WHITE PAPER

The Green Scorecard Plan—Meeting HSPD-12 on time and on budget

Deploying a high-assurance, FIPS-201-compliant issuance process

TABLE OF CONTENTS

Government agencies are under immense pressure to meet Homeland Security Presidential Directive 12 (HSPD-12) within the mandated deadline. The objectives of HSPD-12 are to protect the security of federal facilities and systems, to increase government efficiency, to reduce identity fraud, and to protect personal privacy. To support these objectives, HSPD-12 establishes a new federal standard requiring US government agencies to begin issuing secure and reliable forms of identification to all federal employees and contractors by October 2006. Agencies who are successful in implementing this program will earn a "green" rating on the President's e-Government scorecard. The standard—Federal Information Processing Standards Publication 201 (FIPS 201)—provides the technical specifications and minimum issuance criteria for Personal Identity Verification (PIV) cards.

FIPS 201 requires agencies to establish a trusted identity proofing and registration process for issuing PIV cards because these cards could be dangerous in the wrong hands. PIV smart cards authorize physical access to federally controlled facilities and logical access to federal computer systems. They can also enable PIV card holders to digitally sign electronic documents. For these reasons, your PIV issuance process must be strongly resistant to fraud, tampering, counterfeiting, and falsification. It must also demonstrate a highly auditable chain of trust in order to meet accreditation requirements. However, as the deadline for issuing credentials draws near, most agencies are urgently trying to find ways to deploy an accredited issuance process when little or no additional funding exists to support the project.

This white paper explains how Adobe enterprise solutions can help your agency meet the intent of HSPD-12 and comply with FIPS-201 requirements, on time and on budget, by delivering an automated and streamlined PIV issuance process and high-assurance workflow. Your agency can leverage the free Adobe® Reader® software, Adobe LiveCycle™ server software, and Adobe best-in-class digital signature solutions to incorporate intelligent electronic documents into an automated process, resulting in shortened cycle times and lower PIV card issuance costs. Once you've implemented your Adobe solution, you can benefit by extending the same workflow and process automation to streamline additional mission-critical, inter-agency and intra-agency processes.

Automate processes to reduce the time and cost of PIV card issuance

As your agency races to comply with HSPD-12, implementing automated processes becomes a high priority. Process automation helps overcome the challenges of manual, paper-based processes:

- Labor-intensive manual processing and data re-entry increase the risk of errors and use limited staff resources ineffectively
- The costs of handling paper—printing, copying, faxing, mailing, and archiving—consumes your limited funds
- Stove-piping of existing data in back-end systems makes it difficult to extract, exchange, and incorporate data into business processes
- Hybrid processes that mix electronic and paper-based steps complicate process automation and management
- Compliance with Section 508 guidelines to allow accessibility for people with disabilities requires additional time and resources

In order to issue PIV cards faster and more efficiently, you need a solution that connects documents, people, and processes. This solution should provide an automated, end-to-end electronic process that enables document auto-generation, form auto-fill, instant document delivery, easy interaction with participants in other agencies—including people with disabilities—and allows manual steps when necessary. Such an automated solution would not consume the time and money typical of paper-based processes.

Adobe's automated, fully interoperable solution connects people, information, and processes
Adobe LiveCycle streamlines critical business processes to allow agencies to share information more securely and flexibly, and to accelerate the issuance process. It reliably and efficiently delivers actionable information to the right person—applicant, sponsor, registrar, signatory, or issuer—based on business rules and policies. To reduce manual keying errors, Adobe LiveCycle automatically pre-fills PDF forms with data from back-end systems. When people do need to key data into electronic forms, built-in business logic and error checking improve the accuracy, completeness, and consistency of that data. These capabilities reduce your data entry costs, improve quality of information, and ensure consistency with official information of record.

Process automation tools in Adobe LiveCycle let you automate document-based workflows and incorporate your agency's own business rules. The software supports your procedures by delivering intelligent electronic documents using e-mail or the web—using free Adobe Reader software—so that authorized people can participate in the process, whether inside or outside your firewall. Even when you require paper forms signed with wet-ink signatures, you do not need to revert entirely to a manual process. Adobe captures the paper-based form data in a 2D barcode, so you can simply scan the form and automatically extract the data into your back-end systems without re-keying. Adobe also makes it easier to create intelligent documents and forms that are accessible to people with disabilities.

The Adobe LiveCycle software leverages your agency's existing IT investments by unlocking valuable information from back-end systems and delivering it in a richer, more secure manner. The result is an immediate, faster, and more cost-effective way to review, verify, and approve the documentation for PIV card issuance–and automated workflows you can leverage later to expedite other business processes.

Build a high-assurance PIV process to meet accreditation requirements

To comply with FIPS 201, your agency must design and deploy a high-assurance identity proofing, registration, and issuance process that is:

- Repeatable and consistent
- Measurably secure and resistant to manipulation and falsification
- Auditable and demonstrably compliant with FIPS 201

The process must only allow authorized individuals to approve documents. You need to ensure that document integrity and authenticity are protected, and that you can audit the source of information at every stage in the process.

BENEFITS OF USING DIGITAL SIGNATURES IN PIV CARD ISSUANCE

- Enables automation and delivery of a high-assurance electronic PIV process
- Supported by legislation like the Electronic Signatures in Global and National Commerce Act (E-SIGN), enabling the replacement of written signatures on paper with digital signatures on electronic documents for business transactions
- Complies with the Federal Bridge Certificate Authority (FBCA), who links agencies' public key infrastructures (PKIs) so that agencies can trust a single point to verify digital signatures from any federal employee

Adobe enables persistent, dynamic, and auditable security

With the Adobe LiveCycle enterprise solution, you can control documents throughout the PIV process by applying persistent and dynamic security policies. A security policy specifies which individuals or groups are authorized to access, modify, or extract information from each document. Adobe document control is persistent because the security policy travels with the document at all times. It's also dynamic, because it enables you to change and update security policies at any time, even after distribution. This gives you control over information no matter where a PIV document resides—inside or outside the firewall, on a local hard drive, or even burned to a CD-ROM.

Adobe delivers a high-assurance PIV process that lets agencies:

- Certify and digitally sign all documents to help ensure authenticity and integrity
- Set access policies for documents inside and outside the agency to protect confidentiality
- Dynamically change who can access a document and what each person can do with it—open, print, forward, copy, or modify
- Audit the document history to determine what actions were taken on it, by whom, and when
- Assign different policies to people or groups who access the same document
- Instantly revoke document access, even after distribution
- Send documents more securely to personnel in other agencies
- Comply with the NIST PIKTS and Department of Defense JITC specifications for digital signature verification

DEFINING PERSISTENT DOCUMENT SECURITY

With persistent document security, security parameters are an integral part of the document, and address:

1. Confidentiality: restricting who has access to the document
2. Authorization: defining what each user is allowed to do with the document
3. Accountability: tracking what each recipient has done with the document
4. Integrity: recording if the document has been altered
5. Authenticity: tracking where the document came from

Steps for deploying Adobe enterprise solutions for a FIPS-201-compliant PIV issuance process

The PIV smart card issuance process can be subdivided into three main sub-processes:

A. PIV request generation

B. PIV identify proofing and request approval

C. PIV Card issuance

Adobe LiveCycle software supports each of these sub-processes with more secure, automated electronic workflows.

A. PIV request generation:
Bridging paper and electronic processes to help ensure the generation of authentic requests

Adobe can save your agency the costs of manual processing, data entry, and handling paper by enabling the electronic creation, auto-fill, and routing of all documents involved in the generation of a PIV card request.

Even more important, however, is security: your agency must be confident that the process of generating a PIV card request is completely secure. If it is possible to fraudulently generate a request, no amount of security in the remainder of the process matters. Adobe LiveCycle enterprise solutions greatly reduce the ability to manipulate and falsify a PIV request.

All documents and form templates used in the PIV process can be certified and policy protected. Certification is a special way to apply a signature to a PDF, ensuring that the form is authentic and that no one has manipulated its appearance, business logic, or data structure. Policy protection is a method of providing persistent and dynamic security controls on a document within and beyond the firewall and throughout the life of the document. You can also set up your process to require documents be digitally signed by PIV-authorized individuals to indicate their approval, and require that all forms be certified and/or policy-protected before they are sent.

PIV CARD ISSUANCE PROCESS

(As defined by the Federal Identity Management Handbook)

A. PIV request Generation:

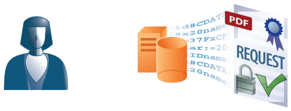
1. **Sponsor initiates PIV request**
   - Sponsor completes a PIV request on behalf of an Applicant and submits it to the Registrar and Issuer
2. **Registrar validates request**
   - Registrar confirms the validity of the Sponsor request
3. **Applicant submits application**
   - Applicant completes a questionnaire, prints, signs, and sends it to the Registrar

Adobe LiveCycle enterprise solutions offer a high and measurable degree of overall process assurance: ensuring the reliability of requests, verifying the authenticity of documents and their sources, providing confidentiality and control over documents throughout their lifecycles, and requiring accountability for responsibilities and approvals.

At each step of the process, Adobe technology delivers high-value process automation and assurance as shown in the figures below.

A PIV request generation

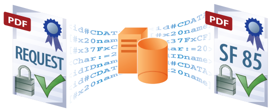
1. Sponsor initiates PIV request



- Sponsor initiates a PIV request by completing a certified, policy-protected PIV Request Form in PDF. The form is pre-populated with contact information extracted from back-end systems.
- Sponsor approves the PIV request by digitally signing the PIV Request Form.
- The PIV Request Form is protected by policies that restrict access to authorized individuals for confidentiality and privacy protection.
- Sponsor sends the PIV Request Form to the Registrar and Issuer.

A PIV request generation

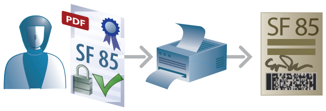
2. Registrar validates request



- Registrar receives the PIV Request Form, and Adobe LiveCycle automatically verifies its authenticity (i.e., the request is from an authorized Sponsor and the information it contains has not been modified).
- Registrar confirms the validity of the Applicant request and approves the request by digitally signing the PIV Request Form.
- A certified, policy-protected Standard Form 85 (SF 85) questionnaire is automatically generated by Adobe LiveCycle, auto-filled with Applicant contact information extracted from back-end systems and sent to the Applicant.

A PIV request generation

3. Applicant submits application



- Applicant fills out the electronic SF 85 using free Adobe Reader software, and the data is encoded in real-time into a 2D barcode on the form.
- Applicant prints the completed SF 85, with 2D barcode, signs with a wet-ink signature, and sends the paper form to the Registrar. The 2D barcode can subsequently be scanned to extract the data electronically.

B. PIV identity proofing and request approval:

Providing a secure and reliable process for automating identity proofing and document assembly

PIV issuance requires a reliable process for proving applicant identity, completing a background check, and capturing biometrics. Adobe streamlines and secures this process by automatically extracting data from back-end systems and generating custom documents from certified templates designed to meet the requirements of each step. Because Adobe automates the assembly of documents, forms, and even biometrics into a single PDF, the Registrar can reliably create and approve custom documents and then send them to the Signatory and Issuer for further processing.

B PIV identity proofing and request approval

4. Registrar validates identity and captures biometrics

SF 85
PDF
BIOMETRIC

- Registrar scans the 2D barcode on the Applicant's printed SF 85 to extract the data and transform it into a completed electronic SF 85 Form.
- Business rules in Adobe LiveCycle help the Registrar validate the consistency of information contained in the PIV Request Form and the SF 85 Form.
- Registrar captures the Applicant's photo, fingerprints, and other biometric data and attaches the biometrics as separate files inside a certified, policy-protected Biometric Form.

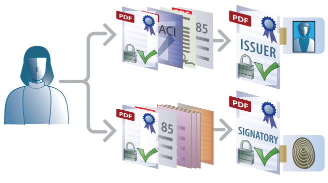
B PIV identity proofing and request approval

5. Registrar initiates NACI background check

- Adobe LiveCycle automatically auto-fills and assembles the required information from all forms, biometrics, and sources into a single, certified, policy-protected National Agency Check with Inquiries (NACI) background check request—NACI Request Form.
- The NACI Request Form is policy-protected, restricting its access to authorized NACI agents to protect the confidentiality and privacy of the Applicant.
- Registrar approves the NACI Request Form by digitally signing it.
- A NACI agent performs a background check, enters the results in the policy-protected NACI Request Form, digitally signs, and returns it to the Registrar.

B PIV identity proofing and request approval

6. Registrar approves PIV card issuance



- Registrar receives the results of the NACI background check. Adobe LiveCycle automatically verifies the NACI Request Form for authenticity, and generates a certified, policy-protected NACI Notice Form containing the results of the background check.
- Registrar digitally signs, thereby approving the NACI Notice Form, and sends it to the Sponsor and Issuer.
- Adobe LiveCycle automatically auto-fills and generates the following policy-protected document packages for the Registrar:
  - Issuer Document Package:
    1) Applicant's photo
    2) Results of NACI background check
    3) Additional Applicant information
  - Signatory Document Package:
    1) Applicant's biometric data
    2) Additional Applicant information
- Registrar approves the Issuer and Signatory Document Packages by digitally signing them.
- Registrar electronically archives all relevant information related to the Applicant's package.

PIV CARD ISSUANCE PROCESS:

B. PIV Identity proofing & request approval:

4. Registrar validates identity and captures biometrics

- Applicant appears in person to the Registrar and provides two identity source documents
- Registrar validates the documents as being authentic, scans to PDF, signs, and files the record
- Registrar captures an electronic facial image and all 10 fingerprints of the Applicant

5. Registrar initiates NACI background check

- Registrar initiates National Agency Check with Inquiries (NACI) on Applicant's behalf

6. Registrar approves PIV card issuance

- Registrar notifies the Sponsor and Issuer that the Applicant request has been approved and assembles the complete application history

C. PIV smart card issuance:

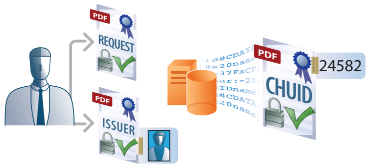
Utilizing persistent security to reliably exchange and verify credential elements

Creating authentic credential elements for smart card personalization and issuance is the final mission-critical step of the PIV process. Adobe LiveCycle software attaches the applicant's identity and credential elements—such as fingerprints or a photo—to a PDF.

Up to this point in the PIV process, Adobe LiveCycle software has enabled only authenticated individuals with policy-defined authorization rights to participate. In addition, it has verified all digital signatures to provide assurance of authenticity of every PDF document and its source. With this evidence that the information provided by the Sponsor, Applicant, and Registrar is reliable, the issuer can confidently proceed with personalizing and issuing the PIV card.

C PIV smart card issuance

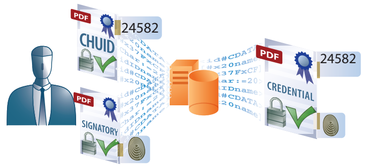
7. Issuer initiates PIV card personalization



- Issuer receives the Issuer Document Package from the Registrar. Adobe LiveCycle automatically verifies its authenticity.
- Issuer validates the request by comparing the information in the package against the PIV Request Form.
- Issuer creates the Applicant's unique identifier (CHUID). Adobe LiveCycle auto-generates and auto-fills a certified, policy-protected CHUID Form, and Issuer attaches the CHUID to the form.
- Issuer digitally signs the CHUID Form and sends it to the Signatory.

C PIV smart card issuance

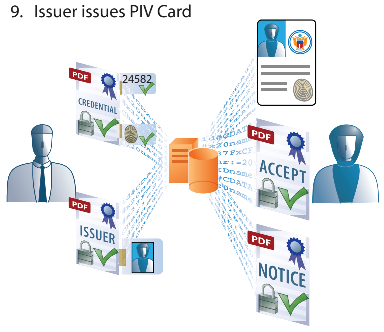
8. Signatory generates credential elements



- Adobe LiveCycle automatically verifies the authenticity of the CHUID Form received from the Issuer and the Signatory Document Package received from the Registrar.
- Signatory extracts the CHUID and biometrics from the two forms, and digitally signs them to create the credential elements.
- Adobe LiveCycle auto-generates a certified, policy-protected Credential Form.
- Signatory attaches the credential elements to the Credential Form, digitally signs, and sends it to the Issuer.

C PIV smart card issuance

9. Issuer issues PIV Card



- Adobe LiveCycle verifies the authenticity of the Credential Form received from the Signatory and the Issuer Document Package received from the Registrar.
- Issuer personalizes the PIV card with Applicant credentials and data that has been through this high-assurance proofing and issuance process.
- Adobe LiveCycle auto-generates a certified, policy-protected Acceptance Form that is auto-filled with the Issuer's and Applicant's information.
- The identity of the Applicant, who appears in person, is verified against authenticated information previously provided by the Registrar.
- Applicant digitally signs the Acceptance Form using the new PIV card.
- Issuer signs the Acceptance Form attesting to a complete and successful PIV card issuance to the Applicant.
- Adobe LiveCycle generates a certified, policy-protected Notice of Issuance Form that is auto-filled with required information. Issuer digitally signs and sends it to the Sponsor and Registrar.
- Applicant's Application Case History Document Package is generated by Adobe LiveCycle and archived for Registrar—package is complete with detailed audit trails that help demonstrate compliance with FIPS-201 requirements.

PIV CARD ISSUANCE PROCESS

C. PIV smart card issuance:

7. Issuer initiates PIV card personalization

- Issuer validates and verifies the Applicant request including the Registrar's approval notification
- Issuer creates a cardholder unique identifier (CHUID) for the Applicant and sends it to the Signatory

8. Signatory generates credential elements

- Signatory creates digitally signed credential elements (biometric and CHUID) needed for card personalization and sends them to the Issuer

9. Issuer personalizes and issues PIV card

- Issuer generates or Applicant provides a PIN for the PIV card
- Issuer uses the information provided by the Registrar and Signatory to complete the PIV card personalization
- Applicant appears in person before the Issuer, who verifies the Applicant's identity
- Applicant signs the PIV card terms of acceptance and receives card
- Issuer notifies the Sponsor and the Registrar that the process has been completed

Meet HSPD-12 and comply with FIPS 201 with Adobe enterprise solutions

Adobe enterprise solutions, including the Adobe LiveCycle server software, can help your agency reduce PIV card issuance time and costs, protect confidential information, and provide greater assurance of compliance with FIPS 201 so that your agency can meet HSPD-12 on time and within budget. Adobe LiveCycle provides fully integrated, interoperable, and automated high-assurance electronic processes through the use of intelligent documents and forms. These documents allow people to use certified templates containing embedded business rules that can validate data, extract, and/or update data from back-end systems. It dramatically speeds the PIV process by enabling participants to review, fill out, and digitally sign documents, add supplemental evidentiary documentation, and submit documents electronically.

With its intelligent electronic workflow, digital signature support, and persistent document control and security, Adobe improves security of all the requests, data, approvals, and exchange steps required for card personalization.

The benefits of Adobe solutions don't stop with HPSD-12, though. In addition to helping agencies meet the immediate deadline for issuing PIV cards, companies can realize the benefits of the Adobe solution for automating other mission-critical processes in the future.

To learn more about how Adobe can automate and better protect your identity proofing and registration process for HSPD-12, visit *www.adobe.com/government*.

To contact Adobe customer service for more information, call 1-800-861-9428.

Better by Adobe.™

Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
www.adobe.com

Adobe