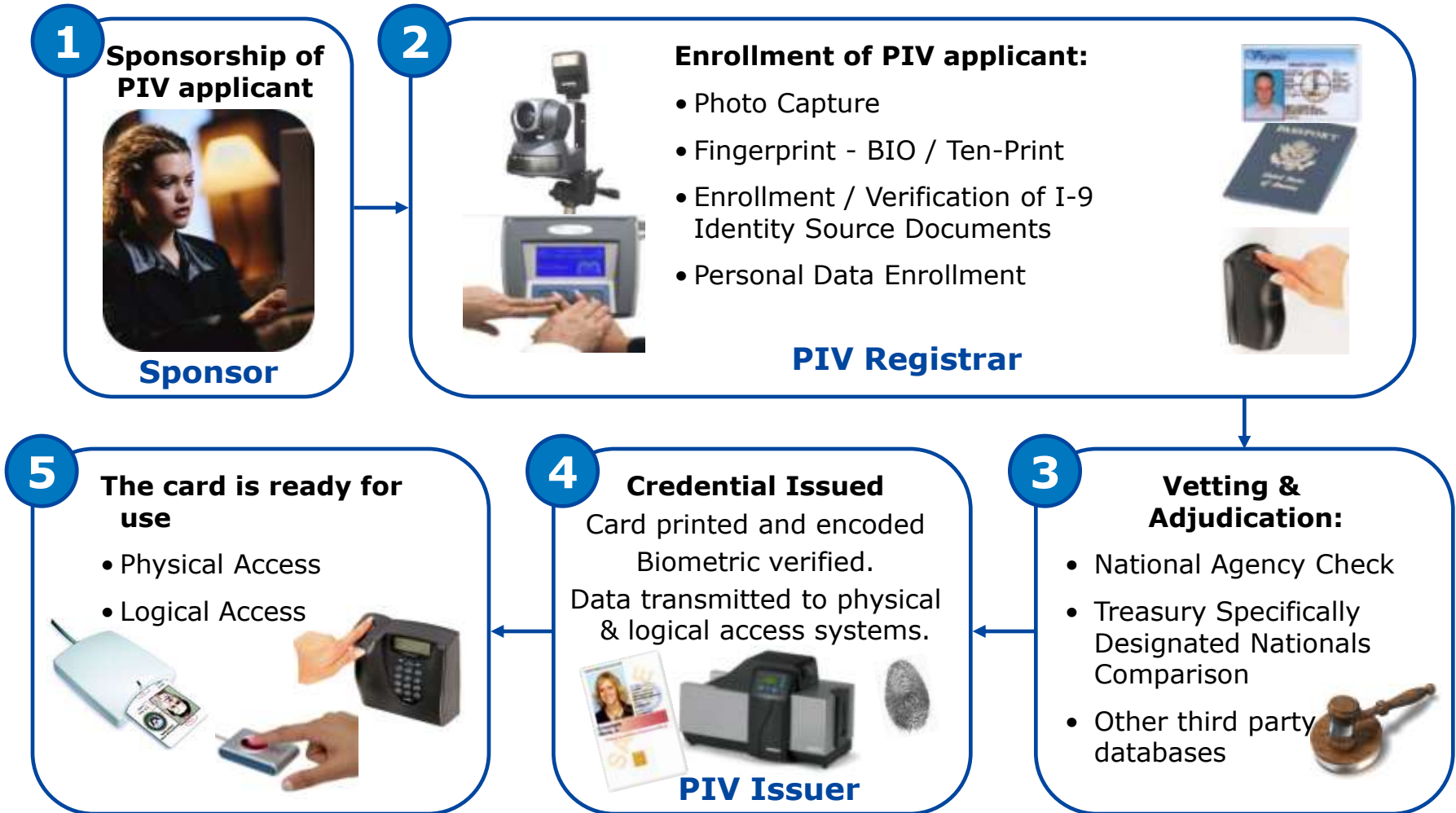


FIPS-201 PREMISE

- *The Smart ID Cards/Badges are issued, based on sound criteria for verification of personal identification.*
- *The SYSTEM is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploration.*
- *Individual identities can be rapidly authenticated electronically.*
- *Identification verifications are issued only by providers whose reliability has been established by an official accreditation process.*



PIV PROCESS FLOW



The comprehensive FIPS-201 compliant identity management system.



THE CARD IS THE ENABLER

- *Identity Management drives the convergence of Physical and Logical Security.*
 - *Personal Identity Verification*
 - *Biometric Identification*
 - *Document Authentication*
 - *Logical System Access*
 - *Multiple Environments (Active Directory, Sun, Unix, etc.)*
 - *Physical System Access*
 - *PACS Independent*



Systems Implementation

- *STEP 1 - SYSTEM SURVEY AND ASSESSMENT*
- *STEP 2 - SYSTEMS DESIGN/INTEGRATION*
- *STEP 3 - SYSTEM INSTALLATION*
- *STEP 4 - SYSTEM CERTIFICATION*
- *STEP 5 - SYSTEMS TRAINING*
- *STEP 6 - FOLLOW-ON SUPPORT*

Smart Card Business Round Table

Russell J. Davis, D.Sc.
CEO Femtosecond Inc.
March 26, 2008

Enabling Logical Access using PIV Cards

Most agencies are getting their PIV cards

Physical and Logical Access approaches will follow

Full utilization of PIV capabilities is mixed

Many are still unaware of the benefits of the PIV card and how security can be enhanced

Security threats that could be mitigated by proper PIV card usage are continuing

Cyber attacks from China

Single user embezzlement at French bank (\$7B)

Phishing attacks

Constant Newspaper Articles about Federal Data and Computers being Lost

Enabling Logical Access using PIV Cards (Continued)

- *Using the PIV card for multiple functions*
 - Physical access control*
 - Logical access control*
 - Password elimination*
 - Network access*
 - Computer access*
 - Application access*
 - Cryptographic function*
 - Digital signatures*
 - Privacy protection*
- *Improving overall security*

Status Quo

- ▶ *The cost of doing nothing*
 - *Security threats are expected to continue*
 - *Increased loss due to malicious software and attacks*
 - *Storm botnet (large numbers of zombie machines)*
 - *Password maintenance is costly*
 - *Increased audit burden*
 - *Negative publicity following successful attacks*
 - *Successful attacks that are currently undetected*

Network Threats Increase Exposure

- ▶ *“From the submissions, IC3 referred 86,279 complaints of crime to federal, state, and local law enforcement agencies around the country for further consideration. The vast majority of cases were fraudulent in nature and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was \$198.44 million with a median dollar loss of \$724.00 per complaint. This is up from \$183.12 million in total reported losses in 2005.” (2006 Internet Fraud Crime Report – www.ic3.gov)*

Alternate Control Costs

- ▶ *Different token technology is expensive*
 - *Licenses*
 - *Training*
 - *Operating*
 - *Distribution and configuration management*
- ▶ *Password do not offer sufficient security*
 - *Without strong identification and authentication there may be no basis for additional security control*

The Potential

- ▶ *The more the PIV card is used, the less the cost per relying application*
- ▶ *Provided the highest NIST SP 800-63 assurance (level 4) for identification and authentication*
- ▶ *The dominant cost is in the personal identity background checks*
 - *If the agency must have PIV cards, why not use them in place of less secure technology?*
 - *The old model that looked for a killer application to justify the cost has been overcome by events*

Organizational Challenges and Questions

