



GSA HSPD-12 Registrar Quick Reference Guide

Version 2.2

November 26, 2008

CM# GSA-DI-00000306-2.2.0



This page intentionally left blank.

Table of Contents

The Enrollment Workstation	1
Credentialing Center Operations.....	3
Site-specific Orientation	3
USAccess Help Desk	3
Attendance.....	4
Daily Setup	5
Handling PIV Credentials	6
Damaged and Defective PIV Credentials	6
Expired Credentials	6
Appointment Management Procedures.....	7
Viewing Daily Appointments.....	9
Checking Appointments In and Out.....	10
Cancelling Appointments	11
Registrar Communication Applications.....	12
TeamRegistrar Web Site.....	12
AI Notify	15
Applicant Enrollment Procedures	20
Log in to Assured Identity™	21
Search for Applicant’s Record.....	24
Capture Biographic Information.....	25
Scan Identity Documents	29
Capture a Photo	33
Capture Fingerprints	37
Rolled Fingerprints	37
Slap Fingerprints.....	39
Primary and Secondary Fingerprints.....	41
Complete the Enrollment Process	42
Exceptions	44
Failure to Scan Exceptions.....	44
Manual Photo Optimization	46

Fingerprint Capture Exceptions.....	49
Amputee	49
No Fingerprints Captured.....	54
Fingers with Long Fingernails	56
Activation Procedures	58
Introduction	58
Attended PIV Credential Activation with Fingerprints.....	59
Attended PIV Credential Activation without Fingerprints ..	73
What if card activation fails?	74
Appendix A - Enrollment Process Flow.....	75
Appendix B - Terms and Acronyms	77
Appendix C - Definitions	79
Appendix D - Homeland Security Presidential Directive 12	81

Registrar Job Aid List

This guide contains references to the following Registrar Job Aids:

- Enrollment Procedures
- Examples of Source Identity Documents
- Acceptable Forms of Identification
- Fingerprinting Guide
- Registrar Daily Checklist
- Unattended Activation Guide
- Attended Activation Guide
- Identity Documents Mismatch

This page intentionally left blank.

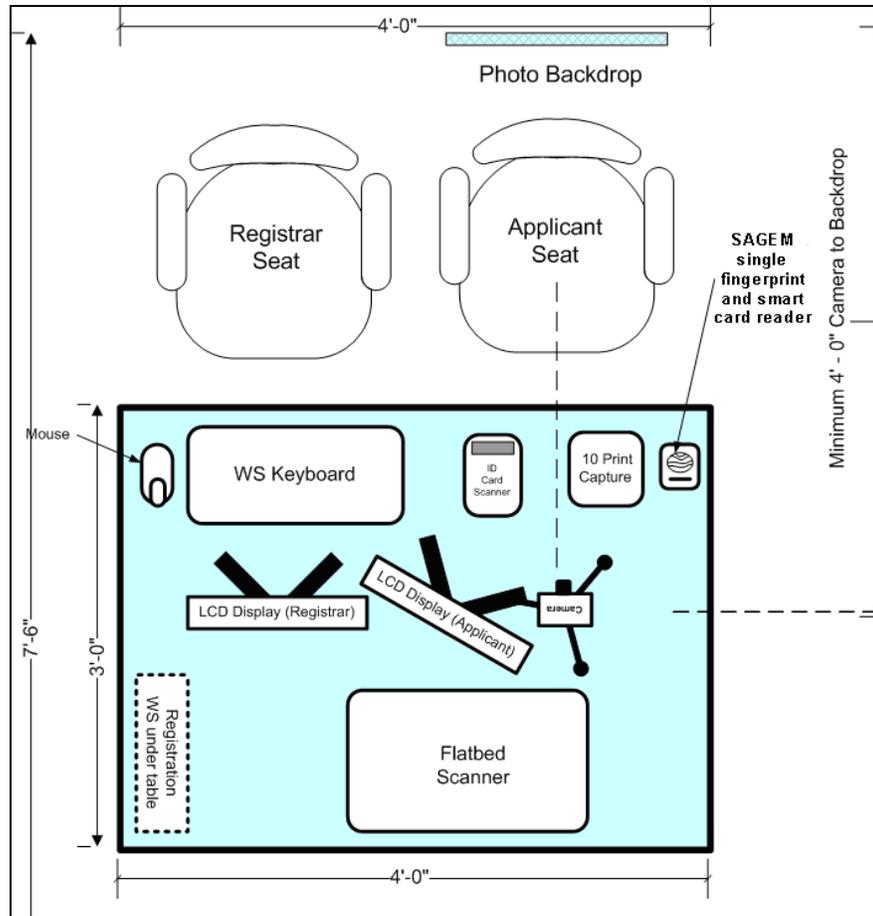
The Enrollment Workstation

Registrars and Applicants meet at HSPD-12 Credentialing Centers to complete the enrollment process. Using the USAccess Credentialing Center devices and software, the registrar obtains the Applicant's biographic and biometric data, and scans the source identity documents.

USAccess Credentialing Centers may be configured as stationary (fixed) or mobile stations. Stationary Credentialing Centers consist of these elements:

- Enrollment workstation with keyboard and mouse
- 2 LCD displays
- Flatbed scanner
- AssureTec ID card scanner
- 10-print fingerprint capture device
- SAGEM fingerprint and card reader
- Digital camera
- Photo backdrop (blue screen)
- Worktable
- 2 chairs

The following schematic illustrates the minimum footprint at a USAccess Credentialing Center.



USAccess Program Credentialing Center

Notice that separate LCD displays are provided for the Registrar and the Applicant. There are two times during the process when the Registrar allows information to be displayed on the Applicant's monitor:

- When the Applicant verifies personal information
- During fingerprinting

Credentialing Center Operations

In your role as Registrar, you will be responsible for many of the daily procedures that contribute to the management of your Credentialing Center. Each Agency and site will have its own policies. You will learn about the unique aspects of your center and responsibilities there prior to reporting for duty.

Site-specific Orientation

EDS will collect specific site information and make it available to you and your supervisor so that you will know where to report, where to park, and the name of your point of contact (POC). Your supervisor will also define the:

- Hours of operation
- Methods for documenting your time (time cards)
- Policies regarding breaks, lunch, etc.
- Center points of contact (POCs)
- Policies for handling PIV Credentials
- Referral telephone numbers

If you have any questions, be sure to contact your supervisor for clarification. It is your responsibility to ask for more clarification when needed.

USAccess Help Desk

EDS provides the following Help Desk services for the USAccess Program:

- A Help Desk is staffed onsite at its Montgomery, Alabama, facility with hours of operation from 6:00 a.m. – 6:00 p.m. Central Time and 7:00 a.m. – 7:00 p.m. Eastern Time, Monday through Friday, excluding federal holidays. Calls outside of these normal business hours will be routed to a mobile on-call help desk analyst and answered on a first come, first served basis. If all analysts are busy, callers are given the option of leaving voicemail messages that will be responded to in a timely manner. All calls are documented and data is captured regarding the caller, purpose of call, actions taken, and resolution.

- An Automated Call Distribution (ACD) system is available to receive, process, log, and handle all calls that are routed to the system from the USAccess Program toll-free telephone number. Ongoing support of the ACD includes maintaining the ability to separately identify/handle USAccess Program calls so that callers receive customized responses when calling the Help Desk. In addition, ACD messages will be updated and maintained as required to ensure appropriate handling of the USAccess Program Help Desk callers to provide improved customer service and response to these callers.
- The Help Desk will respond to e-mail inquiries. All e-mail inquiries will be logged as an incident and responded to within two business days. E-mail the Help Desk at usaccess.helpdesk@eds.com.

There is a learning curve to becoming a proficient Registrar. The Help Desk is a resource to guide you when you need help or have questions.

Attendance

Registrars have the responsibility to ensure that the Credentialing Center is open and ready to receive applications during the hours of operation. This means that you will arrive approximately 15 minutes before the stated opening time so that you have time to open the Center and check that all of the systems are functional using the Registrar's Daily Checklist.

If you are unable to come to work because you are sick, you must call your supervisor as far ahead as possible so that alternate arrangements can be made. Your supervisor may have the ability to arrange for a replacement Registrar to cover for you and will need some time to make the necessary arrangements.

If your supervisor is unable to arrange for another Registrar to take your place, he or she will call the Help Desk and ask them to cancel scheduled appointments in the GSA Online Scheduling System. Once appointments are cancelled, applicants will receive an e-mail advising them of the cancellation and requesting that they reschedule an appointment using the GSA Online Scheduling System.

Every attempt will be made to add an alert regarding the cancellation to the USAccess Program Website explaining the need for the cancellation of appointments at a particular site.

Daily Setup

When you arrive, unlock the Credentialing Center door and perform the activities necessary to set up the center. These activities will include:

- Ensure that Welcome signage and any explanatory handouts are in place. Since there is no designated person to greet Applicants, the signage and handouts play a vital role in alerting the Applicants to center operations.
- Follow the steps in the Registrar's Daily Checklist to set up the enrollment station and perform the equipment/application daily test.
- Check the lighting to make sure that the room lights are working properly and close/open the window blinds as appropriate. The digital camera is set to function properly without flash in lighting conditions that are normally found in an office environment.
- Ensure camera and chair are in proper places. The camera and Applicants chair will not be stationary and may be inadvertently moved during the day. However, tape lines may be in place to indicate where the camera and chair must reside in order to capture an acceptable photo.

At the end of the day, you must:

- Log off the Assured Identity Application
- Cancel all no-shows in the GSA Online Scheduling System
- Close the GSA Scheduling System.
- Close all open Windows on the Enrollment and Activation workstations.
- Press Ctrl+Alt+Del and click the **Lock Computer** button on the pop-up window.
- Do NOT log off the workstation or turn off the workstation.

The workstation needs to be on and logged in for remote maintenance to occur during evenings and weekends.

- Lock the door when you leave

Handling PIV Credentials

PIV Credential handling is site and agency-specific. There are several situations in which you may be asked to handle PIV Credentials. These include:

- Receiving the credential from the shipper and storing before activation
- Handing out credentials for activation
- Collecting damaged or defective credentials

Again, procedures for receiving and storing credentials and handing them out for activation are site specific. You will be provided with proper procedures should you need to perform these tasks.

Damaged and Defective PIV Credentials

PIV Credentials may be damaged during the activation process or arrive defective from the manufacturer. It may be impossible to determine if a credential's failure to activate is due to damage or defectiveness. Defective credentials will be replaced by the manufacturer without cost to the USAccess Program.

In this situation, call the USAccess Help Desk and follow the directions given to you. Explain to the Applicant that they will receive a new PIV Credential and email will be sent to them when the credential is ready for pick-up.

Expired Credentials

Registrars are not responsible for collecting old PIV Credentials. If you are asked to accept a credential, tell the Applicant to return it to their Agency Security Officer.

Appointment Management Procedures

Appointments in the GSA Online Scheduling System are scheduled every 15 minutes for a specific enrollment workstation. Applicants are asked to arrive early for their appointments and set aside an adequate amount of time in their personal schedule for their enrollment (approximately 45 minutes). Use your own judgment and flexibility when working with people who arrive late and attempt to fit them in if possible. You may need to take people out of turn.

If there are multiple workstations in your center, it may also be possible to use a different workstation for enrollment after checking the Applicant into the GSA Online Scheduling System.

GSA's Online Scheduling System is a Web portal that serves as an appointment book, allowing Registrars to manage appointments scheduled online by Applicants. These tasks include:

- Checking appointments in and out
- Cancelling appointments

Your workstation desktop will have a shortcut to GSA Online Scheduling System, also known as TimeTrade.



Desktop Shortcut to GSA Online Scheduling System

You will be given a Username and Password to log in to the GSA Online Scheduling System. Follow these steps to log in:

1. Log in to the USAccess System.
2. Double click the TimeTrade shortcut on your desktop.
3. Or, launch your Internet Explorer browser and, from the Favorites folder, select the **GSA Online Scheduling System** link.

*The **GSA Online Scheduling System Login** screen displays in your browser.*

GSA Online Scheduling System Login Screen

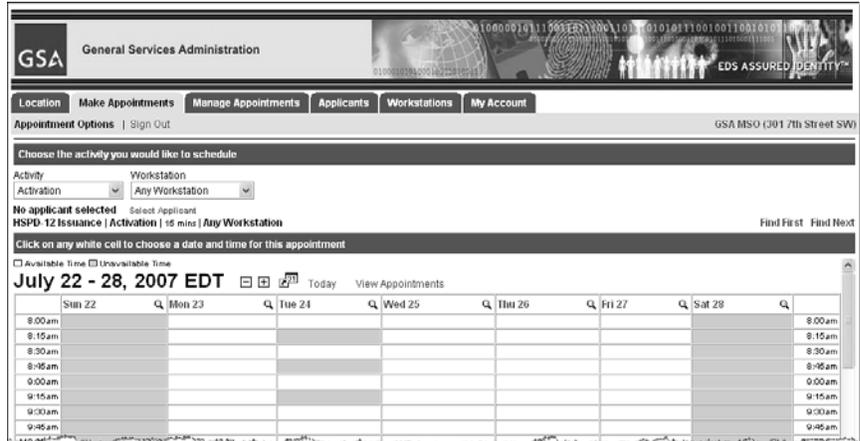
4. Type your username in the **Username** field.
5. Type your password in the **Password** field.
6. Click the **Sign In** link.

*The **Choose a Location** screen displays.*

Choose a Location Screen

7. Choose your state from the **Location Group** dropdown list.
8. Choose your location from the **Location** dropdown list.
9. Click the **Next** button.

*The **Make Appointments – Appointment Options** screen displays.*

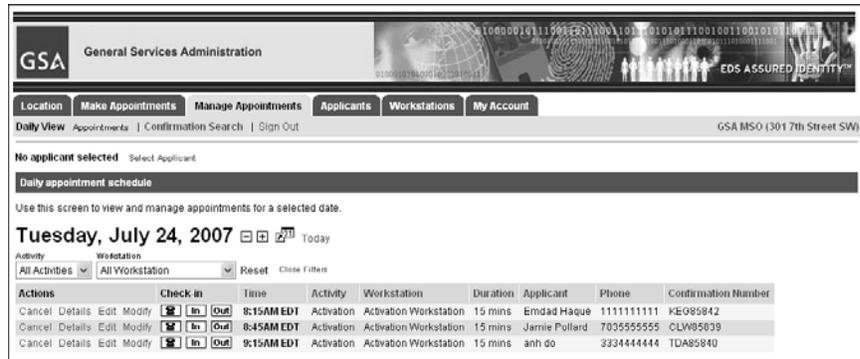


Make Appointments – Appointment Options Screen

Viewing Daily Appointments

To view the daily appointments for your chosen location, click the **Manage Appointments** tab.

*The **Manage Appointments–Daily Appointment Schedule** screen displays.*



Manage Appointments – Daily Appointment Schedule Screen

The **Daily Appointment Schedule** screen provides a daily view of all appointments scheduled for the current day. Appointments listed can be filtered by activity or workstation.

Checking Appointments In and Out

Canceling Appointments

Wait until the end of the day to cancel scheduled appointments for Applicants that did not show up. Missed appointments will be the ones remaining at the end of the day in the GSA Online Scheduling System, and you should cancel them all at once.

Metrics

Metrics are collected from the GSA Online Scheduling System to determine the efficiency of the enrollment process. The ideal enrollment appointment should take approximately 15 minutes; however, this is an average. There are situations in which Applicants will need additional time because they are experiencing difficulties with fingerprint capture or have questions.

Be sure to answer an Applicant's questions, even if it takes extra time. Your goal is to complete the enrollment within 15 minutes, but customer service is a priority. Remain aware that this is an aggressive schedule, and you will need to keep up.

In order to collect the metrics, Applicants need to be checked in to the system when they arrive for their appointment, and checked out of the system when their appointment is complete.

Follow these steps to check an Applicant in and out of the system:

10. Click the **In** button that corresponds to the Applicant's appointment on the **Manage Appointments–Daily Appointment Schedule** screen.

*The **In** button turns green.*

When the Applicant's appointment is finished:

11. Click the **Out** button that corresponds to the Applicant's appointment on the **Manage Appointments–Daily Appointment Schedule** screen.

*The **Out** button turns green.*

The Applicant has now been checked in and out of the system.



Hint

If you check in the wrong Applicant, simply click the green **In** or **Out** box to change it back to white. Then click the boxes for the correct Applicant.

Cancelling Appointments

When Applicants fail to appear or cannot be registered once they have arrived, their appointment must be cancelled in the system. When you cancel an appointment, an e-mail is sent to the Applicant asking them to re-schedule the appointment.

Wait until the end of the day to cancel scheduled appointments for Applicants who did not show up.

Follow these steps to cancel an Applicant's appointment:

1. Click the **Cancel** link that corresponds to the Applicant's appointment on the **Manage Appointments-Daily Appointment Schedule** screen.

*A **Cancellation** dialog box appears, asking you to confirm the cancellation.*



Cancellation Dialog Box

2. Click the **OK** button to confirm the cancellation. The appointment has been cancelled and an e-mail sent to the Applicant that they must reschedule.

Registrar Communication Applications

Registrars do not have access to the Internet or e-mail applications at the Enrollment or Activation Stations. To facilitate communication between the support staff and the Registrars, two applications have been made available. Registrars can get program and status updates, system enhancement announcements, and network outage notifications using these tools.

TeamRegistrar Web Site

TeamRegistrar is a Web site accessible to Registrars on the Enrollment Stations. It contains Critical Updates, Reminders, Job Aids and Tips, Frequently Asked Questions, and a Contact Us feature.



TeamRegistrar Icon

The **Home Page** has critical updates, reminders and a tip of the day. Critical updates are new information Registrars need to be aware of immediately. Check the Web site in the morning and as needed during the day. **Tips of the day** will rotate so there will always be something new. **Reminders** are reminders of upcoming training events, impending changes to the system, new policies, etc.



TeamRegistrar Home Page

The **Critical Updates** page contains two types of updates and the icons that indicate them. Updates can be:

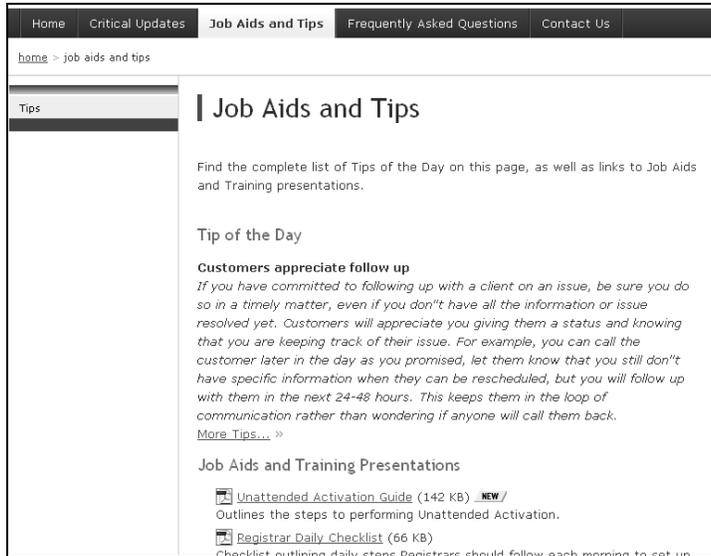
- **Information Only** indicated by the  icon
- **Action Required** indicated by the  icon

Search for previous updates using the drop-down lists. Registrars can search by type of update, the system update references, or the date of the update. Training presentations are available as attachments to the critical updates.



Critical Updates Page

The **Job Aids and Tips** page contains training documents and job aids located under the Job Aids and Tips tab. Registrars cannot print these docs from the Enrollment Stations, but you can pull them up and read them. Your POC can access updated materials and job aids at the Agency Lead Portal through the USAccess Web site, www.fedidcard.gov. Detailed instructions for POC access is available on the Participating Agency Tools page of the USAccess Web site, www.fedidcard.gov/tools.aspx.



Job Aids and Tips Page

The **Frequently Asked Questions** page is constantly updated with questions and comments from the field. When Registrars have time between appointments, they can look for new questions and answers on this page. Before you call the Help Desk or send a question in via the Contact Us form, please check the FAQs to see if your question has been answered.



Frequently Asked Questions Page

Finally, the **Contact Us** form is for Registrars with questions, suggestions, or comments. You can enter the information requested, choose a topic from the **Select Nature of Request** drop-down box, and click **Submit**. The support staff will try to

answer these messages within 24 hours. This is NOT A REPLACEMENT FOR THE HELP DESK. The Contact Us feature can be used if Registrars have an issue that is not resolved by FAQs, Help Desk, policy questions, or just questions about the program.

Contact Us Page

AI Notify

AI Notify is a tool that allows Registrars to be alerted to changes in the system or critical updates posted on TeamRegistrar through an icon on the Enrollment Station and Activation Station system trays.



System Tray with AI Notify Icon

The icon is a green square with the letter S. This icon remains green in the system tray until an alert is posted by Tier 3, a critical update is posted to TeamRegistrar, or a network outage occurs.

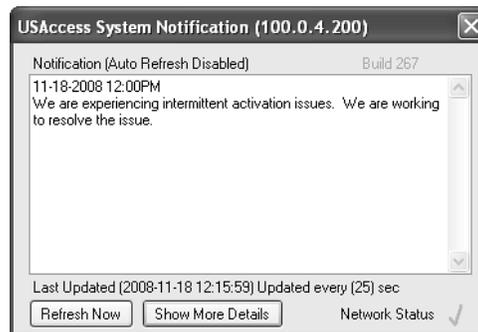


AI Notify Symbols

System Alert



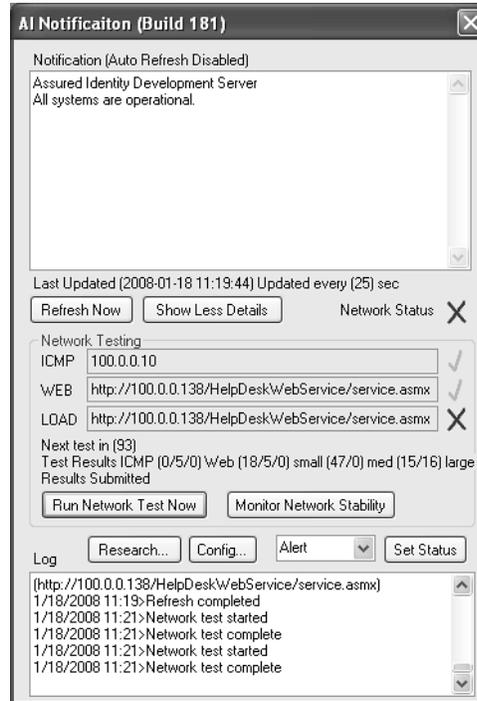
If a system alert is posted by Tier 3, the icon flashes yellow and red. Right click or double click the flashing icon to read the alert. If you right click on the icon to open the alert, select **Open** from the list displayed.



System Alert Message Window

There are three things to notice at the bottom of the screen:

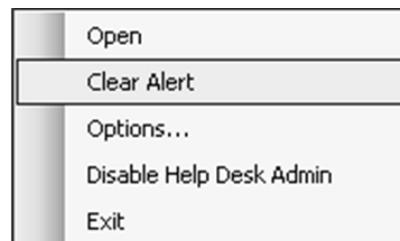
1. Click the **Refresh Now** button to refresh the message window if you have left the window open and you think there may be another alert posted. If a new message was posted while the window was open, clicking **Refresh Now** displays the new message.
2. The **Show More Details** button expands the alert message window to display some diagnostic tools. Tier 3 may ask you to use these tools to help them diagnose problems with the system. These tools are of no use to you without Tier 3. Do not expand the window and attempt to use the tools on your own. You won't hurt anything, but you won't accomplish anything either. Wait for Tier 3 instructions.



Expanded System Alert Message Window

- The **Network Status** indicator is currently disabled. When it is turned on you will see a Network Status indicator when you open the alert message window.

When you have finished reading the alert, close the alert window. To clear an alert, right click the icon on the system tray and select **Clear Alert**.



System Alert Options

Critical Update



If a critical update is posted to TeamRegistrar, the icon flashes between the usual letter **S** and the red and white **R** for TeamRegistrar.

If you double click the icon, a message alert window displays with a button to launch Team Registrar.



TeamRegistrar Message Alert Window

Network Issues



When there are network issues, a red lightning bolt flashes. When you see this icon, check all network connections and make sure they are plugged in correctly. If you are still experiencing the flashing lightning bolt, call the Help Desk to report the issue.

This page intentionally left blank.

Applicant Enrollment Procedures

The following table lists the tasks the Registrar performs during the enrollment process on the workstation using the Assured Identity™ application. The same tasks are shown in the Enrollment Procedures job aid. This list may be kept near the Enrollment Station to guide you through the enrollment procedure.

Enrollment Tasks Performed by Registrar

Enrollment Tasks
1. Greet and welcome the Applicant.
2. Ensure the Applicant has the appropriate source identity documentation.
3. Check-in the Applicant using GSA Scheduler on the Manage Appointments page.
4. Open the Assured Identity application; search for Applicant record.
5. Scan the driver's license in the AssureTec scanner. (If you receive an error message, click OK , cancel the Data Difference Report, and rescan the license up to three more times.)
6. Review the Data Difference Report.
7. Ask the Applicant if the biographical data entered by the Sponsor is correct.
8. Complete the remaining fields on the Biographic Data page and ensure all data are correct. Click Next .
9. If license fails the scan, clear it and rescan up to 10 times. If failed, check More Validation Required box and enter this comment: <i>[State] license failed to scan after multiple attempts</i> (add observations to end of statement, e.g., peeling laminate, bent license, etc.)
10. Scan the remaining source identity documents using the flatbed scanner.
11. Capture the Applicant's photo.
12. Capture rolled fingerprints.
13. Capture slap fingerprints.
14. Verify the Applicant's primary and secondary fingerprints.
15. On the Enrollment Status page, verify Registered status.
16. Save the Applicant's record.
17. Enter your PIN to digitally sign the enrollment record.
18. Check out Applicant on GSA Scheduler.
19. Return all identity documents to the Applicant.

Your workstation desktop will have a shortcut to the EDS Assured Identity™ Enrollment Application. This is the software application that guides you through enrollment and collects the Applicant's data.



EDS Assured Identity™ Shortcut

You will be given a Password to log in to the system.

Log in to Assured Identity™

Follow these steps to access the Assured Identity™ Enrollment application:

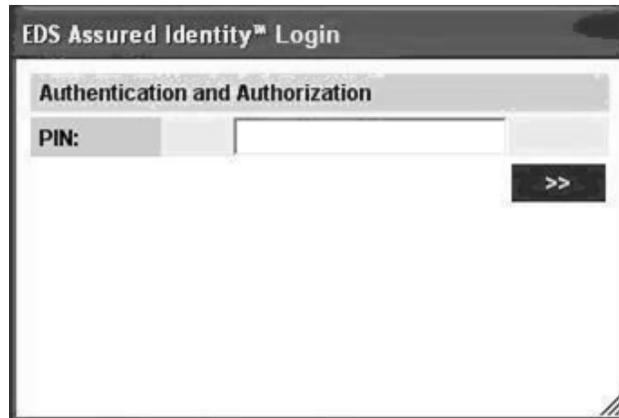
1. Insert your PIV Credential into the card reader.
2. Double click the EDS Assured Identity™ shortcut on your desktop.

*The **Welcome** screen displays in your browser.*



Welcome Screen

*The **Authentication and Authorization** window displays.*



Authentication and Authorization Window

3. Enter your **PIN** and press **Enter** or click the **>>** button.

This initiates the Registrar's authentication process.



Watch Out!

The system only allows six attempts to enter the correct PIN. With each incorrect entry, the system displays the message **Incorrect PIN. Attempts remaining: [5]**. Once the six attempts are exhausted, the Registrar's PIV credential is locked.

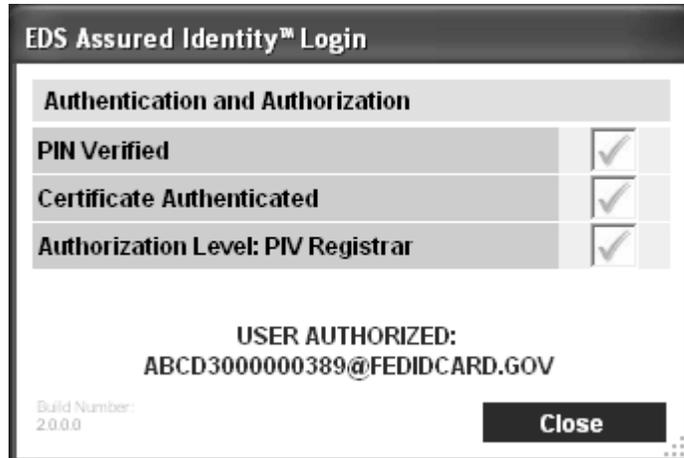


Key Point

Do not remove your credential from the card reader during enrollment. The system will cancel the enrollment and close the Assured Identity application.

Once the correct PIN is entered, the **Authentication and Authorization** window expands to display the following messages:

- PIN Verified
- Certificate Authenticated
- Authorization Level: PIV Registrar



Successful Authentication and Authorization Window

If a green ✓ mark is displayed to the right of each level of authentication, it indicates your login has been authorized.

4. Click the **Close** button.

*The **Enrollee Search** screen displays.*



Enrollee Search Screen



Watch Out!

Note that there are no partial saves in the enrollment procedures. To save all data and images entered, you must complete the entire enrollment process.

If you try to exit before completing the enrollment process, a pop-up message will display asking, **Are you sure you want to exit record without saving? Yes/No**. These are your options:

- Clicking **Yes** will close the record and lose all data entered.
- Clicking **No** returns the Registrar to the current screen to continue the enrollment process.

Search for Applicant's Record

The **Enrollee Search** screen is used to search for an Applicant's record.

To search for an Applicant, do the following:

1. Enter the Applicant's last name or Social Security Number, and date of birth in the search fields:
 - Last Name/SSN
 - Birth Date
2. Click the **Search** button.

*The search results display in the **Results** section.*

Enrollee Search							
First Name				Agency			
Last Name	DOE			Sub-agency			
Employee ID				Enrollee ID	3000002861		
Social Security Number	Birth Date	01/01/1950		Data Source	<input type="radio"/> Pre-Enrollment <input checked="" type="radio"/> IDMS		
Update Enrollee				Clear		Search	
Results							
Enrollee ID	Last Name	First Name	Middle Name	Employee ID	Sub-org	Status	Expire Date
3000002861	DOE	JOHN	EDWARD			NEW	

Enrollee Search Results

Notice that the Applicant's Status is indicated as **NEW**.

3. Click **Update Enrollee**.

*The **Biographic Information** page displays.*

Capture Biographic Information

The **Biographic Data** screen contains all information that was previously entered by the Sponsor. Notice that some of the fields cannot be edited. If the information in these fields is incorrect, the Applicant must return to their Sponsor to have any errors corrected.

1. From the **Enrollee Search** screen, select the Applicant from the list and click the **Update Enrollee** button.

The **Biographic Data** screen displays.

Biographic Data Screen

Turn on the Applicant's LCD Monitor at this point or drag your screen onto the Applicant's monitor so that he or she can view the Biographic Data screen. Ask the Applicant to verify that their information is correct.

If it is not correct, explain that only the Sponsor can update the data fields and the Applicant will not be able to complete the enrollment until the Sponsor corrects the biographic data. Use language similar to this:

"We will not be able to continue your enrollment at this time because the information your Sponsor has entered is either inaccurate or does not match your source identity documents.

As you can see, the required fields are inactive and the system does not allow me to update your information. Only your Sponsor can make the changes that are required. The system is set up this way because HSPD-12

makes sure that there is a separation of duties between the person enrolling you and the person sponsoring your credential.

It is up to you to contact your Sponsor and request that your information be corrected or updated. When your Sponsor makes these changes, you will receive an e-mail with instructions to reschedule your enrollment appointment. Do you have any questions about how to contact your Sponsor”?

Follow this procedure to scan and authenticate drivers' licenses with the AssureTec scanner. If a driver's license is not included as an identity document, complete the biographic data screen and click the **Next** button to move to the documents page. Scan identity documents using the HP Flatbed scanner (Step 9 below).

2. Insert the Applicant's driver's license into the AssureTec card scanner.

*The **Data Difference Report** window displays.*

Data Difference Report Window

The **Data Difference Report** compares data entered by the Sponsor (Sponsored Applicant Name Data) with data scanned from the license (Scanned Name Data).

All fields are required except Suffix, and all required fields must have data. Check boxes indicate data fields that will be used to populate the Applicant's record.



Watch Out!

Scan only state Driver's Licenses in the AssureTec scanner. The scanner will not validate other forms of ID.



Key Point

When you see the **Document Failed Validation** message after scanning the drivers license, the right side of the Data Difference Report will most likely display with blank fields and the license has failed the scan.



3. Click **OK**.
4. On the Data Difference Report, click **Cancel**. Rescan the license up to three times. If the license continues to fail the scan, cancel the Data Difference Report and complete the fields marked with an asterisk.
5. Compare all the data fields to ensure the data matches.
6. If any of the data fields differ, click the check box next to the correct data field to select the appropriate information to save to the Applicant's file.
7. Utilize the dropdown lists to fill in editable, blank fields with any missing data.
8. When you have finished comparing and editing fields, click the OK button.

*The **Biographic Data** screen displays, showing the Applicant's updated data.*

Biographic Data Screen

9. Complete all fields marked with an asterisk. The system will not allow you to move to the next page until all fields marked with an asterisk have been completed.
10. Enter aliases the applicant may have. Ask the applicant if there are other names they have legally used or been known by. Enter any aliases in the Alias Information box. Do not include nicknames.
11. Click the **Next** button.

*The **Document Collection** screen displays.*

Document Collection Screen – Document 1

Notice that the Applicant's driver's license appears in the **Document 1 Image** section and the corresponding data is entered into the **Document 1 Information** fields.

The AssureTec scanner will let you know if a license needs more verification by setting a **FAILED** message, instead of **PASSED**, below the Document 1 image.

If the license fails the scan, scan up to 10 more times to try to receive a **PASSED** message. If the license continues to show the **FAILED** message below the picture, and the license looks valid, enter the required information into the fields below the license and continue scanning the remaining documents. If you believe the license to be fraudulent in any way, check the **More Validation Required** checkbox and enter your observations in the **Comments** box.



Hint

See Failed to Scan under the Exceptions section in this Guide for additional steps to take if you receive a **FAILED** message.

Scan Identity Documents

There are two objectives to successfully completing the document collection portion of the enrollment process:

- Capture at least two documents in the system.
- The system must identify the documents as either "PASSED" or "Not Authenticated."

PASSED – Driver's licenses are scanned and authenticated using the AssureTec scanner.

Not Authenticated – Documents scanned using a flatbed scanner are unable to be authenticated (e.g., birth certificate, passport, etc.)

Linking Documents

Although the Applicant is required to provide two identity documents, the document collection screen can display up to three documents, accommodating a linking document if necessary.

When a linking document is presented, you must scan the document in the **Document 3 Image** section.

Linking documents are required when documents with different names are offered as primary and secondary source identity documentation.



Key Point

The only time identity source documents with different names can be accepted is when an official linking document such as a marriage certificate, certified copy of birth certificate, or court record can be provided linking the two names.

The linking document must have both the former and current legal names on it and both the primary and secondary documents must be valid and not expired.

For example, a married woman may use both a current driver's license, with her married name, and a certified copy of her birth certificate, with her maiden name, as primary and secondary sources of identification as long as she brings a linking document, her marriage license, with both her maiden name and married name on it.

12. Click the **Scan** button under the **Document 2 Information** section.

*The **Select Device** dialog box displays.*

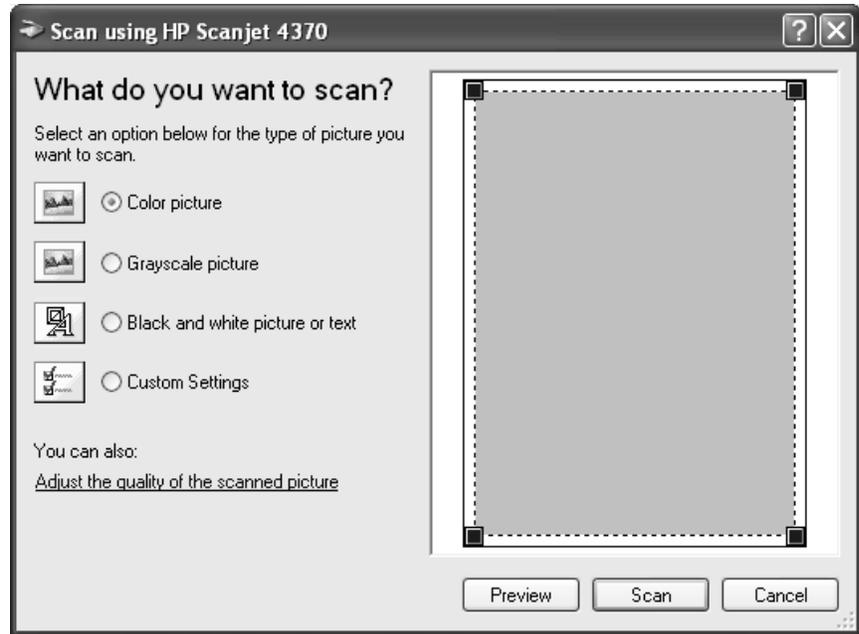


Select Device Dialog Box

Follow these steps to begin scanning identity documents:

13. From the **Select Device** dialog box, select the **HP Scanjet**.
14. Place the identity document to be scanned face down on the HP Scanjet scanner bed.
15. Click the **OK** button.

*The **Scanner Control and Preview** dialog box displays.*



Scanner Control and Preview Dialog Box

16. In the **Image Scanning** window, select an option for the type of picture you want to scan (Color picture, Grayscale picture, Black and white picture or text, or Custom Settings).

If you are scanning a paper document with a raised seal, such as a birth certificate, select **Grayscale**. Otherwise, leave the default set to **Color picture**.

17. Click the **Preview** button.

The scanned image displays in the preview window.

18. Crop the image if necessary to remove excess spacing around image.
19. If the image is upside-down or if there is a problem with the image, adjust the document on the scanner and click the **Preview** button again.
20. If the image quality is acceptable, click the **Scan** button.

*The **Document Collection** screen displays.*

Notice that the Applicant's document appears in the **Document 2 Image** section.

Click  in the lower right corner of the Document Image section for an expanded view of the image; click **X** to close window.

21. Enter data in the **Document 2 Information** fields using the dropdown lists.

The required Document Information fields for each identity document are:

- Title
- Number



Hint

Click the **Clear** button to remove a Document Image and the Document Information below it.

The screenshot shows a web interface for document collection. At the top, it says 'GSA General Services Administration' and 'EOS ASSURED IDENTITY'. Below this are three document slots:

- Document 1 Image:** Shows a 'DEMO DRIVER LICENSE' for JOHN EDWARD JR. DOE. The status is 'PASSED'.
- Document 2 Image:** Shows a 'BIRTH CERTIFICATE' for JOHN EDWARD JR. DOE. The status is 'Not Authenticated'.
- Document 3 Image:** Shows a blank document. The status is 'Not Authenticated'.

Below each image are 'Document Information' fields:

Document 1 Information	Document 2 Information	Document 3 Information
Title: DRIVERS LICENSE	Title: BIRTH CERTIFICATE	Title: [Empty]
Issuing Authority: UNITED STATES	Issuing Authority: UNITED STATES	Issuing Authority: [Empty]
State/Province: ALASKA	State/Province: ALASKA	State/Province: [Empty]
Number: B86540	Number: B12345	Number: [Empty]
Expiration Date: 09/21/2010	Expiration Date: [Empty]	Expiration Date: [Empty]
<input type="checkbox"/> More Validation Required	<input type="checkbox"/> More Validation Required	<input type="checkbox"/> More Validation Required
Buttons: Scan, Clear	Buttons: Scan, Clear	Buttons: Scan, Clear

At the bottom, there is an 'Additional Comments' field and navigation buttons: Cancel, < Previous, Next >.

Completed Document Collection Screen

22. After all identity documents are scanned, click the **Next** button to proceed to the next screen.

*The **Photo Capture** screen displays.*



Hint

If any required fields on the **Document Collection** screen are missing data, the system will prompt you to enter the data before you can move on to the next task.



Photo Capture Screen

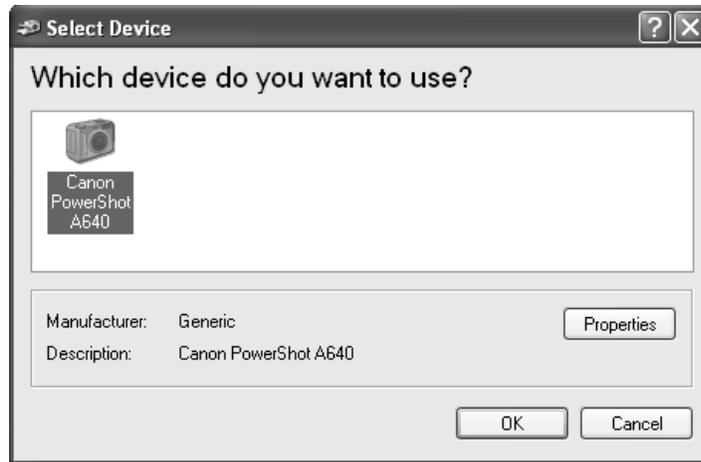
Capture a Photo

Your subject should be sitting in front of a blue screen for their photo. They should be sitting up straight and looking straight at the camera while you take the photo. The subject can have a neutral expression or smile, provided no teeth are visible. No part of the face should be hidden or otherwise obscured by hair or any type of head covering. You may need to raise or lower the camera tripod if your subject is either very tall or very small in stature.

To capture a photo image of the Applicant, do the following:

1. Position the Applicant in front of the camera. Tell the Applicant to have a plain expression for the photo.
2. Click the **Capture** button.

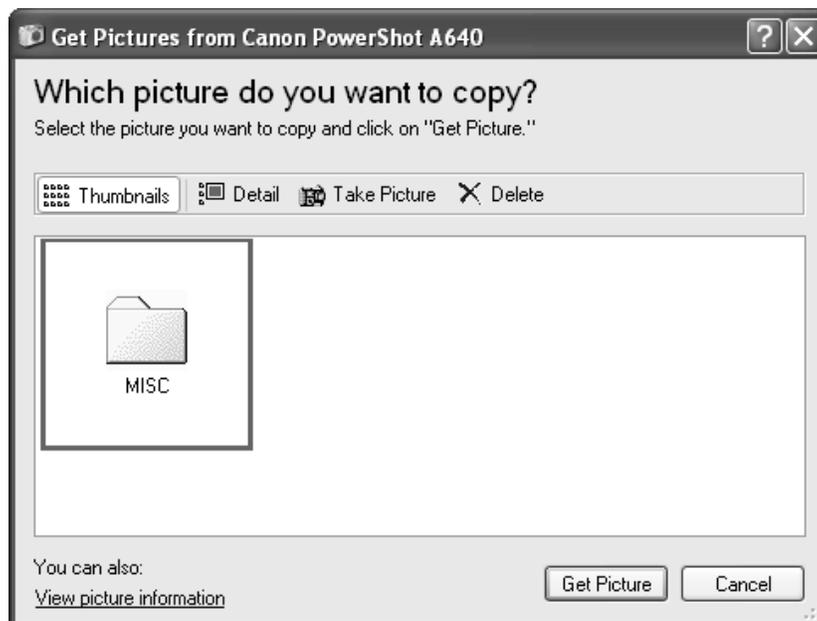
*The **Select Device** dialog box displays.*



Select Device Dialog Box

3. Select the camera from the list of available devices and click the **OK** button.

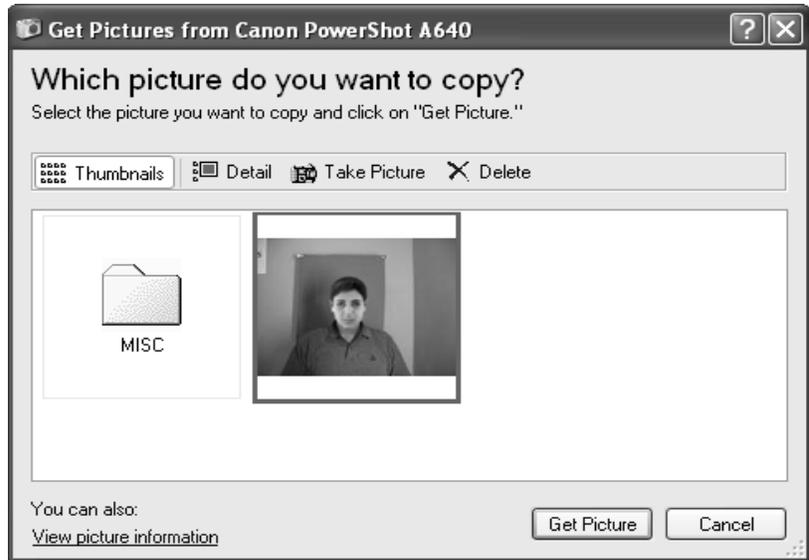
*The **Get Pictures** dialog box displays.*



Get Pictures Dialog Box

4. Click the **Take Picture** button on the toolbar.

The captured image displays on the screen.



Captured Photo Image

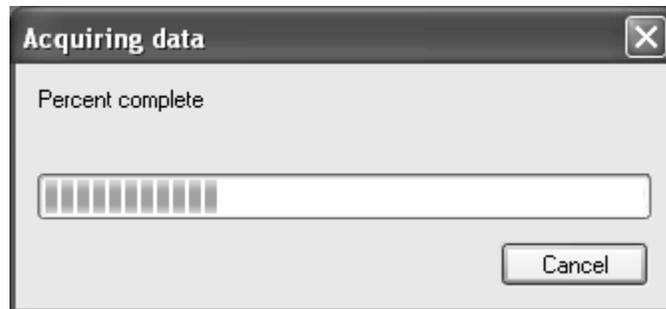


Hint

You may need to take more than one picture. Take additional pictures by clicking the **Take Picture** button again. You will be able to select the best of those taken.

5. Click on the desired photo and then click the **Get Picture** button.

*The **Acquiring data** window displays while the image transfers to the application.*



Acquiring Data Window

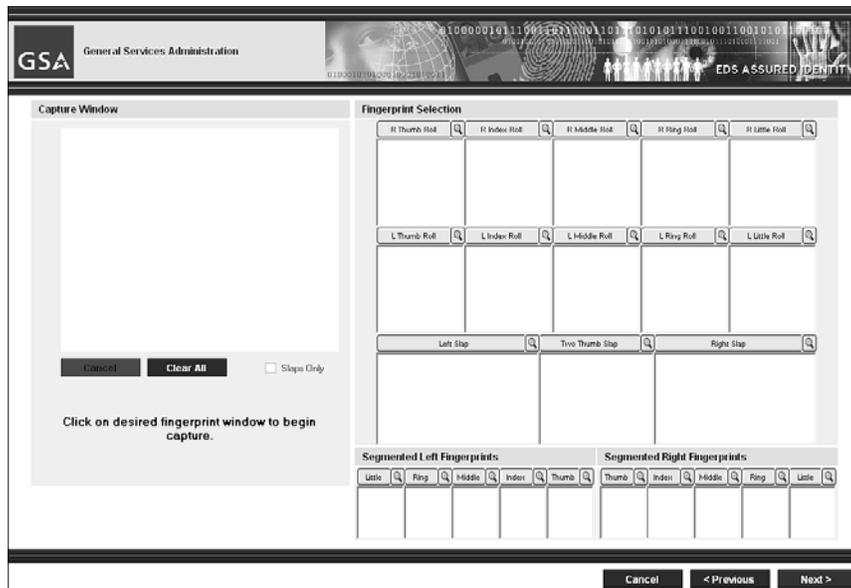
The photo displays as two images in the **Photo Capture** screen: **Original Image** and **Optimized Image**.

Be patient, it may take 10 to 15 seconds for the optimized image to appear.



Original and Optimized Images

6. If there are no error messages and the photo image resembles the referenced (silhouetted) image, click the **Next** button to proceed to the next screen.
*The **Ten Print Capture** screen displays.*



Ten Print Capture Screen

Capture Fingerprints

The **Ten Print Capture** screen has the ability to capture slap and rolled fingerprint images.

The images required on this screen are:

- 10 Rolled fingerprints
- Left Slap
- Two Thumb Slaps
- Right Slap
- Segmented left fingerprints (automatically populated after Left Slap completed)
- Segmented right fingerprints (automatically populated after Right Slap completed)

Rolled Fingerprints

Rolled fingerprints are obtained when the Applicant rolls their fingers on the scanner to capture a “wrap-around” image of the fingerprints. Capturing individual rolled fingerprints can be conducted in any order.

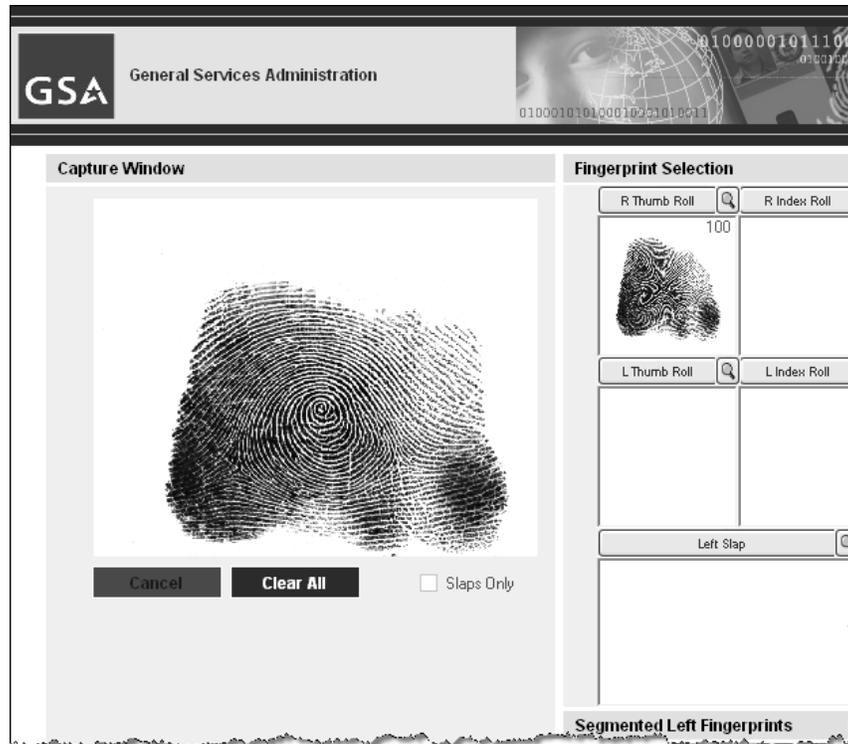
Follow these steps to capture rolled fingerprints:

1. Click the **image box** or **title bar** above the thumb or finger to be printed.
2. Based on your selection in step 32, have the Applicant press their finger or thumb on one of the red dotted lines on the fingerprint scanner.

Two red lights display on the scanner. When the scanner detects the finger, the light closest to the finger turns green and the machine sounds a beep indicating it is OK to proceed with the roll.

3. Have the Applicant wait for the green light, then roll their finger or thumb slowly across the platen from one dotted red line to the other.

*The fingerprint displays in the **Capture Window** as it is being captured.*



Capture Window

When the Applicant finishes the role and lifts their finger, both lights turn green. The Applicant may have to try step 3 a few times to acquire the proper technique for rolling a quality print.

4. View the image in the **Capture Window** and note the quality score in the image box.
A score below 60 is displayed in red and must be recaptured.
5. If the fingerprint is poor quality, click the **image box** or **title bar** to delete the print and ask the Applicant to roll the print again.



Hint

You can click the  in the upper right corner of each rolled image to open a window for an expanded view. Click the **X** to close the window.

Coach the Applicant to assist them in acquiring an acceptable print. You may also have to assist the Applicant to roll their fingers.

6. Repeat steps 1 through 5 until all fingerprints are processed.

Slap Fingerprints

Slap fingerprints can be obtained by placing fingers flat on the scanner without rolling any of the fingers. Follow these steps to obtain slap fingerprints:

1. Click the **image box** or **title bar** above the set of fingerprints to be captured (Left Slap, Two Thumbs, or Right Slap).

Fingerprinting Left Slap, Two Thumb Slap, or Right Slap can be conducted in any order.

2. Click in the **Left Slap** image box.
3. Ask the Applicant to place the four fingers of their left hand on the platen.

You will see four red lights, one for each finger.

4. Ask the Applicant to press firmly, but not too hard, and adjust their fingers as they watch for all four lights to turn green.

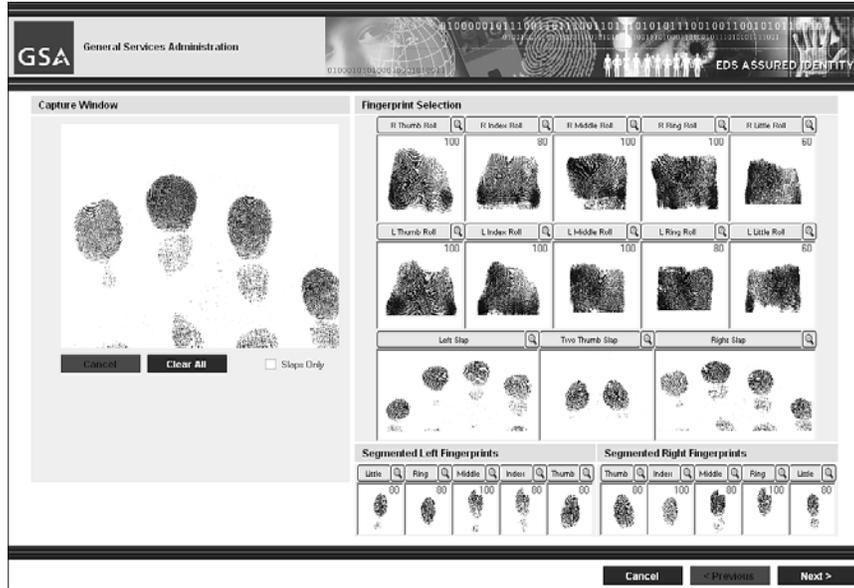
When the lights turn green, the slap will be captured.

The fingerprints display in the Capture Window as they are being captured.

5. View the image in the **Capture Window** and note the quality score in the image box. An acceptable score is 60 or higher.

If the score is below 60, click the image box or title bar to delete the prints and capture the prints again.

6. Repeat the same process with both thumbs and the four fingers on the right hand.



Completed Ten Print Capture Screen

7. Click the **Next** button to proceed to the next screen.
*The **Fingerprint Verification** screen displays.*



Fingerprint Verification Screen

Primary and Secondary Fingerprints

Once all fingerprints have been captured, the system requires the Applicant to verify the two primary fingerprints - normally the right and left index fingers. The **Fingerprint Verification** screen is used to validate the Primary and Secondary Fingerprint templates that were generated from the Ten Print Capture.

Follow these steps to verify the Primary and Secondary fingerprints:

1. Click the **Verify** button in the **Primary Fingerprint** section.
2. Have the Applicant press their primary finger, as indicated on the screen, on the **Single Fingerprint Reader**.
*The image displays in the **Fingerprint Capture** window.*

Once the system validates the fingerprint, it sounds a chime and displays the message **Primary Finger Verified**.

If the system is having difficulty processing the fingerprint, it displays various messages in the **Fingerprint Capture** window to facilitate a clear reading (e.g., press harder, move left, move up).

3. Click the **Verify** button in the **Secondary Fingerprint** section.
4. Have the Applicant press their secondary finger, as indicated on the screen, on the **Single Fingerprint Reader**.
*The image displays in the **Fingerprint Capture** window.*

Once the system has validated the fingerprint, it displays the message **Secondary Finger Verified**.

5. Click the **Next** button to proceed to the next screen.
*The **Enrollment Status** screen displays.*

Enrollee	
First Name	JOHN
Middle Name	EDWARD
Last Name	DOE

Registration Status	
Biographic Data Capture	<input checked="" type="checkbox"/>
Document Collection	<input checked="" type="checkbox"/>
Photo Capture	<input checked="" type="checkbox"/>
Fingerprint (10 Print) Capture	<input checked="" type="checkbox"/>
Fingerprint Verification	<input checked="" type="checkbox"/>
Enrollee Status	REGISTERED

Enrollee Photo: 

Expiration Date: 7/6/2010

Enrollment Status Comments:

Buttons: Cancel, < Previous, Save

Enrollment Status Screen

Complete the Enrollment Process

The final step in the enrollment process involves reviewing the information on the **Enrollment Status** screen.

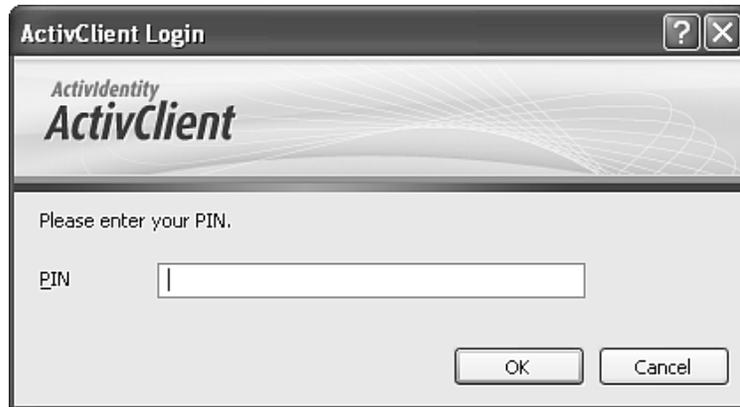
To complete the enrollment process, do the following:

1. Review contents of the **Enrollment Status** screen to compare and verify that the name and photo on the screen match the enrollee.

Green ✓ marks in the **Registration Status** section indicate that all steps have been completed. A red X marks any part of the enrollment that was not completed. Use the **Previous** button to return the section that is incomplete. Complete the section and use the **Next** button to return to the **Enrollment Status Screen**.

2. Enter any appropriate comments in the **Enrollment Status Comments** field.
3. Click the **Save** button.

*The **ActivClient Login** dialog box displays.*



ActivClient Login Dialog Box

You must verify your identity to save the changes and digitally sign the record.

4. Enter your PIN in the **ActivClient** dialog box.
5. Click the **OK** button.

*A blank **Enrollee Search** screen displays.*

Enrollment of the Applicant is complete. At this point, the Registrar can continue to enroll the next Applicant or click the **Logoff** button to log off of the system.



Key Point

Fluctuations in the VPN line may cause an error message when you try to save the record. If this happens, try to save it again. Occasionally, you may have to cancel the record and begin again.



Watch Out!

Remember, there are no partial saves in the enrollment procedures. When you save and digitally sign the record, you can no longer access this record. You cannot go back and change data, recapture a photo or fingerprints. The data is sent to the Identity Management System. No data remains behind on the enrollment workstation computer.

Exceptions

Failure to Scan Exceptions

Occasionally, an Applicant's driver's license, fails to properly scan into the AssureTec scanner during the Applicant's enrollment session. For example, an Applicant's driver's license may scan and the image may be available, but the machine-readable data on the license cannot be read. The AssureTec scanner will display a FAILED indicator below the scanned document if the scan has been unsuccessful.

In this scenario, the Applicant's driver's license has been scanned through the AssureTec scanner and it appears on the **Document Collection** screen. The corresponding document information, however, does not appear on the screen because the card reader could not read the data on the license. The license receives a red FAILED indicator below the picture.

The screenshot shows the 'Document Collection' interface with three document slots. Each slot includes a 'Front' and 'Back' view button, a scanned image, a status indicator, and a form for document information.

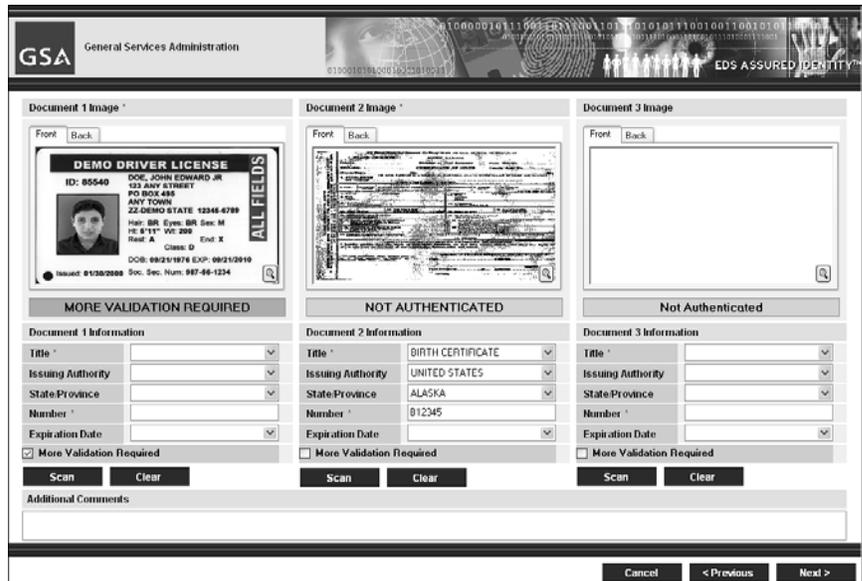
Document 1 Information	Document 2 Information	Document 3 Information
Title: <input type="text"/>	Title: BIRTH CERTIFICATE	Title: <input type="text"/>
Issuing Authority: <input type="text"/>	Issuing Authority: UNITED STATES	Issuing Authority: <input type="text"/>
State/Province: <input type="text"/>	State/Province: ALASKA	State/Province: <input type="text"/>
Number: <input type="text"/>	Number: B12345	Number: <input type="text"/>
Expiration Date: <input type="text"/>	Expiration Date: <input type="text"/>	Expiration Date: <input type="text"/>
<input type="checkbox"/> More Validation Required	<input type="checkbox"/> More Validation Required	<input type="checkbox"/> More Validation Required
Buttons: Scan, Clear	Buttons: Scan, Clear	Buttons: Scan, Clear

At the bottom of the screen are navigation buttons: Cancel, < Previous, and Next >.

Document Collection Screen – FAILED Indicator

Follow these steps to address the FAILED indicator and manually enter the document information.

1. Rescan the license up to 10 more times to see if the AssureTec will pick up the data and validate the license.



Document Collection Screen – MORE VALIDATION REQUIRED Indicator

If the data could not be read from the license and the **Document 1 Information** fields have not been populated, refer to the license to enter this information manually. Two of the fields, marked with a red asterisk, are mandatory: **Title** (the type of document), and **Number**.

2. From the **Title** dropdown list, select DRIVER’S LICENSE.
3. In the **Number** field, enter the driver’s license number.
4. Complete as many data fields as possible.

If the license appears valid, continue scanning the remaining identity documents and continue with the enrollment. To determine if the license is valid, look for signs of tampering, for example: peeling laminate, text that is scratched out, hologram is not visible, or the license is expired. If you are not confident that the license is valid, mark the document for more validation by the Security Officer.

5. In the **Document 1 Information** section, on the Document Collection screen, click the **More Validation Required** check box.

The FAILED indicator changes to MORE VALIDATION REQUIRED

6. Type the reasons for clicking the **More Validation Required** checkbox in the **Additional Comments** field.



Watch Out

If you click the **More Validation Required** checkbox, you must enter a comment in the **Additional Comments** field. The Security Officer must know why you checked the **More Validation Required** checkbox.

Please indicate your observations in clear and concise comments. For example:

Virginia license failed to scan after multiple attempts, laminate peels back, date looks like it was changed.

OR

GA license failed to scan after multiple attempts, no hologram visible on license.

7. Click the **Next** button.

You have completed flagging the document for further validation. You would now continue with the rest of the steps required for enrolling the Applicant.

Manual Photo Optimization

You may need to manually optimize an Applicant's photo taken during the enrollment process. Manual photo optimization is used to correct for minor size and orientation problems with the photo in lieu of re-capturing the photo. Also, if the image does not resemble the referenced (silhouette) image to the lower left of the **Optimized Image** (body facing forward, both shoulders visible), the photo image will need to be optimized manually.

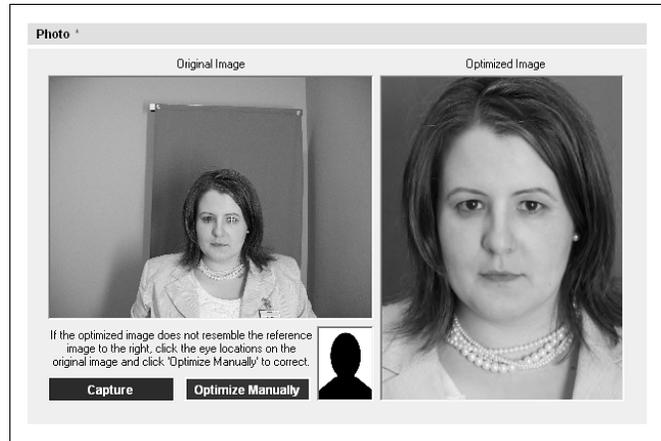
Manual optimization is performed by clicking on the **Original Image** to place two crosshairs on it. These crosshairs are taken by the system to define the desired horizontal distance between the two eyes and the horizontal alignment of the eyes and head.

The system then remaps the **Original Image** to the **Optimized Image** that will be used for identity purposes. This scales and rotates the head as desired, and can be repeated until desired results are achieved.

This procedure starts when the initial steps of photo capture are completed and the system displays an error message, or you determine that manual optimization is necessary.

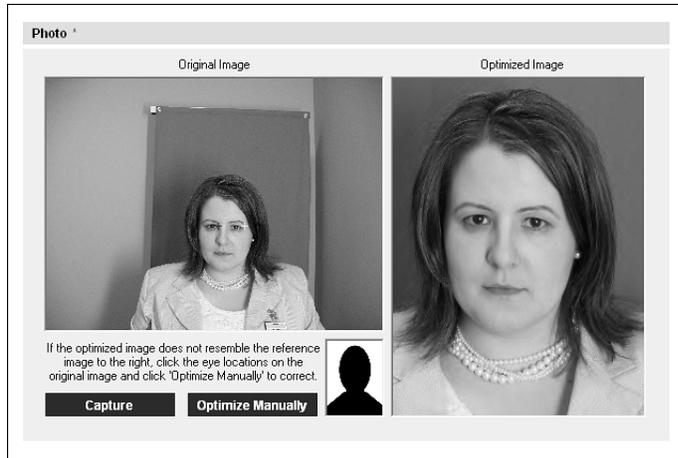
To manually optimize a photo image:

1. If a **Photo** error message displays, click **OK**.
2. In the **Original Image** box of the **Photo Capture** screen, click on the center of one of the Applicant's eyes.
A red crosshair (+) displays on the eye.
3. Click on the center of the other eye.
A yellow crosshair (+) displays on that eye.



Unsatisfactory Image - Image does not resemble silhouette

4. Click the **Optimize Manually** button. Note that this button is grayed out until the crosshairs are triggered on the **Original Image**.
*The image is repositioned in the **Optimized Image** box.*
5. Once the desired results are achieved, click the **Next** button to proceed to the next screen and continue the enrollment process.
6. Review the **Optimized Image**.
7. If the **Optimized Image** is still not satisfactory, repeat steps 2 through 4 until desired results are reached, and the **Optimized Image** resembles the referenced (silhouette) image to the lower left of the **Optimized Image** (body facing forward, both shoulders visible).



Satisfactory Optimized Image

8. Once the desired results are achieved, click the **Next** button to proceed to the next screen and continue the enrollment process.



Key Point

Check lighting, distance of the Applicant from the camera, camera flash and even applicant's hair. All of these things can affect photo optimization. Retake photo and optimize as necessary to achieve an acceptable photo. Remember, this photo is part of the Applicant's identity record and must meet FIPS standards. It is also the picture that is placed on the Applicant's PIV Credential.

Fingerprint Capture Exceptions

There are several scenarios in which an Applicant's fingerprints may be difficult to capture. This is called a Failure to Enroll (FTE). When the system detects problems with capturing fingerprints, the **Fingerprint Verification** screen will request the Registrar to identify the problem and provide any applicable comments.

Special fingerprinting situations may involve poor quality fingerprints and amputees.

Amputee

When an Applicant is missing fingers, the system will request identification of the existing fingers. In this example, an Applicant is missing the right index finger.

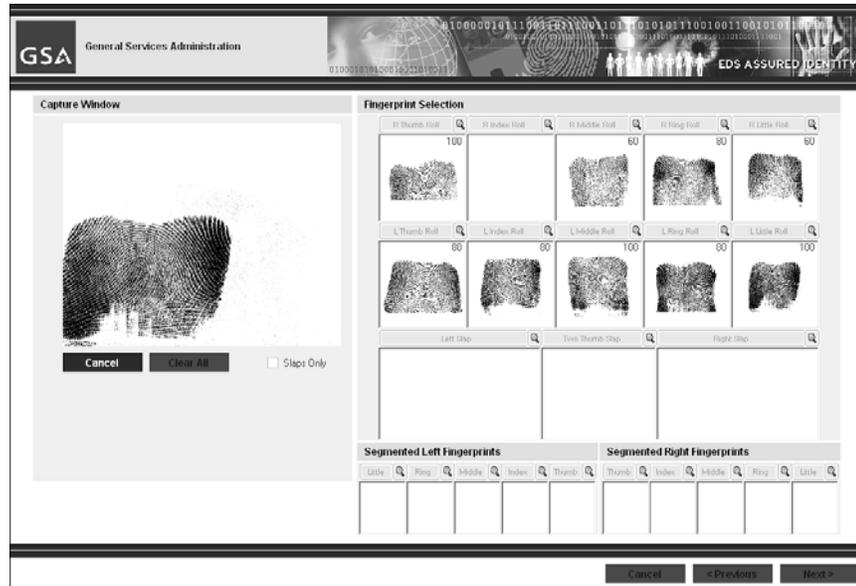
Follow these steps to process fingerprints for an amputee:

1. On the **Ten Print Capture** screen, capture individual fingerprint rolls as you normally would, skipping over the missing finger.



Key Point

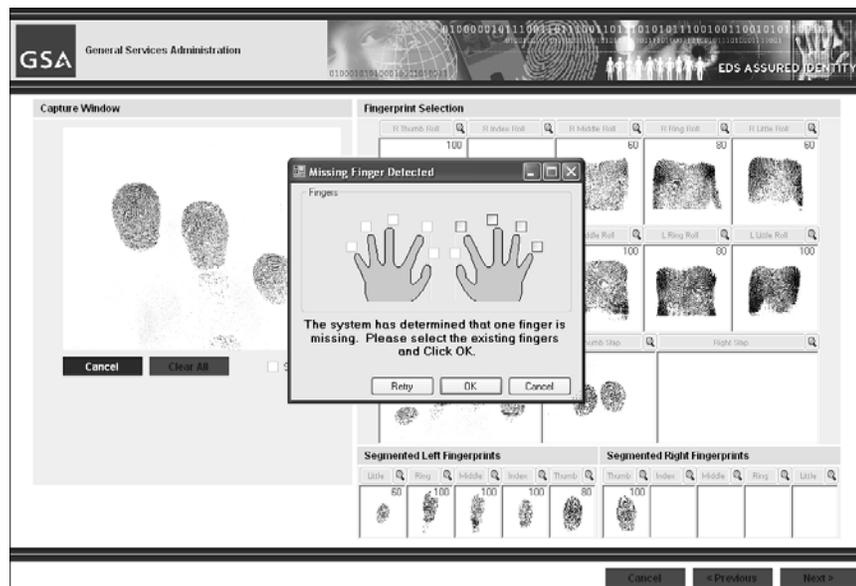
For fingerprint rolls, the system will not request identification of the existing fingers. For slaps, the system will request identification of the existing fingers as soon as it recognizes an incomplete slap.



Ten Print Capture Screen – Missing Fingerprint Roll

2. Proceed to capture the Left Slap, Two Thumb Slap, and Right Slap.

*When you capture the Right Slap (with the missing index finger), the system detects the missing finger and the **Missing Finger Detected** dialog box displays.*



Missing Finger Detected Dialog Box

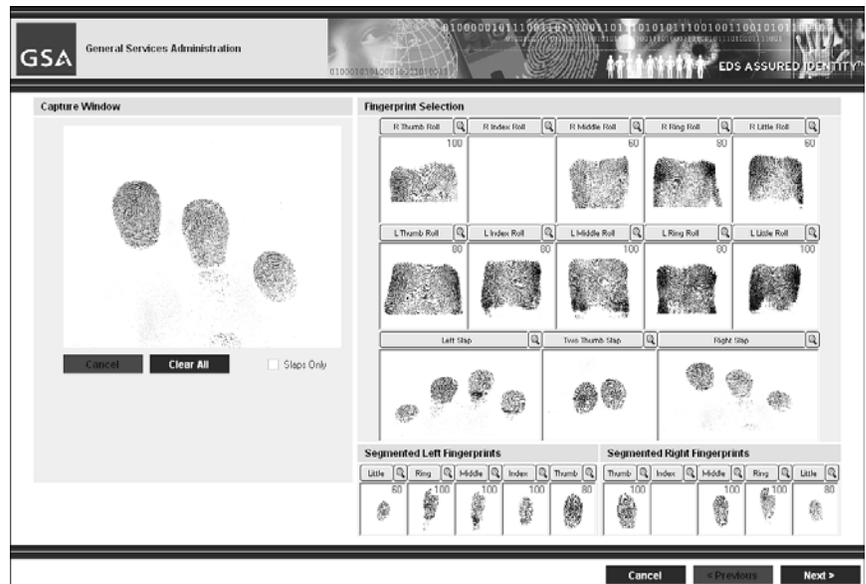
3. In the **Missing Finger Detected** dialog box, identify the existing fingers on the right hand by clicking the **check box** by each existing finger.



Missing Finger Detected – Identifying Existing Fingers

4. Click the **OK** button.

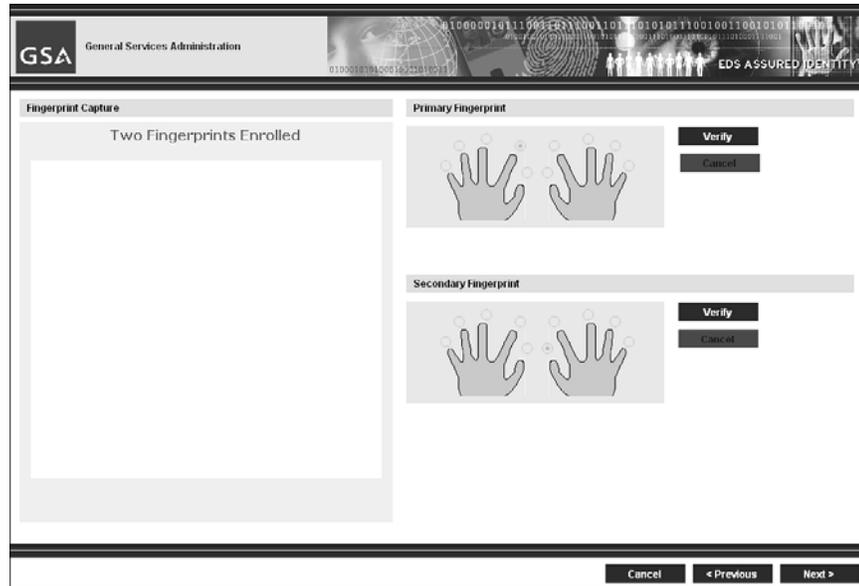
*The **Ten Print Capture** screen displays, showing the missing fingerprints.*



Ten Print Capture Screen – Missing Fingerprint

5. Click the **Next** button on the **Ten Print Capture** screen.

*The **Fingerprint Verification** screen displays.*



Fingerprint Verification Screen

In this example, the Primary Fingerprint will be the left index finger. The Secondary Fingerprint will be the right thumb.

Follow these steps to verify the Primary and Secondary fingerprints:

6. Click the **Verify** button in the **Primary Fingerprint** section.
7. Have the Applicant press their primary finger on the **Fingerprint Reader**.

*The image displays in the **Fingerprint Capture** window.*

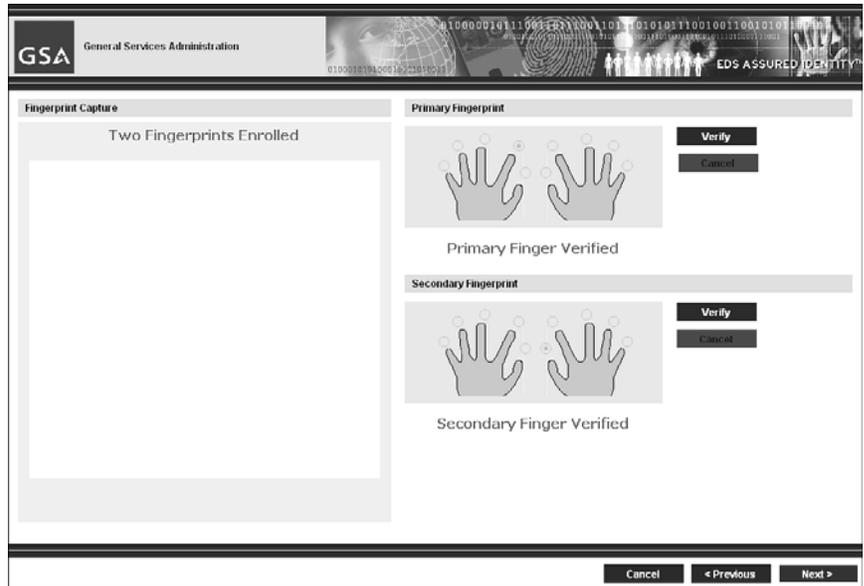
Once the system validates the fingerprint, it displays the message **Primary Finger Verified**.

If the system is having difficulty processing the fingerprint, it displays various messages in the **Fingerprint Capture** window to facilitate a clear reading (e.g., press harder, move left, move up).

8. Click the **Verify** button in the **Secondary Fingerprint** section.
9. Have the Applicant press their secondary finger on the **Fingerprint Reader**.

*The image displays in the **Fingerprint Capture** window.*

Once the system has validated the fingerprint, it displays the message **Secondary Finger Verified**.



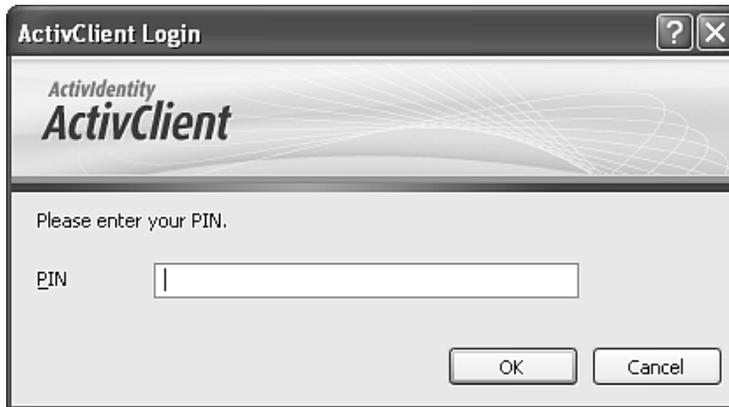
Fingerprint Verification Screen – Fingerprints Verified

- Click the **Next** button to proceed to the next screen.
*The **Enrollment Status** screen displays, indicating the steps have been completed.*



Enrollment Status Screen – Steps Completed

- Click the **Save** button on the **Enrollment Status** screen.
*The **ActivClient Login Window** displays.*



ActivClient Login Window

12. Enter your PIN and Click the **OK** button.

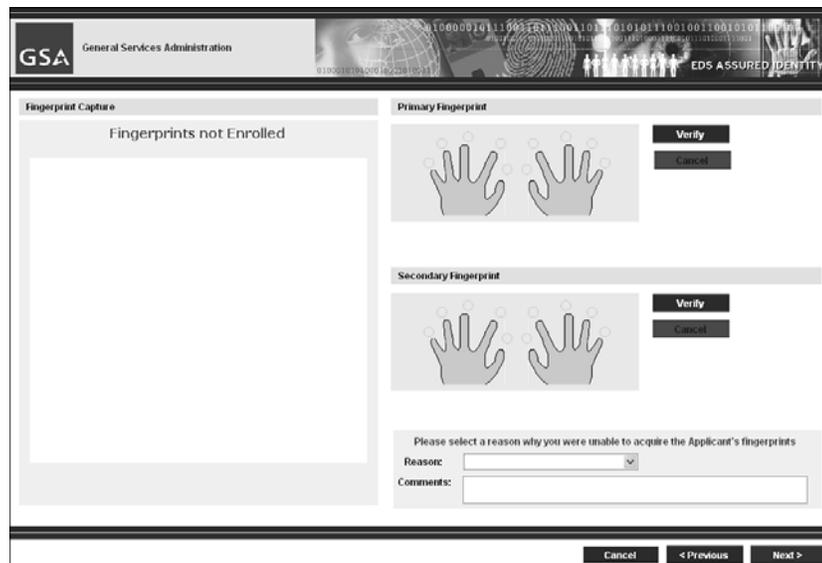
*The system returns you to the **Enrollee Search** page.*

The Enrollment process is complete.

No Fingerprints Captured

With an Applicant physically incapable of providing any fingerprints, you will completely skip the fingerprint capture steps.

1. On the **Ten Print Capture** screen, click the **Next** button.
*The **Fingerprint Verification** screen displays.*



Fingerprint Verification Screen

Note that you must provide a reason for the lack of fingerprints.

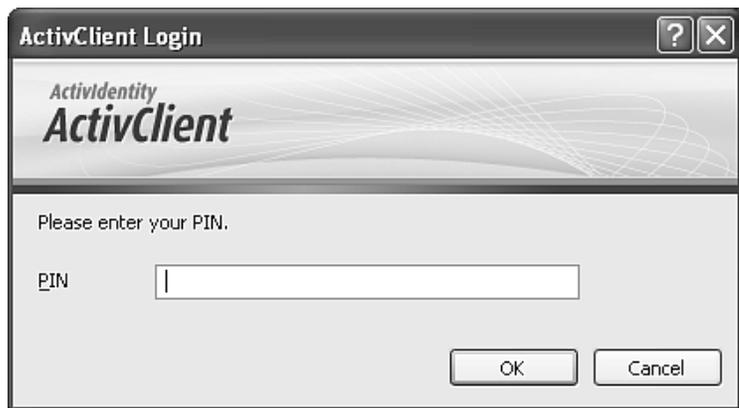
2. In the **Reason** field, select **AMPUTEE** from the dropdown list.
3. Enter appropriate comments in the **Comments** field.
4. Click the **Next** button.

*The **Enrollment Status** screen displays, indicating all steps have been completed.*



Enrollment Status Screen - Steps Completed

5. Click the **Save** button on the **Enrollment Status** screen.
*The **ActivClient Login Window** displays.*



ActivClient Login Window

6. Enter your PIN and Click the **OK** button.
*The system returns you to the **Enrollee Search** page.*

The Enrollment process is complete.

Fingers with Long Fingernails

Occasionally, you may encounter an Applicant with long fingernails that interfere with the fingerprint capture process.

1. Attempt capture of rolls and slaps.
2. If prints are unattainable on the 10-print scanner because of fingernail length or curvature, the Applicant must make another appointment when his or her fingers will fit on the platen.
3. If rolls and slaps are captured, but fingernails prevent verification on the single-print scanner, the Applicant must make another appointment when his or her fingers will fit on the platen.

This page intentionally left blank.

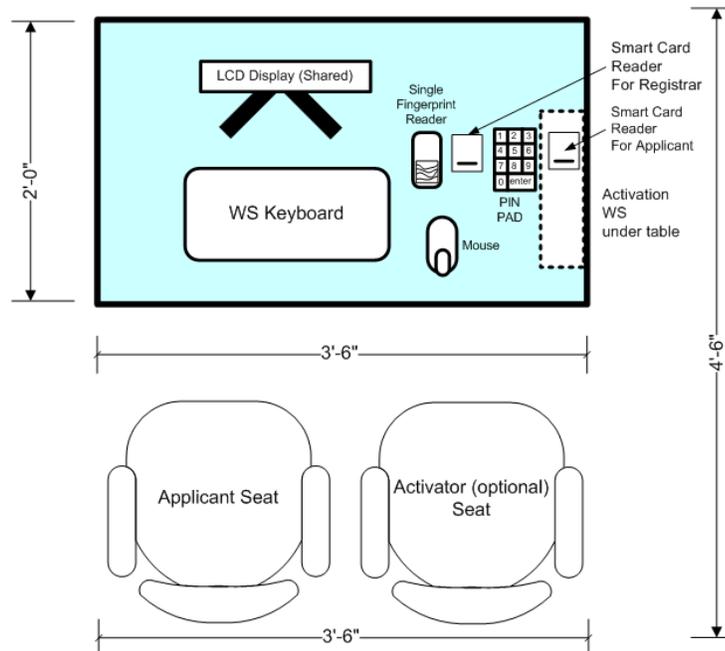
Activation Procedures

Introduction

HSPD-12 Credentialing Centers can be configured with attended activation stations, consisting of:

- Activation workstation with keyboard and mouse
- LCD display
- PIN Pad
- ID card scanner
- Smart card reader for Applicant
- Smart card reader for Registrar
- Single fingerprint reader
- Worktable
- Two chairs

The following schematic illustrates the minimum footprint of an activation workstation at a USAccess Credentialing Center.



Attended Activation Workstation

Attended PIV Credential Activation with Fingerprints

This section outlines the steps a Registrar follows to activate a PIV Credential for an Applicant. All system information is read-only at this point. The Registrar's responsibility is to verify that the system information matches the Applicant present to receive the PIV Credential.

The Applicant and PIV Credential are present and, because the Applicant has viable fingerprints physically available, they are authenticated as part of the procedure.

Steps include:

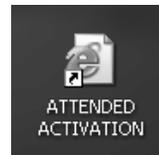
- Logging in to the ActivIdentity Card Management System
- Searching for the Applicant
- Personalizing the PIV Credential

Launching the ActivIdentity Card Management System

This procedure begins at the Activation workstation, with the ActivIdentity Card Management System portal open and waiting for the Activator to log in.

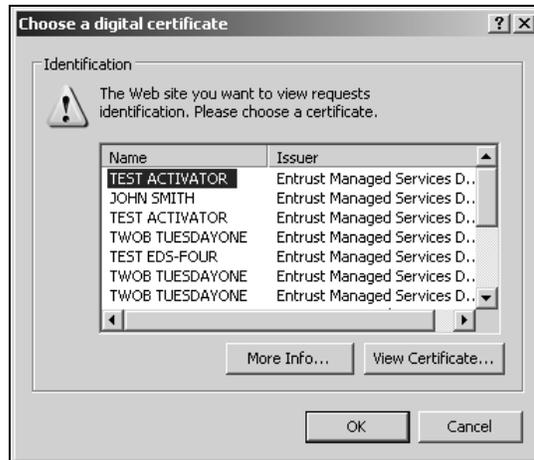
Follow these steps to log in to the ActivIdentity Card Management System:

1. Insert your PIV Credential into either of the card readers to begin the login process.
2. Click the **Attended Activation** icon on the desktop.



Attended Activation Icon

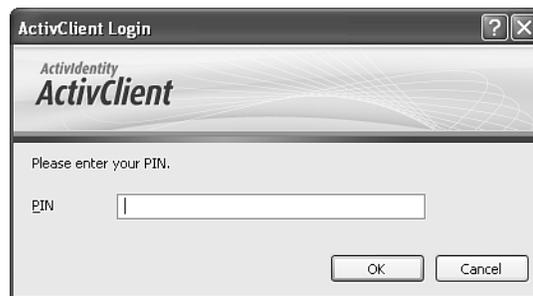
*The **Choose a digital certificate** window displays.*



Choose a digital certificate Window

3. Locate your name in the certificate list and click to select it.
4. Click the **OK** button.

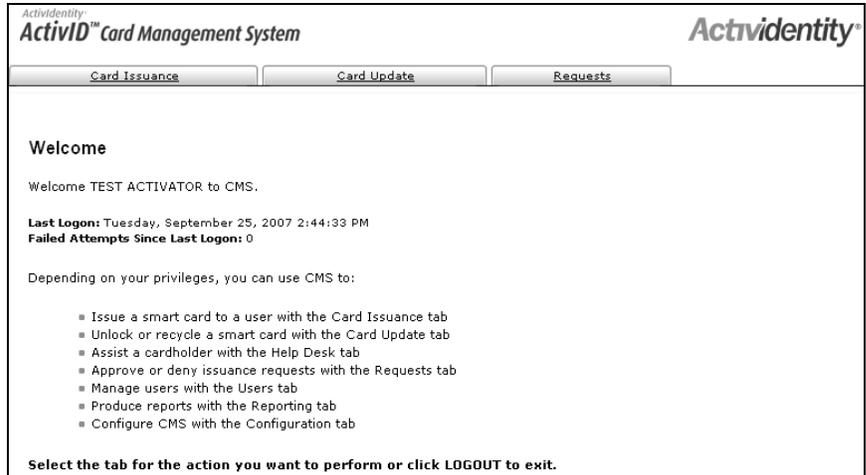
*The **ActivClient Login** window displays.*



ActivClient Login Window

5. Enter your PIN and click the **OK** button.

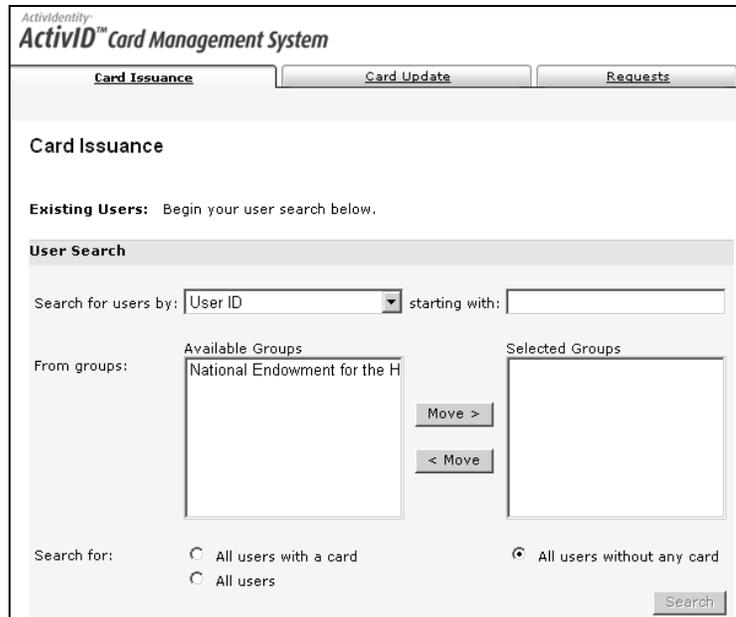
*The **ActivIdentity Card Management System– Welcome** screen displays.*



ActivIdentity Welcome Screen

- Click the **Card Issuance** link at the top of the **Welcome** page.

*The **Card Issuance** screen displays.*



Card Issuance – User Search Screen

Searching for the Applicant

The **Card Issuance** page contains **User Search** fields to help narrow down the Applicant search.

Follow these steps to select the criteria for your Applicant search and begin the PIV Credential activation process.

1. Select **Last Name** from the **Search for users by:** drop-down list.

The screenshot shows the 'User Search' form. The 'Search for users by:' dropdown menu is open, displaying a list of options: 'User ID', 'First Name', 'Last Name', 'Email Address', and 'cn'. A mouse cursor is pointing at 'Last Name'. The 'starting with:' field is empty. The 'From groups:' section is empty. The 'Selected Groups' section is empty. There are 'Move >' and '< Move' buttons between the 'From groups:' and 'Selected Groups' sections.

Select Last Name from Drop-down List

2. Enter the Applicant's last name in the **starting with:** search field.
3. Select the agency/department from the list in the **Available Groups** column.



Hint

Determine the groups that need to be selected by looking for the agency and sub agency listed on the Applicant's PIV credential. If in doubt, you may ask the Applicant, to indicate the sub agency with which they are affiliated.

The screenshot shows the 'User Search' form. The 'Search for users by:' dropdown menu is set to 'Last Name'. The 'starting with:' field contains 'natendowmentmon'. The 'From groups:' section is titled 'Available Groups' and contains a list with one item: 'National Endowment for the Humanities'. A mouse cursor is pointing at this item. The 'Selected Groups' section is empty. There are 'Move >' and '< Move' buttons between the 'Available Groups' and 'Selected Groups' sections. At the bottom, there are radio buttons for 'Search for:': 'All users with a card', 'All users', and 'All users without any card'. The 'All users without any card' option is selected. A 'Search' button is located at the bottom right.

Agency/Department Selection from Available Groups Column

4. Click the **Move** button to move the selected agency/department to the **Selected Groups** column.
5. Repeat steps 12 and 13 until you have selected all the groups you want to search.

6. Select the **All users without any card** radio button in the **Search for:** section. (This is the default setting for the radio button.)
7. Click the **Search** button.
*If there is only one match, the system will take you to the **Issuance to [Applicant's Name]** screen to view the Applicant's information. If there is more than one Applicant match, the list of users meeting the search criteria displays below the **User Search** fields.*

User ID	First Name	Last Name	Email Address	cn
0000005551	TESTER	NATENDOWMENTMONFIVE	NATENDOWMENTMONFIVE@NGC.COM	TESTER NATENDOWMENTMONFIVE
0000005550	TESTER	NATENDOWMENTMONFOUR	NATENDOWMENTMONFOUR@NGC.COM	TESTER NATENDOWMENTMONFOUR
0000005549	TESTER	NATENDOWMENTMONTHREE	NATENDOWMENTMONTHREE@NGC.COM	TESTER NATENDOWMENTMONTHREE

Search Results below the User Search fields

8. Select the Applicant's **User ID** link
*The **Issuance to [Applicant's Name]** screen for the selected user displays.*

Initiating Card Activation

Follow the step-by-step instructions on the **Issuance to [Applicant's Name]** screen.

Issuance to TESTER NATENDOWMENTMONTHREE User Lookup > User Enrollment

1. Review the user information below.

User ID:	000005549	Photo:	
First Name:	TESTER		
Last Name:	NATENDOWMENTMONTHREE		
Email Address:	NATENDOWMENTMONTHREE@NGC.COM		
cn:	TESTER.NATENDOWMENTMONTHREE		

Image From File:

An issuance has been requested for TESTER NATENDOWMENTMONTHREE. You are about to execute this issuance request.

2. Select the action you want to perform: Local Issuance

3. Choose the smart card reader for issuance:

4. Insert the smart card to issue in the smart card reader and click Next.

Issuance to [Applicant’s Name] Screen

Step 1. Review the Applicant’s information and digital photograph to verify identity.

Step 2. The action you want to perform is Local Issuance. It is selected by default.

Step 3. Choose the smart card reader for issuance: from the drop-down list. Select the smart card reader that is not holding a card.

2. Select the action you want to perform: Local Issuance

3. Choose the smart card reader for issuance:

- ActivCard ActivKey 0
- ActivIdentity ActivKey Sim 0
- OMNIKEY CardMan 3x21 0
- OMNIKEY CardMan 3x21 1

4. Insert the smart card to issue in the smart card reader and click Next.

Smart Card Reader Drop-down List

Choosing the Empty Card Reader

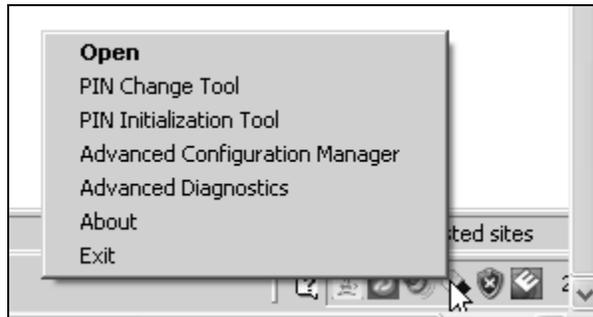
You can determine the name of the empty smart card reader by accessing the ActivClient Agent program. Locate the ActivClient Agent icon in the system tray at the lower-right corner of your monitor.



ActivClient Agent Icon in System Tray

- a. Right-click the **ActivClient Agent** icon .

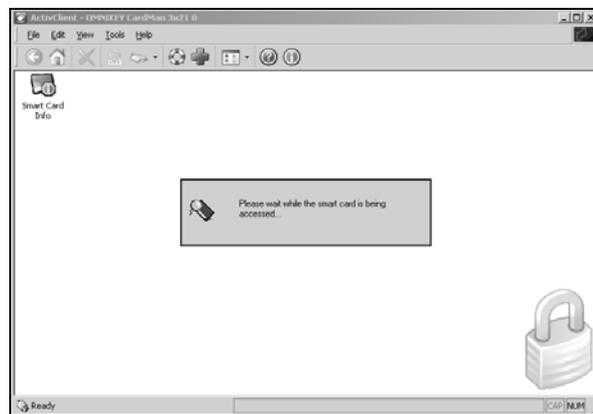
The **ActivClient Agent** menu displays.



ActivClient Menu

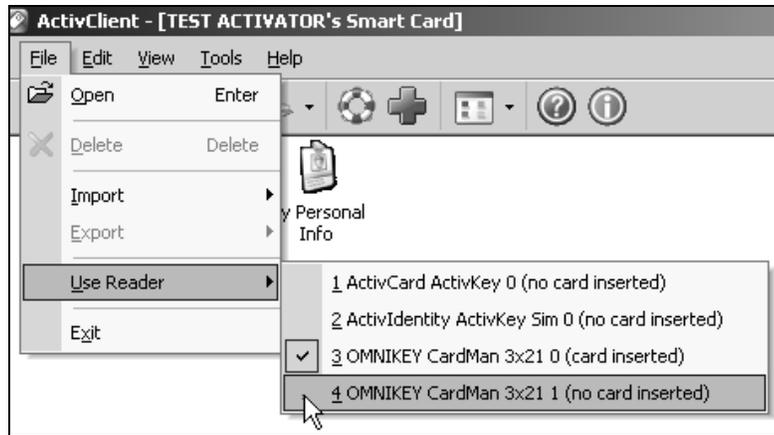
- b. Select the **Open**.

The **ActivClient Smart Card Info** window displays and the system checks for readers that contain smart cards.



ActivClient Smart Card Info Window

- c. On the Menu Bar, select **File > Use Reader** to view readers.



Use Card Reader Menu Items

- d. Make note of which OMNIKEY reader is displaying (**no card inserted**).
- e. Click the  icon at the top right of the browser to close the ActivClient window.

*You should once again view the **Issuance to [Applicant's Name]** screen. If not, bring it up from the task bar.*

Complete **Step 3** by choosing the correct smart card reader, the reader that displayed (no card inserted). In the example above, you would select OMNIKEY CardMan 3x21 1.

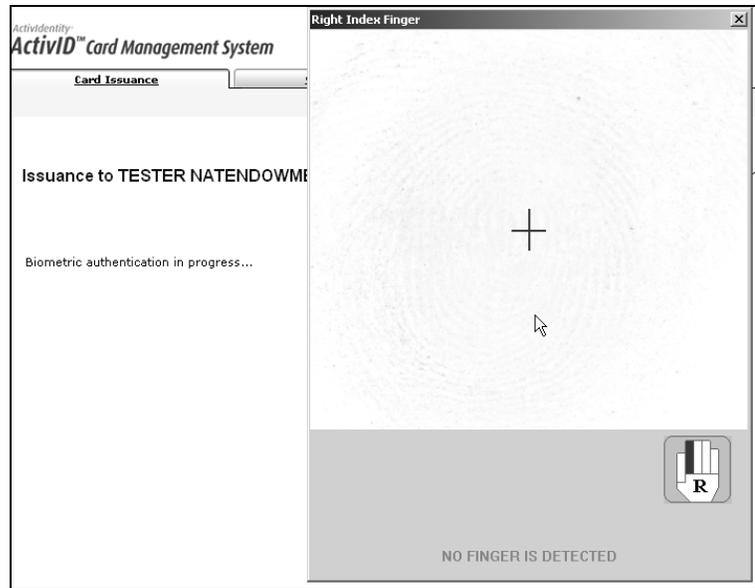


Hint

If the card readers at the Activation workstation have not previously been labeled, label them now with a 0 or 1. This will allow you to perform Step 3 of the Activation process without stopping to determine the card reader number.

Step 4: Insert the Applicant's PIV Credential into the card reader for activation.

9. Click the **Next** button.
*The system indicates that biometric authentication is in progress and the **Fingerprint Capture** window displays.*



Fingerprint Capture Window

Verifying the Applicant's Fingerprint against the Database

The system requires biometric authentication of the Applicant.

10. Ask the Applicant to place his or her primary finger, which is indicated by the hand diagram, on the fingerprint reader.



Hint:

The primary finger is indicated in the window title bar and in the pictogram of the hand in the lower right corner of the window.



Hand Diagram with Primary Finger

The Applicant's fingerprint displays in the Fingerprint Capture window and the message "IMAGE IS GOOD FOR CAPTURE" appears at the bottom of the window. You will also see a message if the Applicant needs to press harder or move the finger.

Note: The system omits this step when fingerprints are not

available during enrollment.

The **Information Gathering** screen displays. Note that the **Biometric authentication succeeded** message also displays.

Issuance to TESTER NATENDOWMENTMONTHREE	Information Gathering
Biometric authentication succeeded.	
1. Select the card policy for the smart card:	<input type="text" value="NEH-F2F-V1"/>
2. Choose a PIN for the smart card:	<input type="text"/>
Confirm the PIN:	<input type="text"/>
3. Click Next to personalize the smart card.	
<input type="button" value="Back"/>	<input type="button" value="Next"/>

Information Gathering Screen

Completing the Information Gathering Screen

11. Use the drop-down menu to complete the **Select the card policy for the smart card** field:

- a. Select **F2F-V1** to activate cards with fingerprints.
- b. Select **F2F-NOFP-V1** to activate cards without fingerprints.



Watch Out!

The default card policy is set to **F2F-NOFP-V1**. If you do not choose a card policy, the default policy will be used to encode the card. The system will not encode a card when fingerprints exist in the Applicant's record and the card policy is set to **F2F-NOFP-V1**. The only time this policy should be selected is when the Biometric Authentication page indicates no biometrics are available for this Applicant. For most Applicants, you will have to click the **Card Policy** drop-down box and choose, the **F2F-V1**.

12. Ask the Applicant to choose a Personal Identification

Number (PIN) for the smart card.

The PIN must contain at least 6 but no more than 8 numerals. Predictable sequences of numbers are not allowed.



Watch Out!

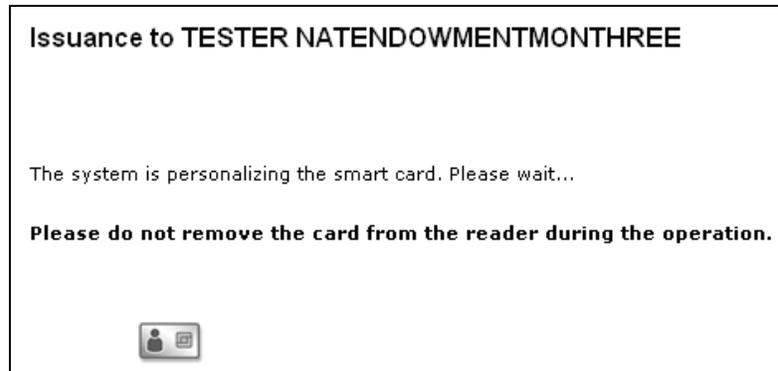
DO NOT choose or suggest a PIN for the Applicant.

13. Ask the Applicant to type his or her PIN in the **Choose a PIN for the smart card:** field.
14. Ask the Applicant to retype his or her PIN in the **Confirm the PIN:** field.
15. Click the **Next** to personalize the smart card.
*The **Card Personalization** page displays. During PIV Credential personalization, data will be read from and written to the card. Personalization may take from 6 and 8 minutes.*



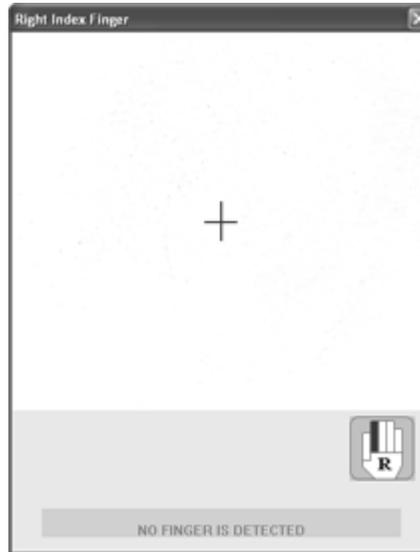
Watch Out!

The system instructs you to not remove the card during this process.



Personalization Message

*The **Fingerprint Capture** window displays at the end of the personalization process.*



Fingerprint Capture Window

Verifying the Applicant's Fingerprints against the Card

16. Ask the Applicant to place his or her primary finger, which is indicated by the hand diagram, on the fingerprint reader.



Hand Diagram with Primary Finger

The Applicant's fingerprint displays in the Fingerprint Capture window and the message "IMAGE IS GOOD FOR CAPTURE" appears at the bottom of the window. You will also see a message if the Applicant needs to press harder or move the finger.

Note: The system will omit this step when fingerprints are not available.

The Applicant's fingerprint appears in the **Fingerprint Capture** window and the message "IMAGE IS GOOD FOR CAPTURE" appears at the bottom of the window.

THE CARD HAS BEEN PERSONALIZED. The **Acknowledgment Required:** message displays and you are automatically

redirected to the **Privacy Act Statement**.

Agreeing to the Privacy Act Statement and Acknowledgement of Responsibilities

As the final step of the activation process, the Applicant must use his or her personalized credential to agree to the terms of the **Privacy Act Statement** and **Acknowledgement of Responsibilities**.

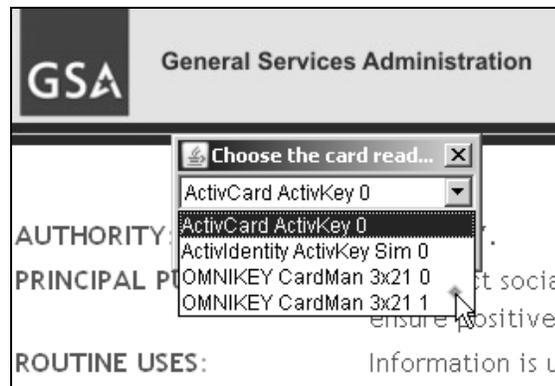
17. Ask the Applicant to read the Privacy Act Statement and the Acknowledgement of Responsibilities.
18. Type his or her first and last names into the First Name and Last Name fields. Type the names exactly as they appear on the Applicant's credential.
19. Remove the PIV card from the card reader and find the card number, which is located on the back of the card in the bottom left corner.



Location of Card Number on Card Back

20. Type the card number into the **Card Number** field.
21. Reinsert the card into the card reader.
22. Scroll to the bottom of the page.
23. Ask the Applicant to click the **I Agree** button to agree to the terms.

*The **Choose Card Reader** menu option displays.*



Choose the Card Reader Menu Option

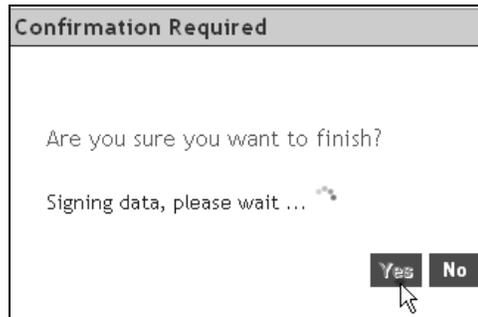
24. Select the card reader containing the Applicant's card from the drop-down list.
25. Click the **OK** button.

*A **Confirmation Required** dialog box displays, asking, **Are you sure you want to finish?***



Hint

If you cannot remember the name of the empty card reader, repeat actions a. through e. in the **Choosing the Empty Card Reader** section of this guide.



Confirmation Required Dialog Box

26. Click the **Yes** button.

*The **ActivClient Login** window displays.*



ActivClient Login Window

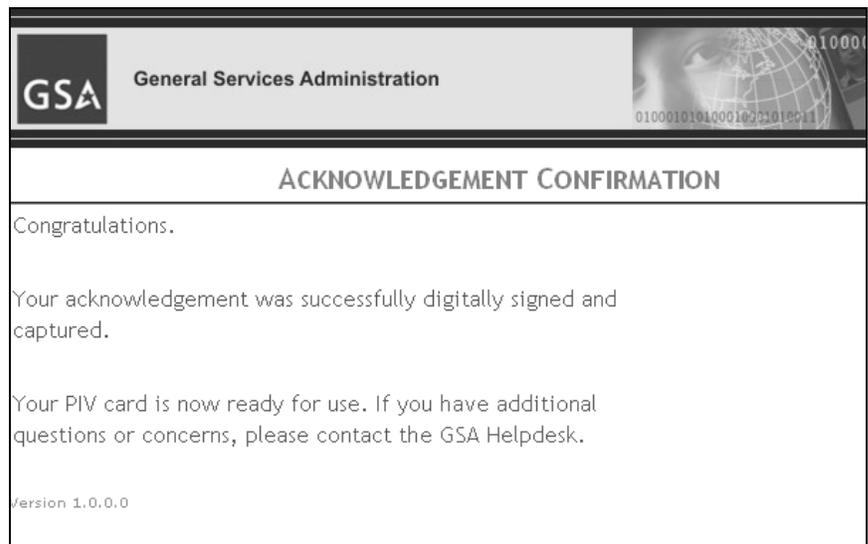
Digitally Signing the PIV Credential

27. Ask the Applicant to type his or her new PIN.
28. Click the **OK** button.

*A **Confirmation Required** dialog box displays.*

29. Click the **Yes** button.

The **Acknowledgement Confirmation** screen displays and the Applicant's digital signature has been recorded.



Acknowledgement Confirmation Screen

Completing the PIV Credential Activation

30. Ask the Applicant to remove his or her credential from the card reader.
31. Log out of the ActivClient program by clicking the **LOGOUT** link in the upper right corner of the window.

Attended PIV Credential Activation without Fingerprints

For the most part, the Activation process is the same for an Applicant who is unable to provide viable fingerprints during activation. You will follow the steps in the *Attended PIV Credential Activation with Fingerprints* section of this guide to:

- Launch the ActivIdentity Card Management System
- Select a digital certificate
- Log in to the ActivIdentity Card Management System
- Search for the Applicant
- Initiate card activation

When you click the **Next** button after inserting the card into the card reader, the system will skip the primary finger verification against the database and take you directly to the **Information Gathering** screen. A message displays at the top

of the screen alerting you that there is **No biometric information** and the system is **Skipping authentication**.

In this case, you must select the **F2F-NOFP-V1** card policy to indicate that no viable fingerprints presented by the Applicant.

No biometric information. Skipping authentication.

Continue with the steps in the *Attended PIV Credential Activation with Fingerprints* section of this guide to:

- Complete the **Information Gathering Screen** to begin card personalization
- Agree to the **Privacy Act Statement** and **Acknowledgement of Responsibilities**
- Digitally sign the PIV Credential
- Complete the PIV Credential activation

Note: The system will not ask for verification of the Applicant’s fingerprint during card personalization.

What if card activation fails?

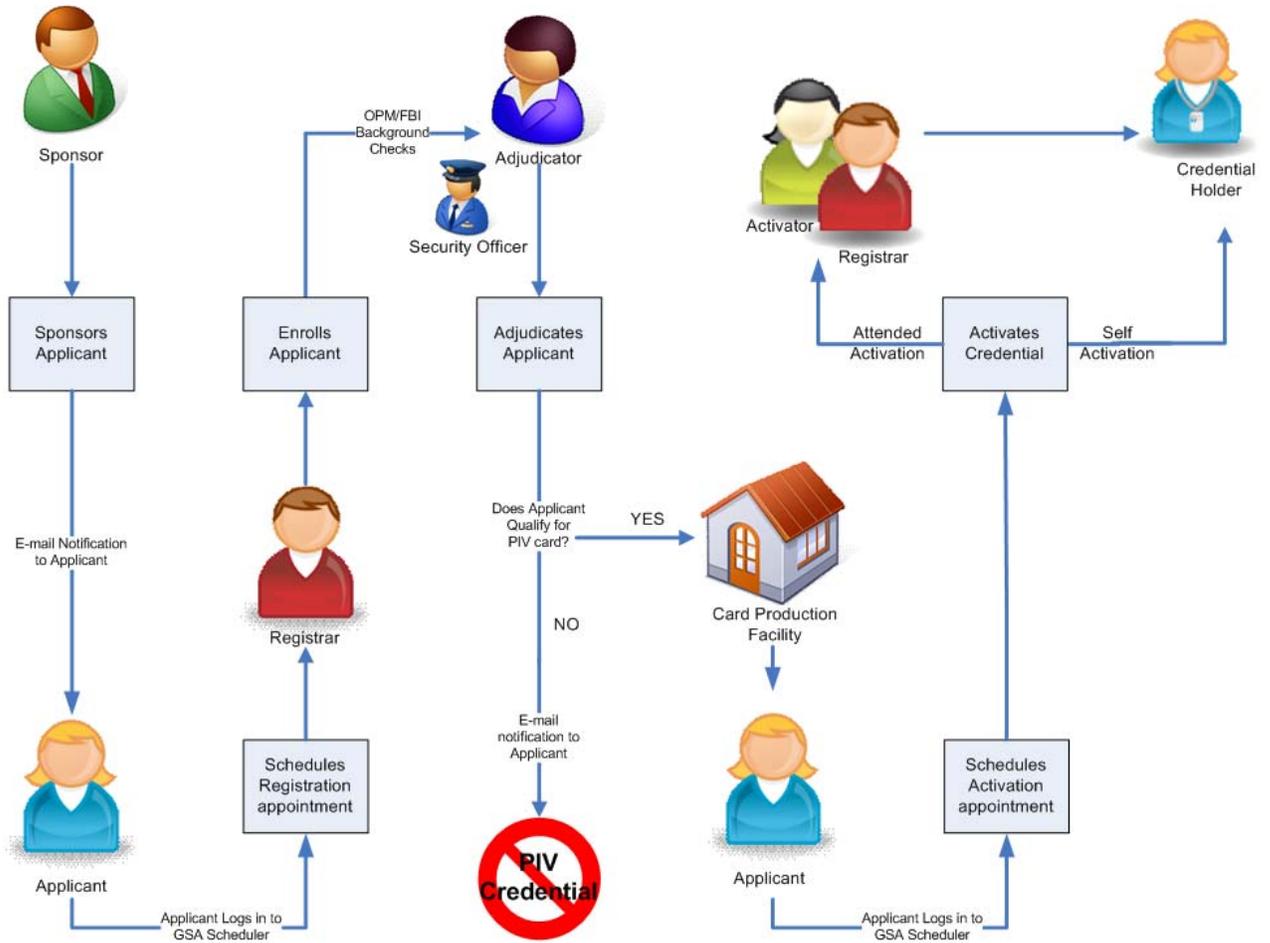
Follow these procedures if card activation fails before the first fingerprint verification:

1. Ask the applicant to remove his or her card from the card reader.
2. Try to activate the card a second time.

Follow these procedures if card activation fails after the first fingerprint verification:

1. Ask the Applicant to remove the card from the card reader.
2. Call the Help Desk for assistance at 866-493-8391 and explain the problem.
3. Ask the Applicant to wait while you follow the Help Desk directions to activate the card.

Appendix A - Enrollment Process Flow



This page intentionally left blank.

Appendix B - Terms and Acronyms

Acronym	Definition
C&A	Certification and Accreditation
CA	Certificate Authority
CHUID	Cardholder Unique Identifier
DAA	Designated Approval Authority
DHS	Department of Homeland Security
EDS	Electronic Data Systems
e-QIP	Electronic Questionnaire for Investigations Processing
FBI	Federal Bureau Investigation
FBI FP	FBI National Criminal History Fingerprint
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSA	General Services Administration
HSPD - 12	Homeland Security Presidential Directive #12
IDMS	Identity Management System
INS	Immigration & Naturalization Service
LACS	Logical Access Control System
MSO	Managed Services Office
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PCI	PIV Card Issuer
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification – Phase 1
PIV-II	Personal Identity Verification – Phase 2
PKI	Public Key Infrastructure
SP	Special Publication

This page intentionally left blank.

Appendix C - Definitions

Access control – the process of granting or denying requests to access physical facilities or areas, or to logical systems (e.g., computer networks or software applications). See also “logical access control system” and “physical access control system.”

Authentication - the process of establishing an individual’s identity and determining whether individual Federal employees or contractors are who they say they are.

Authorization - process of giving individuals access to specific areas or systems based on their rights for access and contingent on successful authentication.

Background Investigation – any one of various Federal investigations conducted by OPM, the FBI, or by Federal departments and agencies with delegated authority to conduct personnel security background investigations.

Biometric – a measurable physical characteristic used to recognize the identity of an individual. Examples include fingerprints and facial images. A biometric system uses biometric data for authentication purposes.

Contractor – see “Employee”.

Employee – as defined in Executive Order (EO) 12968, “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head. See also “Employee” as defined in title 5 U.S.C §2105.

e-QIP Tracking Number – Number assigned by e-QIP to each Form SF-85 application. For those Interior bureaus and offices using e-QIP, the tracking number must be written on the fingerprint card when it is submitted to OPM in order to bind the fingerprint card to the proper applicant.

FBI FP Check – National Criminal History Fingerprint check of the FBI fingerprint files. This check is an integral part of the NACI.

Identity Management System (IDMS) - one or more systems or applications that manage the identity verification, validation, and card issuance process. The IDMS software is used by PIV Registrars to enroll Applicants.

Identity-proofing – the process of providing identity source documents (e.g., driver’s license, passport, birth certificate, etc.) to a enrollment authority, or the process of verifying an individual’s information that he or she is that individual and no other. FIPS 201-1 requires that one of these documents be an original State or Federal Government-issued photo ID, and the other be from the approved set of identity documents listed on Form I-9.

Logical Access Control System (LACS) – protection mechanisms that limit users' access to information technology (IT) systems by restricting their form of access to those systems necessary to perform their job function. These LACS may be built into an operating system, application, or an added system.

National Agency Check (NAC) – The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index, Defense Clearance and Investigation Index, FBI Name Check, and FBI National Criminal History Check.

National Agency Check with Inquiries (NACI) – the basic and minimum investigation required of all Federal employees and contractors consisting of searches of the OPM Security/

Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary. A NACI also includes written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Physical Access Control System (PACS) – protection mechanisms that limit users' access to physical facilities or areas within a facility necessary to perform their job function. These systems typically involve a combination of hardware and software (e.g., a card reader), and may involve human control (e.g., a security guard).

PIV-II Credential – a government-issued identity credential, referred to as a smart card, which contains a contact and contact-less chip. The Cardholder's facial image will be printed on the card along with other identifying information and security features that can be used to authenticate the user for physical access to federally controlled facilities. The card may include a PKI certificate, which controls logical access to federally controlled information systems.

Public Key Infrastructure (PKI) – A service that provides cryptographic keys needed to perform digital signature-based identity verification, and to protect communications and storage of sensitive data.

SF-87 - Fingerprint Chart for Federal employee(s) or applicant for Federal employment.

Submitting Office Identifier (SOI) – Number assigned by OPM to identify office that submitted the NACI request.

Appendix D - Homeland Security Presidential Directive 12



For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard,

the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

###
