GSA FIPS 201 Evaluation Program Information Day

October 16, 2007

GSA

GSA FIPS 201 APPROVED

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Evaluation Program History

April Giles

GSA FIPS 201 EP History

- Evaluation Program Objectives
- Phases 0-4
- APL status
- Authorized Labs

GSA FIPS 201 EP History

- Evaluation Program Objectives
  - To determine if a Product/Service ***defined by FIPS 201 documentation*** complies with mandated requirements
  - To establish/maintain an Approved Product/Service List (APL) for use by agencies in the acquisition of FIPS 201 Products/Services

GSA FIPS 201 EP History

- Phase 0
  - Analyzed FIPS 201 documentation - NIST
  - Developed a strategy for evaluating disparate technologies concurrently under one laboratory - Evaluation Program Strategy
  - Extracted requirements from FIPS 201 documentation- Created RTM
  - Performed gap analysis defining Card to Reader Interoperability issues
  - Developed and Proposed funding strategy

GSA FIPS 201 EP History

- Phase 1
  - Maintained critical document alignment with FIPS 201 documentation changes
    - RTM
    - FIPS 201 EP Product/Service Category List
  - Defined technology categories
  - Created Card to Reader Interoperability specification → SP 800-96
  - Designed/Built Card/Reader Test Fixture

GSA FIPS 201 EP History

- Phase 2
  - Defined Approval Mechanisms (6)
  - Created Approval &Test Procedures
  - Vetted documents through EPTWG
  - Defined a modular laboratory
    - Paperless applications
    - Web-based application & status portal
    - Lab Specification
    - Website –general info, standards, test tools, test docs
      - www.fips201ep.cio.gov
  - Engaged a contractor to provide lab services which implemented modular laboratory

GSA FIPS 201 EP History

- Phase 3
  - EP Lab Instantiation
  - Designed/Implemented Supplier Fee Structure

GSA FIPS 201 EP History

- Phase 4 (currently in)
  - Developed Lab Qualification Procedure
  - Qualified 2 labs
    - 2 more in the hopper
  - Created EP PMO
    - Maintain EP Lab Docs
    - Maintain Test Software
    - SIN 132-62 products/services
  - Agency Data Validation

GSA FIPS 201 EP History

- APL Status
  - 304 Approved Products listed online at: http://fips201ep.cio.gov/apl.php
  - Averaging 9 days to complete evaluation (after all application info received)

GSA FIPS 201 EP History

- Authorized GSA FIPS 201 EP Laboratories
  1. Atlan Labs
     - Based in McLean, Virginia
  2. InfoGard
     - Based in San Luis Obispo, California

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

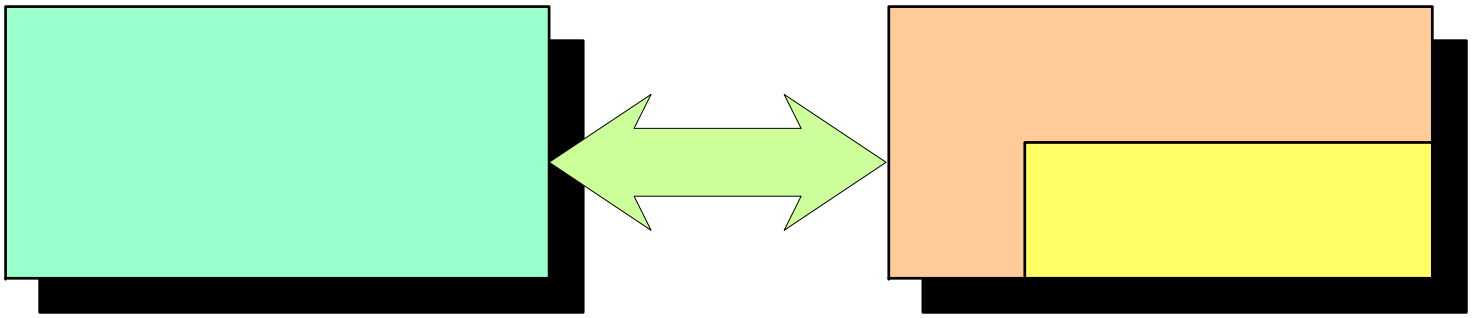
GSA FIPS 201 APPROVED

Updated Evaluation Program Structure and Fees

Nabil Ghadiali

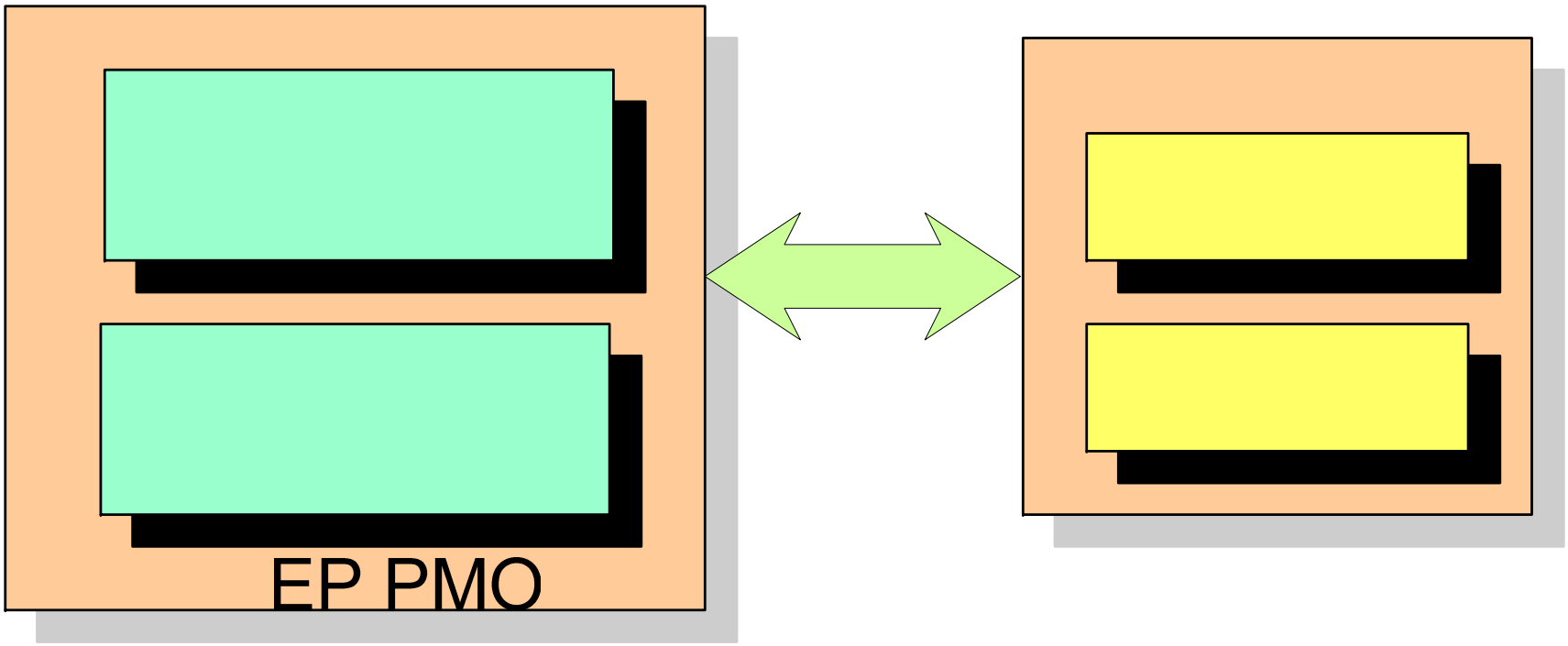
Former FIPS 201 EP Structure

- June 2006 – June 2007



Current FIPS 201 EP Structure

- June 2007 onwards



EP Roles

- GSA
  - Final Authority over all EP policies, procedures documents, forms, tools etc
  - Final Approval Authority for products and services

- Electrosoft
  - Support all aspects of the EP (Login Requests, Website, Lab documents, forms, Tools)
  - Oversee the Lab activities and address evaluation-related issues and concerns
  - Maintain the Approved Products List (APL)

EP Roles

- Evaluation Program Labs
  - Perform evaluation of products and services in accordance with the approval and test procedures
  - Provide suggestions and recommendations to the Program Management Office (PMO) to enhance evaluation criteria and augment Lab efficiency

Evaluation Fees

- Until April 3, 2007
  - No fees levied on Suppliers for Product/Service evaluation
- After April 3, 2007
  - Fees for evaluations borne on a cost-reimbursable basis by the Supplier
  - Fees not dictated by the Evaluation Program PMO
  - Fees independently decided by each EP Lab and are based on number of variable factors (e.g. product/service category, new or upgrade evaluation, etc.)

Lab Documentation (I)

- Lab Specification
  - Provides details on the policies, processes and facility requirements for EP Laboratories
- Suppliers Handbook
  - Provides details on the policies and processes that need to be followed by Supplier submitting applications for evaluation
- Approval Procedures
  - Provides details on the requirements, application package contents and the evaluation criteria for each requirement that applies to a particular category

Lab Documentation (II)

- Test Procedures
  - Provides details on the test cases and the test processes followed by the Lab to evaluate requirements that are tested within the Lab
- Forms
  - Login Request Form, Reseller Acknowledgement Form, Upgrade Form, Non-Conformance Review Form
- Lab Qualification Requirements
  - Provides details on qualification and accreditation of Labs to participate within the EP

EP Lab Qualification

- Qualification Criteria
  1. Accredited by the National Voluntary Laboratory Accreditation Program (NVLAP)
  2. Scope of testing includes NPIVP test methods
  3. Extended their scope of testing to include all GSA FIPS 201 EP test methods
  4. Located in North America

EP Lab Accreditation

- Accreditation Criteria
  - Request an application package from GSA
  - Submit completed paperwork
  - Assign EP Lab Assessor
  - Documentation Review
  - Conduct on-site assessment
  - Perform mock evaluations to determine proficiency
  - Non-conformity notification and resolution (if applicable)
  - Approve the Lab (approval without restriction, interim approval or provisional approval)

Available EP Tools

- SP 800-85B Tool
  - Used for Data Model Conformance Testing (Electronic Personalization)
- INCITS 385 Profile Test Tool
  - Work in Progress
  - Used to test biometric facial image template conformance (Facial Image Capturing Middleware and Electronic Personalization)

***Please note that the Evaluation Program will not provide any support for the usage or debugging of any aspect of these tools.

Available Resources

- EP Announcement Webpage
  - http://fips201ep.cio.gov/announcements.html
- Frequently asked Questions
  - http://fips201ep.cio.gov/faqList.html
- Send queries via email to:
  - fips201eplabmain@gsa.gov (general EP mailbox)
  - April.giles@gsa.gov (EP Chief Architect)
  - nabil@electrosoft-inc.com (Project Manager, Tech Lead)

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Product/Service Category Description

Drew Founds

Product/Service Categories

No.	Title
1	Authentication Key Reader
2	Biometric Reader
3	Card Printer Station
4	CHUID Authentication Reader (Contact)
5	CHUID Authentication Reader (Contactless)
6	CHUID Reader (Contact)
7	CHUID Reader (Contactless)
8	Cryptographic Module
9	Electromagnetically Opaque Sleeve
10	Electronic Personalization
11	Electronic Personalization (Service)
12	Facial Image Capturing Camera

No.	Title
13	Facial Image Capturing Middleware
14	Fingerprint Capture Station
15	Graphical Personalization
16	OCSP Responder
17	Single Fingerprint Capture Device
18	PIV Card
19	PIV Card Delivery
20	PIV Middleware
21	Template Generator
22	Template Matcher
23	Transparent Reader

Fingerprint Acquisition

- Fingerprint Capture Station
  - Hardware device used at enrollment, typically, to capture the Applicant's fingerprints for FBI/OPM criminal history check
  - Software component generates INCITS 381 (image) template for Agency retention
- Single Fingerprint Capture Device
  - Hardware device used at issuance, typically, to capture the Applicant's fingerprint for the 1:1 biometric check before releasing the PIV Card to the Cardholder

Fingerprint Conversion

- Template Generator
  - Software library that generates the INCITS 378 minutiae template to put onto the PIV Card.
- Template Matcher
  - Software library that creates the live fingerprint acquisition template and matches it, to a certain degree of accuracy, to the minutiae template extracted from the PIV Card

Facial Image Acquisition

- Facial Image Capturing Camera
  - The hardware device used to capture the digital picture of the Applicant at the time of enrollment
  - Optionally, software used to control zoom, contrast, brightness, etc. via the camera
- Facial Image Capturing Middleware
  - The software component which wraps the digital photograph in an INCITS 385 profile

Card Graphical Printing

- Card Printer Station
  - The device used to print PIV Cards in accordance with FIPS 201 *and/or* SP 800-104
- Graphical Personalization (Service)
  - The service oriented provider which is able to print PIV Cards in accordance with FIPS 201 *and/or* SP 800-104

Card Data Loading

- Electronic Personalization
  - The software component that orchestrates PIV data object generation, signing, and loading of objects onto a PIV Card
- Electronic Personalization (Service)
  - The service oriented provider which is capable of encoding PIV Cards in accordance with FIPS 201, SP 800-73 and SP 800-78 (800-78-1)

Cardstock & Middleware

- PIV Card
  - The hardware device which serves as the secure platform for HSPD-12 interoperable forms of identification
- PIV Middleware
  - The software libraries that serve as an intermediary between the PIV Card and client applications

Cryptographic Devices

- Cryptographic Module
  - A hardware device which has been certified to FIPS 140-2 Level 2 or higher under the NVLAP CMT program

PIV Card Privacy

- Electromagnetically Opaque Sleeve
  - The hardware device used to hold and display PIV Cards worn by Cardholders. The EOS blocks radio frequencies around13.56 MHz, preventing an adversary from skimming data from a PIV Card

PIV Card Issuance

- PIV Card Delivery
  - The service oriented provider for delivering personalized PIV Cards (MSO: PIV Card pickup) to their respective Cardholders.

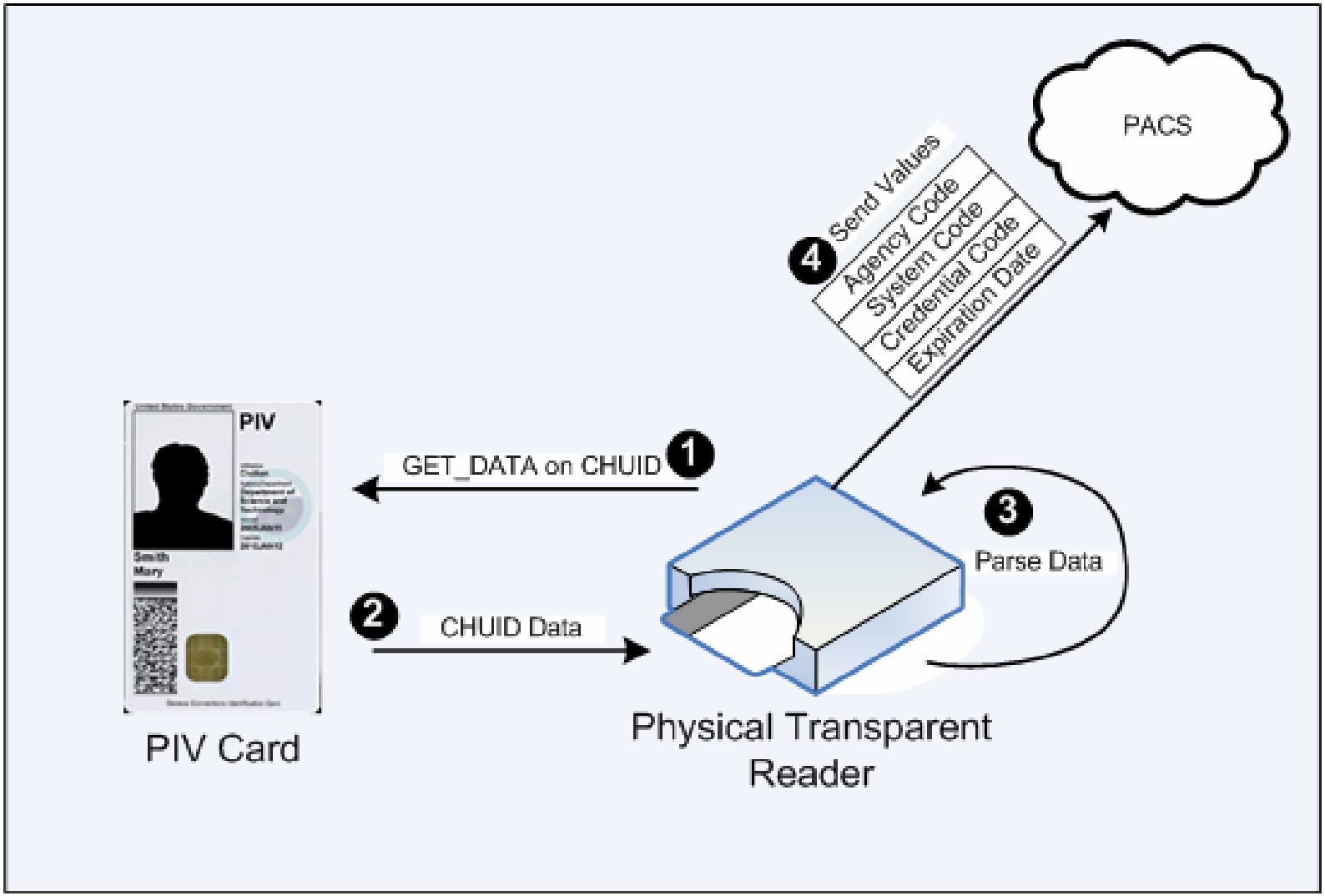
Certificate Validation

- OCSP Responder
  - The hardware device which provides relying parties the revocation status of a certificate in question. OCSP responders must communicate with relying parties via RFC 2560 requests and responses

PIV Card Readers

- Transparent Reader
  - A device used for physical or logical access into a resource. Two types of TREs exist:
    - Logical transparent readers are synonymous with “dumb” smartcard readers
    - Physical transparent readers are to parse 4 fields found in the CHUID to provide to backend systems for the access control decision.
    - Transparent readers can communicate with PIV Cards via the contact or contactless interfaces

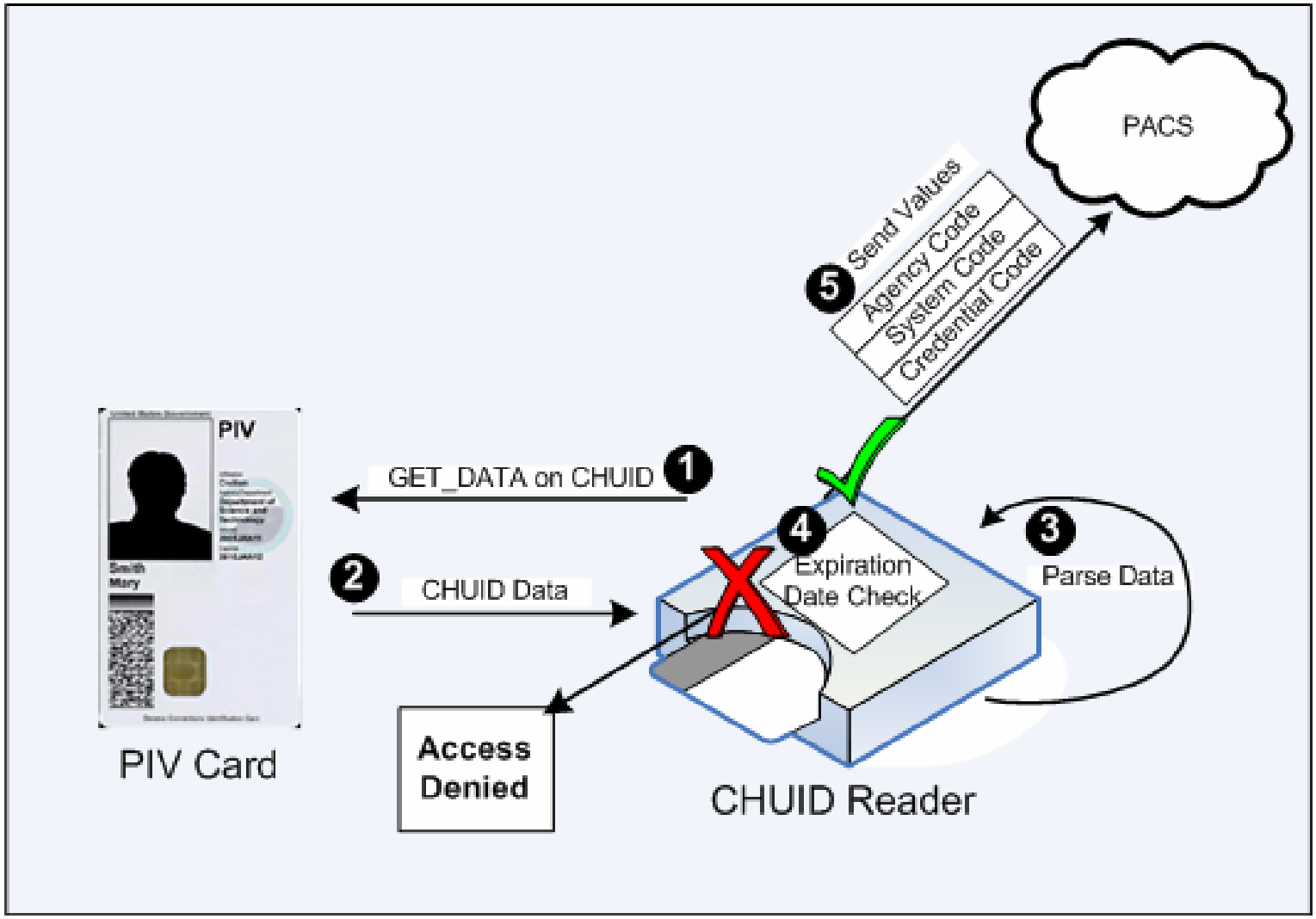
Transparent Reader Depiction



PIV Card Readers (cont)

- CHUID Reader
  - A device used to authenticate a Cardholder using the CHUID, in accordance with the CHUID use case in FIPS 201. CHUID readers, in addition to parsing 4 fields from the FASC-N, determine the expiration date of the PIV Card and provide another value, if needed, to make the access control decision.
  - Two types of CHUID readers exist:
    - Contact
    - Contactless

PIV Card Readers (cont)



PIV Card Readers (cont)

- CHUID Authentication Reader
  - A device which performs the same set of functions as the CHUID reader. In addition, provides the ability to perform certificate path processing and validation, in accordance with RFC 3280
  - Must contain a cryptographic module which as been certified to FIPS 140-2 Level 1

PIV Card Readers (cont)

- Authentication Key Reader
  - A device used to authenticate a Cardholder, using the PIV Authentication Certificate, in accordance with the PIV Authentication Certificate use case in FIPS 201. In addition, provides the ability to perform certificate path processing and validation, in accordance with RFC 3280
  - Must contain a cryptographic module which as been certified to FIPS 140-2 Level 1

PIV Card Readers (cont)

- Biometric Reader
  - A device used to authenticate a Cardholder, using the fingerprint biometrics found on the PIV Card, in accordance with the biometric use case in FIPS 201.

Document Locations

- Approval & Test Procedures
  - GSA FIPS 201 EP Website
- Documents necessary for submission
  - Found within Application Package zip file

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Approval Process (Upgrade Process)

Nabil Ghadiali

Approval Process (I)

1. Review Product/Service Categories
   - If product falls with any one or more categories, it needs to be evaluated by the EP
   - If not, then there is no need to submit it for evaluation

2. Login Request
   - Complete Login Request Form
   - Available at http://fips201ep.cio.gov/obtainlogin.php
   - Email (fips201eplabmain@gsa.gov) or Fax (703-437-9452) the completed form to the EP PMO

Approval Process (II)

3. Download AP Package (Supplier)
   - Read and re-read the Approval Procedure
   - Develop, Gather all necessary Documentation
   - Prepare the Application Submission Package

4. Identify an EP Lab (Supplier)
   - Enter into a contractual agreement (negotiate fees)
   - Approved EP Labs located at http://fips201ep.cio.gov/labs.php

Approval Process (II)

5. Create Application (Supplier)
   - Login to the EP Web Tool
   - Complete the application sheet
   - Select the EP Lab that will perform the evaluation
   - Application Status – "Begin Application"

6. Acknowledge Application (EP Lab)
   - Status updated once fees have been negotiated
   - Must be done within 10 business days after application is created or application will be automatically deleted
   - Application Status – "Package Submitted"

Approval Process (III)

7. Application Package Submission (Supplier)
   - Verify latest version of the Approval Procedure
   - Upload all necessary documentation and submit required artifacts/products to the Lab
   - Must be done within 5 business days after application is set to “Package Submitted” or else application will be rejected.
   - If rejected, within 10 business days to correct the deficiencies or else it will be deleted from the EP Web Tool
   - Application Status – “Package Complete”; EP tool automatically sets status to “Evaluation in Progress”

Application Package

- Typical Application Package Contents
  - Non Disclosure Agreement or Lab Services Agreement depending on whether Lab testing is involved
  - Category-specific Attestation Form
  - VDR/VTDR Worksheet
  - Other relevant documentation (Supplier tests, whitepapers, user guides, technical specifications etc.)
  - Product and/or Sample Artifacts***
  - Reseller Acknowledgement Form

***Please note that as part of the evaluation, any products and/or artifacts submitted will not be returned as these have to be retained for Lab records.

Approval Process (IV)

8. Execution of Evaluation Procedure (EP Lab)
   - Perform Supplier product/service evaluation based on current version of Approval Procedure and Test Procedure (if applicable)
   - Product/Service evaluated using approval mechanisms applicable for that category
   - Performed within 10 business days after application is deemed complete by the EP Lab
   - Application Status – "Evaluation Complete"

Approval Process (V)

9. Evaluation Report Preparation (EP Lab)

- Prepared irrespective of whether product/service is conformant or not
  - Application Status – "Evaluation Report Complete"
- If yes, evaluation report and approval request letter submitted to the GSA Approval Authority
  - Application Status – "Awaiting Govt. Approval Authorization"
- If not, evaluation report and non-conformant letter submitted to Supplier
  - Application Status – "Non-conformant"

Approval Process (VI)

10. GSA Approval (Approval Authority)
    - Discusses any issues or concerns with the EP Lab for the evaluation performed
    - Final Government approval of product/service for placement on the APL
    - Application Status – "Approved"

11. Placement on the APL (EP PMO)
    - Performed within 1 business day of product/service being approved by the GSA Approval Authority

Approval Process (VII)

12. Non-Conformance Review (All)

- Initiated by the Supplier if the Supplier feels that the product/service was wrongly deemed non-conformant
- Supplier completes the non-conformance review form, uploads it to the case number and notifies the EP Lab
- EP Lab reviews the evaluation performed with the GSA PMO and schedules a material review meeting with the Supplier
- EP Lab discusses the application evaluation and findings with the Supplier
- EP Lab documents final outcome and notifies Supplier
- If approved, Product placed on the APL within 1 business day

Approval Mechanisms (I)

- Site Visit
  - Primarily used in the case of Services
  - Duration limited to 2 consecutive days

- Vendor Test Data Report (VTDR)
  - Technical report submitted by the Supplier demonstrating the conformance of the product/service to one or more requirements for that category
  - Details can be found in Appendix A.2 of the Supplier Handbook

Approval Mechanisms (II)

- Lab Test Data Report (LTDR)
  - Technical report generated by the Lab during the evaluation process.
  - Provides the test results for requirements that are tested in the Lab
- Vendor Documentation Review (VDR)
  - Formal Supplier document demonstrating the conformance of the product/service to one or more requirements for that category
  - Examples include marketing literature, flyers, brochures etc.

Approval Mechanisms (III)

- Certification (C)
  - Certification statement (from an authority other than an EP Lab) stating the compliance of the product/service to a particular requirement (e.g. NIST FIPS 140-2 certification).

- Attestation (A)
  - Formal statement provided by the Supplier providing testimony to the fact that the product/service meets the necessary requirements for that category.
  - Must be signed by a minimum “C” level individual, e.g. CSO, CEO, CIO, CFO, Vice-President, President, Business Partner or Owner

Supplier Product/Service Updates

- Supplier upgrades product/service
  - Upgrade process – only if part number remains the same
  - Create a new application with the EP Web Tool
    - Complete and upload the Upgrade Form
    - Provide documents substantiating changes that have been made from previous version
  - EP Lab performs an evaluation to determine if previously tested requirements are affected
  - Based on EP Lab decision, product listing is either updated on the APL or product is partially or completely re-evaluated within the Lab

***Please note that if both products (original and updated) need to be listed on the APL, then the part number must be different.

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Approved Products List

April Giles

EP Approved Products List

- HSPD-12 Source for Products & Services
- Evolving List
- Difference between “tested with” vs “restricted for use with”
- Authoritative Source

EP Approved Products List

- HSPD-12 source for Products & Services
  - Evaluated in GSA Approved Lab
  - Online access
    - http://fips201ep.cio.gov/apl.php
  - Use mandated by:
    - OMB m05-24
    - FAR 2005-17
  - Not an Acquisition Vehicle
  - Sortable (with click on column header)
  - Item from each category ≠ HSPD-12 solution

EP Approved Products List

- Evolving List
  - Must comply with current AP requirements
  - Requirement change notification
    - Upgrade policy- discussed in detail in letter session
  - Fees
    - Government does not regulate

EP Approved Products List

- Difference between “tested with” vs “restricted for use with”
  - “tested with”
    - Some categories can comprise multiple categories
      - EP, EPS, OCSP Responder
    - Overall configuration includes additional components from another category/ies
    - Components can be exchanged with APL listed components
  - “restricted for use with”
    - Also equates to “approved with”
    - Component is an integral part of the solution
    - Configuration Solution has multiple options
      - Example
        - » EP (product or service) with 1024 vs 2048 bit keys
  - Approved Products List

EP Approved Products List

- Authoritative Source
  - http://fips201ep.cio.gov/apl.php
- No other websites
  - Other published lists may not be current

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

SIN 132-62 and the Approved Product List

Pat Brooks

GSA

GSA's Federal Acquisition Service

Federal Acquisition Service

Integrated Technology Services (ITS)

Center for Information Technology Schedule Programs

Pat Brooks
Director

E-Authentication Initiative

- **Current Special Item Numbers (SIN)**

  -132-60 Access Certifications for Electronic Services (ACES) Program

  -132-61 PKI Share Service Providers (PKISSPP) Program

  -132-62 HSPD 12 Products and Service Components

E-Authentication

- Proposed change
  -Approved Product List
  SIN 132-62
  -Services and Services Components
  SIN 132-63
- Qualification and certification requirements remain unchanged for both SINs

Process

- **Establish new SIN 132-63**
  - **30-45 days**
- **Update solicitation**
  - **45-60 days**
- **Modify existing contracts**
  - **Based upon submission of proposals**

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Evaluation Program Technical Working Group (EPTWG) Announcement

Nabil Ghadiali

EPTWG Mission

- To strengthen the FIPS 201 Evaluation Program and the evaluation of PIV components to meet the intent of HSPD-12

EPTWG Objectives

- To obtain feedback from Agencies and Private Industry on the Approval Procedures
- To engage in dialogue with the EP to provide feedback on EP Lab and EP activities
- To provide technical support in the variety of technology areas touched by HSPD-12

EPTWG AP Update Process (I)

- EPTWG distribution list creation
  - Interested parties send email to fips201eplabmain@gsa.gov with Subject Line stating "Request for EPTWG Participation"

- Engage in a public comment period
  - Using the distribution list and the announcement page on the EP Website inform the EPTWG participants of the comment period on the approval procedures

EPTWG AP Update Process (II)

- Document Comments
  - EPTWG Participants document comments in EP provided template
  - Email the completed comments spreadsheet to fips201eplabmain@gsa.gov within the timeframe
- Compile Comments
- Update Approval Procedures
  - EP Labs use updated documents for evaluations

Other EPTWG Sessions

- Notify EPTWG Participants
  - Using the distribution list
  - Date and Time for the Meeting (anticipated monthly)
- Solicit Feedback on potential discussion topics
- Develop and Distribute Agenda
- Hold EPTWG Session

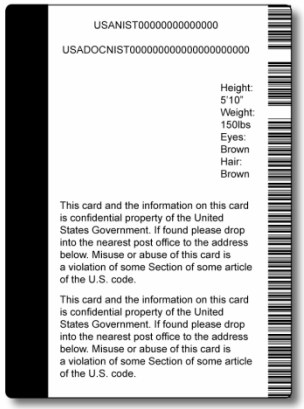
Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Recent NIST Document Updates

William MacGregor



NIST Personal Identity Verification Current Activities

National Institute of Standards and Technology
William I. MacGregor
2007OCT16 GSA HSPD-12 EP Information Day

From Jan07 IAB:

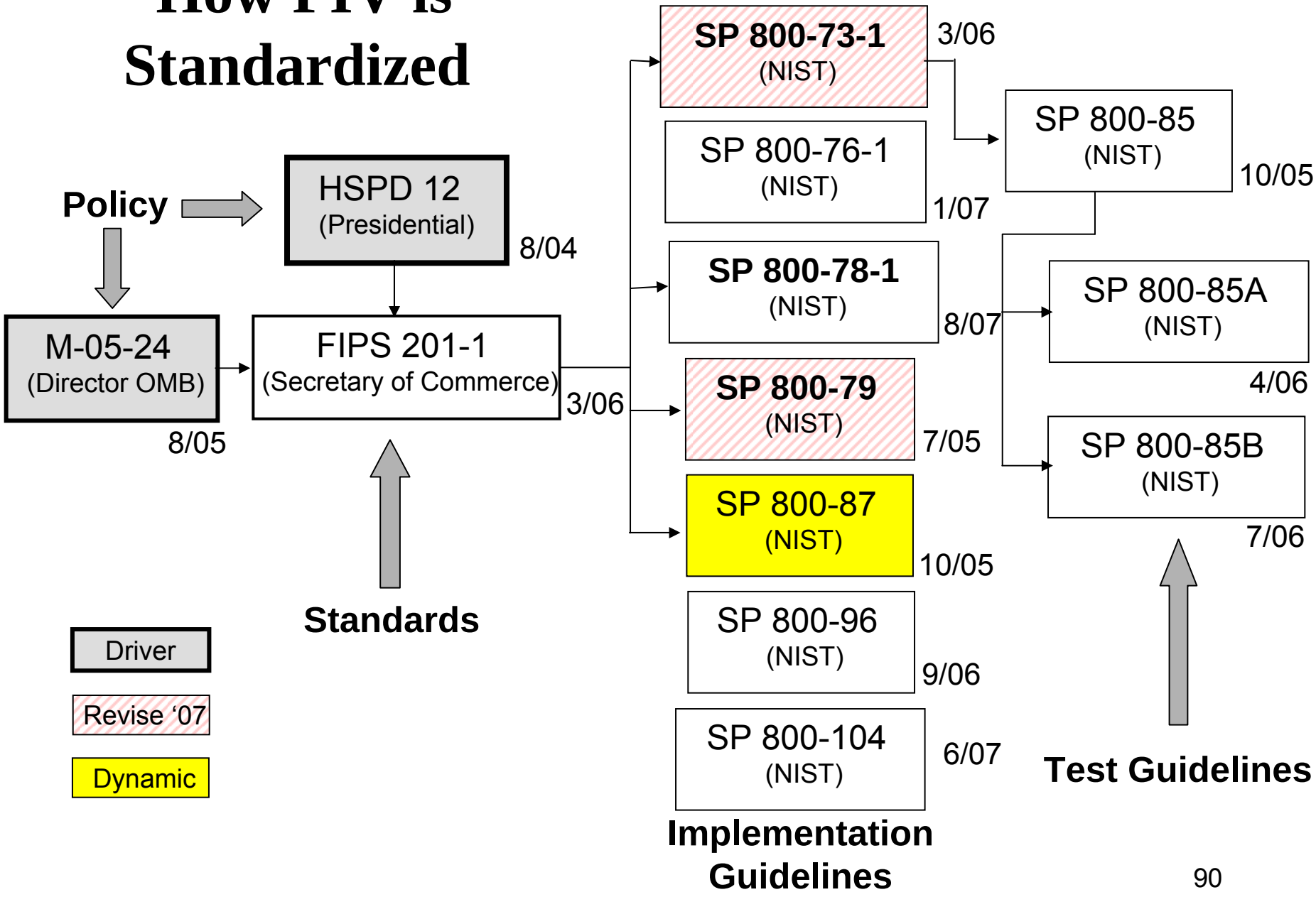
NIST PIV Strategy in 2007

1. Respond to critical urgencies as they arise.
2. Provide application examples & advice.
3. Complete revisions already committed.
   - SP800-76-1 editorial improvements
   - SP800-78-1 and SP800-73-2 changes
   - SP800-104 (color coding)—it's *optional*
4. Technology transfer beyond HSPD-12.
5. Begin work towards PIV step-up.

Recent PIV Activities

- SP800-78-1 FINAL - Tim Polk & Donna Dodson, Lead
- SP800-73-2 DRAFT - Hildy Ferraiolo, Lead
- SP800-79-1 IN PROGRESS - Ramaswamy Chandramouli, Lead
- NISTIR 7452 RESEARCH - Secure Biometric Match-On-Card (SBMOC) Feasibility Report - Bill MacGregor, Lead

How PIV is Standardized



SP800-78-1 FINAL, Crypto Algorithms

- Published on http://csrc.nist.gov
- Correction (made in published text):
  - May be used before 1 Jan 2008 (or -78)
  - Must be used after 1 Jan 2008 (replaces -78)
- SP800-78-1 does not invalidate any properly issued cards

SP800-78-1 Major Changes

- Adjust sunset dates for RSA 1024, SHA-1, and 2TDEA (same as or later than -78)
- Simplify PIV on-card algorithm choices
  - RSA 1024 or RSA 2048
  - ECC P-256 or P-384
  - 2TDEA, 3TDEA, AES-128, -192, -256
- Document PIV key references & algorithm identifiers in SP800-78-1

SP800-73-2 DRAFT, PIV Card Technical

- Sync -73-2 with changes mandated by -78-1
  - Sunsets of 2TDEA, RSA 1024, SHA-1 defined in -78-1
  - Key reference tables and algorithm identifiers tables are referenced from -73-2
- Introduce optional Unsigned CHUID (UCHUID)
- CAK-based authentication use cases
- Informative discovery mechanism discussion
- Reorganize into Parts (editorial)
- Incorporate the current Errata
- Available for public comment at http://csrc.nist.gov

SP800-79-1 IN PROGRESS, Issuance System C&A

- Existing SP800-79 predates first C&A
- Now is the time to capture experience!
- More detailed methodology proposed to help assessors, but deciders need summaries
- Complete traceability to FIPS, SPs, OMB Memoranda
- Public draft expected Dec 07 or Jan 08

NISTIR 7452 RESEARCH , SBMOC Feasibility Study

- Secure Biometric Match-On-Card (SBMOC)
- Potential advantages of SBMOC approach
  - Biometric over contactless without PIN
  - Security, Interoperability, & privacy improvements
  - Secure communication without per-reader key management
- Feasibility Question:
  - Can electronic verification be done in <=2.5 sec while meeting functionality, biometric accuracy, and security constraints?
- Solicited industry participation in SBMOC study
- Performance, functionality, and security tests completed
  - Goal met by 17 cards from 4 suppliers
- MINEX II accuracy testing is in progress
- Draft NISTIR 7452 feasibility study report in review

Thanks for listening!

Bill MacGregor
NIST PIV Coordinator
301 975 8721
william.macgregor@nist.gov

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Effect of NIST Document Updates on EP

Drew Founds

Overview

- Process of updating an AP
- Process for Suppliers to update products
- Recently updated APs

Process

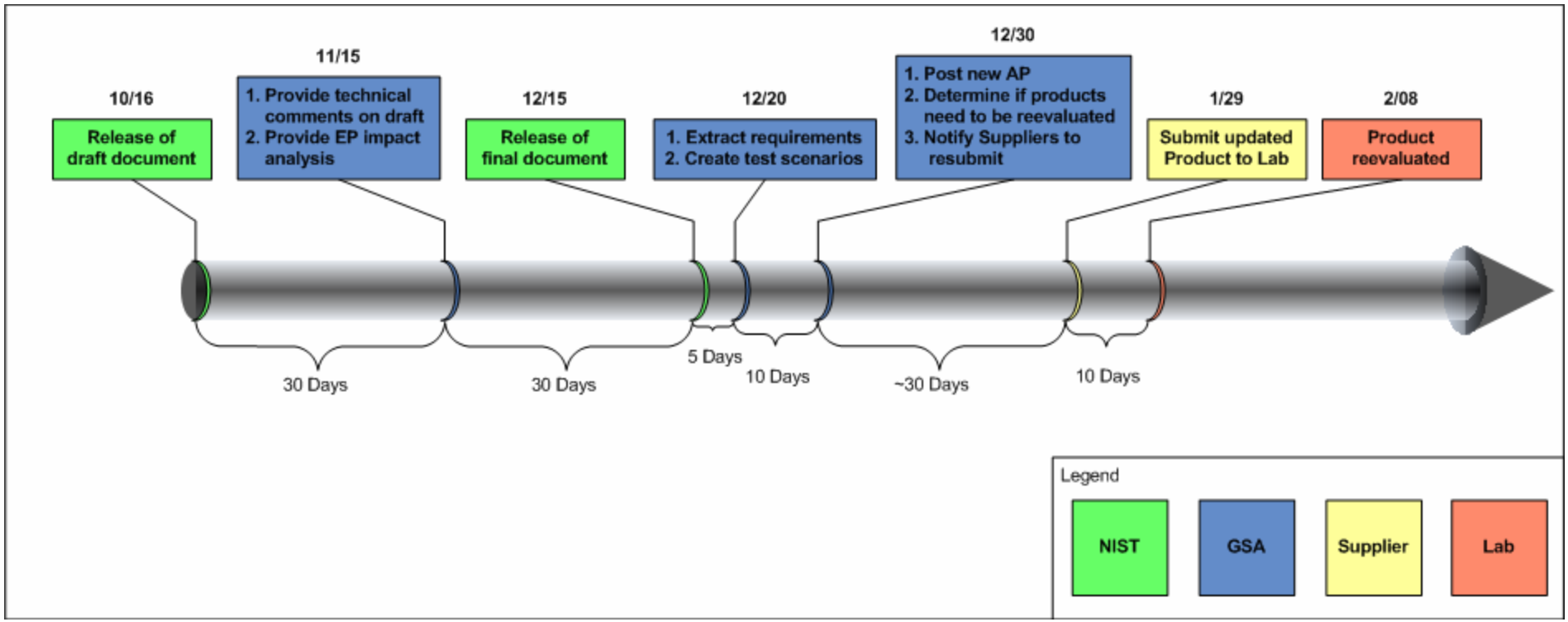
1. NIST releases a new draft or updated document
   - 30 day comment period
2. GSA Comments on Public Draft
   - Informs NIST on impact of approved Products
3. NIST releases a final version of document
4. GSA performs analysis on final version
   - GSA extracts requirements
   - Test scenarios for each requirement discussed

Process (cont)

5. GSA PMO updates APs & TPs
   - Typically 10 – 15 day period
   - Labs determine whether or not products need to be reevaluated
   - Suppliers are notified if an update to Products/Services is needed
     a) Meet technical requirements
     b) Incorporate new optional features
   - Length of time
6. Supplier Updates Product
   - GSA requires agreement from Supplier for deadline

Example Timeline

NIST releases draft SP today



Product/Service Upgrade Process

- Non-Conformant products must be resubmitted
- Special case
  - SP 800-78-1 – Optional compliance until Jan. 1, 2008
- All upgrades submitted in accordance with upgrade process

Recent Document Updates

- SP 800-104
  - Affects the Card Printer Station & Graphical Personalization Categories
  - Updated document to be posted this week
  - New PIV Card layout options
  - 2 optional cards may now be submitted
  - FIPS 201 requirements are still mandatory for all CPS/GP submitted to the Labs

Recent Document Updates (cont)

- SP 800-78-1
  - Effects the Electronic Personalization categories
  - Effective date immediately
    - Compliance until Jan. 1, 2008 is optional
    - Compliance after Jan. 1, 2008 is mandatory
  - Updated document to be posted this week
  - All products & services will be reevaluated in January 2008

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Agency Card Testing

April Giles

Agency Card Testing

- M07-06
- Overview of GSA 800-85B test tool
- GSA 800-85B test tool demo

Agency Card Testing

- M07-06
  - memorandum discusses validation and monitoring agency issuance of Personal Identity Verification (PIV) compliant identity credentials.
    - Validate data containers
    - Quarterly status reports
  - All agencies must provide to GSA by January 19, 2007, a credential with their agency's standard configuration.
  - GSA EP has 3 weeks to complete testing
    - Average completion time is 3 days
  - Configuration change does not require repeat testing
- OMB Memoranda 07-06

Agency Card Testing

- Overview of GSA 800-85B test tool
  - Original Created by NIST
    - Version 2.98
    - 5 test groups
      - » Authentication (Authentication Key, CHUID)
      - » BER-TLV conformance
      - » Biometric data conformance
      - » Certificate data conformance
      - » Digital Signature data conformance
  - Validates 800-73-1 End State data model req
    - Format (fields, and container)
    - Mandatory information
  - Does not validate data content accuracy

Agency Card Testing

- Overview of GSA 800-85B test tool
  - Significant revisions by GSA
    - Current Version 4.0.1
    - Compliant to SP 800-78-1

    - Major changes
      - » Improved error reporting
      - » Auto update of 9A key
      - » Data container Output and storage
      - » Inserted 800-85B test #'s and EP req. #'s
      - » Fixed various Test Cases
      - » Reduced test time

  - Available for download online at:
    - http://fips201ep.cio.gov/tools.php

Agency Card Testing

- GSA 800-85B test tool demo

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Questions & Answers

Topic	Speaker
Welcome	Mary Mitchell
Evaluation Program History	April Giles
Updated Evaluation Program Structure and Fees	Nabil Ghadiali
Product/Service Category Description	Drew Founds
Approval Process (Upgrade Process)	Nabil Ghadiali
Break	-
Approved Products List	April Giles
SIN 132-62 and the Approved Product List	Pat Brooks
Lunch	-
EPTWG Meeting Announcement	Nabil Ghadiali
Recent NIST Document Updates	William MacGregor
Effect of NIST Document Updates on EP	Drew Founds
Agency Card Testing	April Giles
Questions & Answers	-
Closing Remarks	April Giles

GSA

GSA FIPS 201 APPROVED

Closing Remarks