



Lifecycle Workstation Operator Training:

- PIN Reset and Certificate Update**
- Alternative Logon Token/ALT Card
(Cyber Access Smart Card) Issuance & Recycle**

**US Department of Health & Human Services
September, 2012**

Training Overview

- Lifecycle Workstation/Card Management Agent Overview
- Logging into LWS Software
- PIN Reset Process
- Certificate Update Process
- Cyber Access Smart Card Issuance
- Cyber Access Smart Card Recycle



Lifecycle Workstation (LWS)/ Card Management Agent Overview



Logging into LWS Software

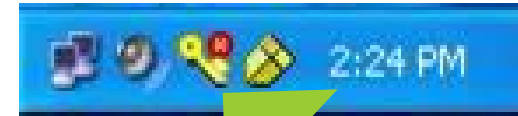
Lifecycle Workstation/Card Management Agent Overview

- The Lifecycle Workstation (LWS) provides card maintenance functions such as PIN reset, certificate renewal, and cyber access card issuance.
- The operators of the Lifecycle Workstation (LWS) are called Card Management Agents (CMA) and are designated by the Role Administrator to administer card maintenance functions.
- The CMA can hold another role in the system (i.e. Sponsor or Issuer).
- There can be multiple CMAs per OPDIV.
- The CMA must receive the necessary approvals, review responsibilities and functions with role administrator, and obtain a PIV card before he/she can be granted LWS privileges.



Logging into LWS Software: Check Point VPN

- The LWS Operator begins by logging into the computer system using their **network** user name and password.
- Launch the Check Point VPN-1 SecuRemote Connection by clicking on the **key icon** located in the tray of the IWS desktop.
- Authenticate to the VPN with the user name and password provided by your training official.
- Click on **“Connect”** in the lower left hand side of the VPN popup screen.



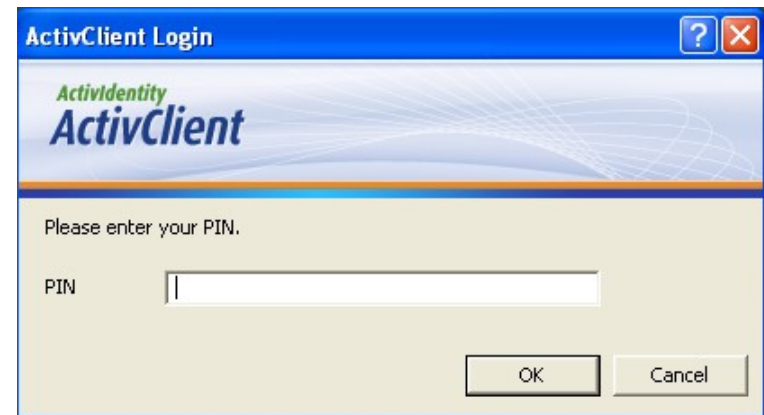
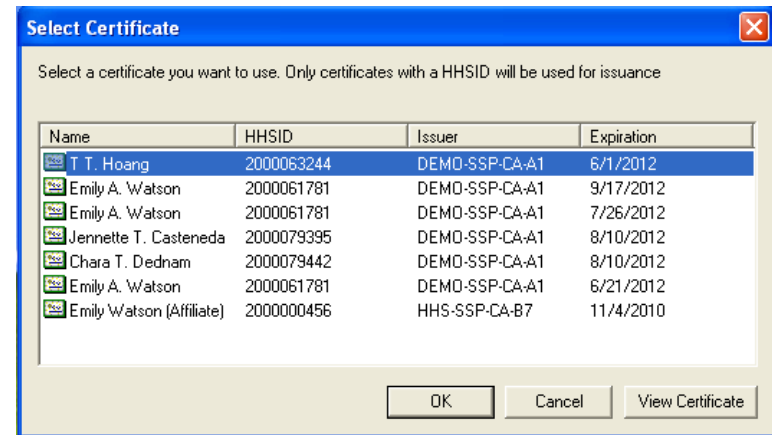
Check Point VPN

A screenshot of the 'Check Point VPN-1 SecuRemote Connection' dialog box. The window title is 'Check Point VPN-1 SecuRemote Connection'. The main area features the Check Point logo and the text 'Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.' Below this is a graphic of a laptop connected to a server via a cloud. The dialog has several input fields and buttons:

- Authentication** section:
 - User name: sbenami
 - Password: (empty)
- Connection** section:
 - Location Profile: 72.166.180.6
 - Destination: BearingPointInternet
 - Use Dial-up: (empty)
- Buttons: Connect, Cancel, Options


Logging into LWS Software: Authentication

- Place the Operator's PIV card into the LWS card reader.
- Click on the Card Issuance Station icon located on the desktop.
- The LWS Operator's certificates on their PIV card will appear on a list.
- Select LWS Operator's name from the list and select **"OK."**
- Enter the LWS Operator's PIN number and select **"OK."**



Logging into LWS Software: Location Selection

- Enter your location's ZIP code and select **“View Sites.”**
- Select your location and select **“OK.”**



Card Issuance Station

CIS

Version 2.4.3.0 (Production Version)
Copyright © 2008 Deloitte LLP. All rights reserved.
This program is protected by U.S. and International copyright laws.

Enter your location's 5-digit ZIP code, and press the "View Sites" button.

Select your current card issuance site:

| Name | Floor | Room | Address |
|---------------------|-------|------|---|
| Spring2 | 4 | 404 | 123 Main Court Suite 400, Springfield, va 22150 |
| FDA-TEST | | | 6564 Loisdale Court, Springfield, VA 22150 |
| FDA ISSUANCE - TEST | | | 6564 Loisdale Court, Springfield, VA 22150 |
| FDA_CIS_2_4_2_0 | | | 6564 Loisdale Ct, Springfield, VA 22150 |
| Cert. Main. WS | | | 6564 Loisdale Ct, Springfield, VA 22150 |



PIN Reset

PIN Reset Overview

A Personal Identification Number (PIN) Reset must be performed if a cardholder “locks” their PIV card by entering an invalid PIN more than the allowed number of retries. Likewise, the PIN Reset function can be performed to reset a forgotten PIN.



PIN Reset Process

- Enter cardholder PIV into the appropriate card reader.
- Select **“PIN Reset”** and select **“Continue.”**

The screenshot displays the 'Maintenance Workstation' interface. At the top left, it shows 'GIS 2.4.3.0 Production Version'. A search bar contains the text 'watson' with a 'Search' button to its right. Below the search bar is a table with the following data:

| HHSID | Full Name | Agency | Email |
|------------|-----------------|--------|-----------------------|
| 2000061781 | Emily A. Watson | NIH | emily.watson@work.com |

Below the table, a confirmation box displays the following information:

Emily A. Watson
Exp: 20141221
NIH
HEALTH & HUMAN SERVICES (HHS)
OK to continue.

To the right of the confirmation box is a small portrait photo of a woman. Below the photo is a 'Continue' button. At the bottom of the interface, there are two buttons: 'PIN Reset' on the left and 'Exit' on the right.

PIN Reset Process: Verifying Biometrics

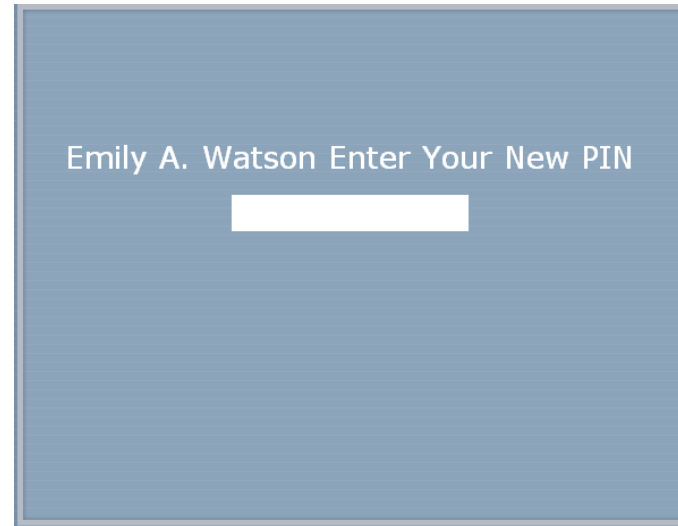
- Ask the cardholder to place their right or left index finger on the verifier and select the corresponding radio button.
- Select **“Go Live”** and then **“Capture and Match”** when the cardholder’s fingerprint is visible on the screen.
- If the first match fails, attempt to match the cardholder’s second reference biometric following the same steps as above.
- Ensure that the reference fingers listed on the screen correspond to the fingers being placed on the verifier.
- The fingerprint verification match score is displayed, select **“OK.”**
- The fingerprint is verified.



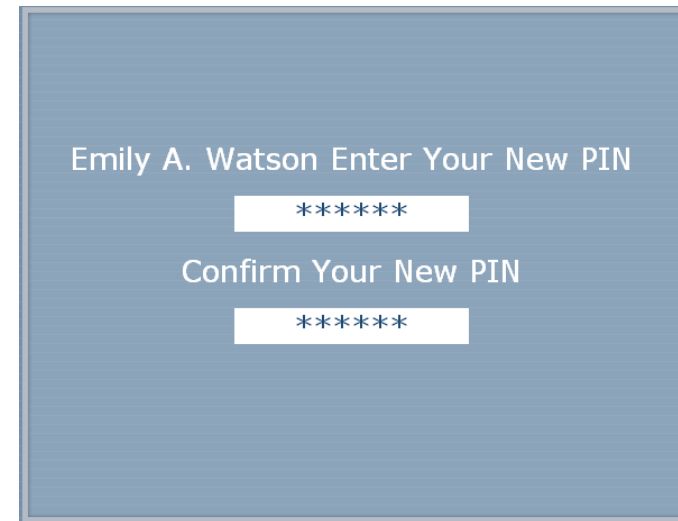
PIN Reset Process: PIN Creation

- The cardholder creates a new numerical PIN between 6 and 8 digits long.
- The cardholder types this PIN into the corresponding field using the numeric PIN pad.
- The cardholder must enter their PIN again for verification.
- The Issuer clicks the **“Enter”** button on the workstation’s keyboard.

Note: *It is important that the cardholder remembers this PIN as it will be required when using the PIV card*



Emily A. Watson Enter Your New PIN



Emily A. Watson Enter Your New PIN

Confirm Your New PIN

PIN Reset Process: PIN Creation

- When completed, you will receive a message stating the PIN reset was successful.
- After the cardholder's PIN has been reset, the Issuer can start over with another applicant by clicking the **“Start Over”** button.

Press Start Over to perform another operation or Exit to close the application.



Certificate Renewal

Certificate Renewal Overview

FIPS 201 allows PIV cards to be valid for up to five years. However, current HHS PKI policy only allows certificates to be issued for a maximum of 30 months. This discrepancy necessitates the need for certificates to be renewed (replaced) prior to PIV card expiration.

Certificate renewal can be performed by a Card Management Agent at a LWS.



Certificate Renewal Process: Searching for the Cardholder

- Type in the cardholder's last name or HHS ID into the search field and select **“Search.”**
- Select the cardholder's name and select **“Continue.”**

CIS
2.4.3.0
Production Version

Maintenance Workstation

watson

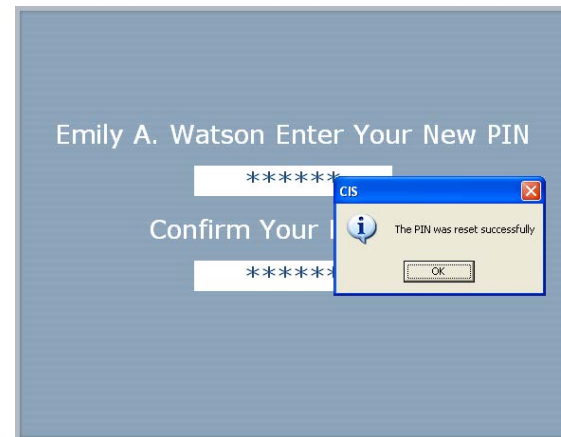
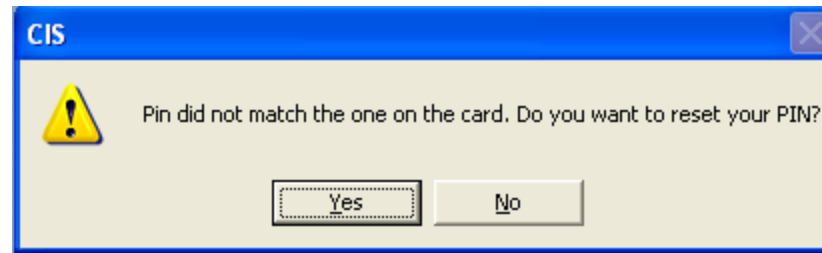
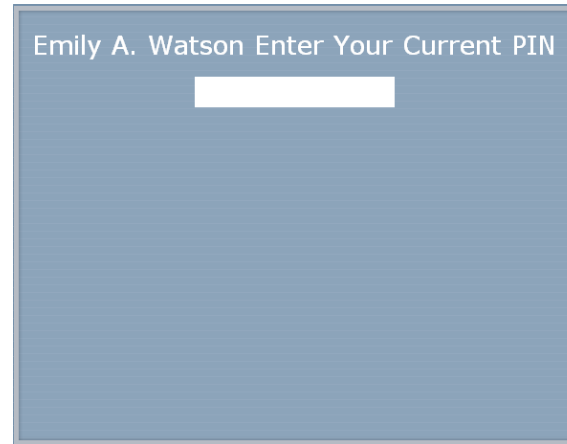
| | | | |
|------------|-----------------|--------|-----------------------|
| 2000060354 | Dennis Watson | NIH | |
| 2000060387 | Emily A. Watson | FDA | |
| 2000060395 | Emily A. Watson | FDA | |
| 2000061167 | Denny Watson | NIH | |
| 2000061206 | Emily Watson | OS | ewatson@deloitte.com |
| 2000061222 | Emily Watson | SAMHSA | |
| 2000061239 | Emily Watson | OS | EWATSON@DELOITTE.COM |
| 2000061298 | Abby Watson | AHRQ | |
| 2000061781 | Emily A. Watson | NIH | emily.watson@work.com |
| 2000063783 | Testone Watson | FDA | ewatson@deloitte.com |

Emily A. Watson
Exp: 20141221
NIH
HEALTH & HUMAN SERVICES (HHS)
OK to update card.



Certificate Renewal Process: PIN

- Have the cardholder enter their current PIN.
- If the cardholder enters an incorrect PIN, they will be asked if they would like to reset their PIN.
- Have the cardholder create a new PIN and type in again to confirm.
- A message will indicate that the PIN was reset successfully.



Certificate Renewal Process: Verifying Biometrics

- Ask the cardholder to place their right or left index finger on the verifier and select the corresponding radio button.
- Select **“Go Live”** and then **“Capture and Match”** when the cardholder’s fingerprint is visible on the screen.
- If the first match fails, attempt to match the cardholder’s second reference biometric following the same steps as above.
- Ensure that the reference fingers listed on the screen correspond to the fingers being placed on the verifier.
- The fingerprint verification match score is displayed, select **“OK.”**
- The fingerprint is verified.



Certificate Renewal Process

- Select “**Start**” to begin the certificate update.
- When process is complete, the user agreement will appear.
- Instruct the cardholder to read the agreement carefully.

The screenshot displays the 'Issue Card' and 'Digital Signature' screens of the certificate renewal process. The 'Issue Card' screen on the left features a 'Start' button at the top, a list of steps (Initialize, Connect, Request, Encode, Disconnect) on the left, and a 3D rendering of a white PIV card with a green stripe and a yellow chip on the right. The 'Cardholder Information' section on the right includes a photo of a woman and the following details: Full Name: Emily A. Watson, Department: HEALTH & HUMAN SERVICES (HHS), and Affiliation: NIH. A 'Cancel Operation' button is located at the bottom right of this section. The 'Digital Signature' screen on the right has a title 'Digital Signature' and a heading 'Please read the following information carefully'. The main content area contains the following text:

Health and Human Services (HHS)

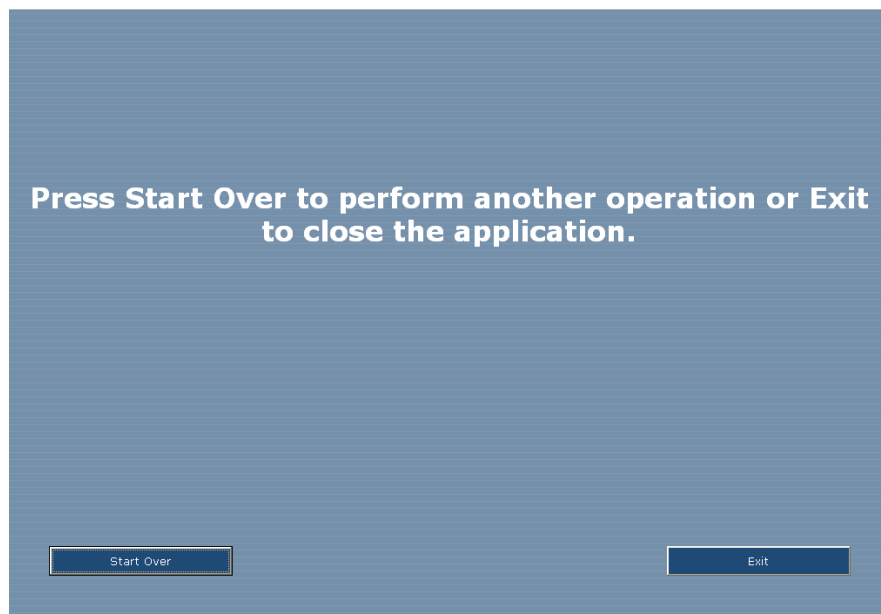
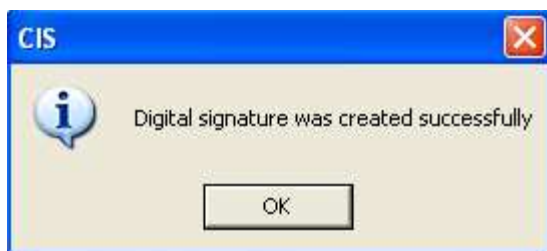
You have been authorized to receive one or more digital credentials (PKI certificates) associated with private and public key pairs. If you are receiving a PIV card, these PKI certificates are contained on your PIV card. If you are not receiving a PIV card, these PKI certificates are being provided on portable media and you will need to transfer these certificates into approved HHS storage, e.g., browser of your workstation, desktop, laptop, etc. At a minimum, these key pairs enable you to electronically identify yourself for systems access. Additional key pairs may enable you to digitally sign documents and messages and perform encryption/decryption functions.

Acknowledgement of Responsibilities: I acknowledge receiving my PIV card and/or digital certificates and will comply with the following obligations:

- I will accurately represent myself in all communications with the HHS issuing authorities, to include sponsor, authorizing official, enrollment officials, and issuance officials;
- I will comply with the instructions described to me today for selecting a Personal Identification Number (PIN) or other required method for controlling access to my private keys and will not disclose same to anyone, leave it where it might be observed, nor write it on the token itself;
- I will protect the contents of my PIV card at all times, by treating my PIV card as valuable personal property and keeping my PIN from disclosure as described above;

Certificate Renewal Process

- If the cardholder agrees, select **“Agree”** and have them enter their PIN number.
- A message will display indicating that the digital signature was created successfully.
- The certificate renewal is complete.





Alternate Logon Token (ALT) Issuance

ALT Issuance: Search

Deloitte Card Management Client
2.4.7.12
Production Version

Lifecycle Workstation

Enter Last Name or HHSID

Deloitte Card Management Client
2.4.7.12
Production Version

Lifecycle Workstation

Enter Last Name or HHSID

| HHSID | Full Name | Agency | Email |
|------------|------------|--------|--------------------|
| 2000124268 | John Smith | CDC | testhhs2@gmail.com |

| HHSID | Full Name | Agency | Email |
|------------|------------|--------|-------|
| 2000124276 | Jane Smith | CDC | |

Jane Smith
Card Exp: 2014JAN01
Cert Exp: 01-JAN-2014
CMS
HEALTH & HUMAN
OK to issue logical access card.

TEST
PHOTO

Continue

Continue

- Type in the cardholder's last name or HHS ID into the search field and select **"Search."**
- Select the cardholder's name and select **"Continue."**

ALT: Verify



- Ask the cardholder to place their right or left index finger on the verifier and select the corresponding radio button.

- Select **“Go Live”** and then **“Capture and Match”** when the cardholder’s fingerprint is visible on the screen.

- The fingerprint verification match score is displayed, select **“OK.”**

ALT: PIN



- The cardholder creates a new numerical PIN between 6 and 8 digits long.
- The cardholder types this PIN into the corresponding field using the numeric PIN pad.
- The cardholder must enter their PIN again for verification.
- The Issuer clicks the **“Enter”** button on the workstation’s keyboard.

Note: It is important that the cardholder remembers this PIN as it will be required when using the card

ALT: Encode

Issue Card

Start

Initialize
Connect
Request
Encode
Disconnect

Cardholder Information

TEST PHOTO

Full Name
Jane Smith

Affiliation
CMS

Primary SMTP
jane.smith@cms.gov

UPN
smith.jane@cms.local

Certificate Expiration Date
01-JAN-2014

Cancel Operation

SEARCH VERIFY PIN ENCODE SIGNATURE FINISH

Deloitte Card Management Client
2.4.7.12
Production Version

Select
“Start” to
begin the
certificate
update.

ALT: Digital Signature

Digital Signature Cardholder Information

Please read the following information carefully

Health and Human Services (HHS)

You have been authorized to receive one or more digital credential certificates associated with private and public key pairs. If you receive a PIV card, these PKI certificates are contained on your PIV card. If you receive a PIV card, these PKI certificates are being provided on and you will need to transfer these certificates into approved HHS browser of your workstation, desktop, laptop, etc. At a minimum, it enable you to electronically identify yourself for systems access. pairs may enable you to digitally sign documents and messages and encryption/decryption functions.

Acknowledgement of Responsibilities: I acknowledge receiving my PKI digital certificates and will comply with the following obligations:

- I will accurately represent myself in all communications with the authorities, to include sponsor, authorizing official, enrollment, issuance officials;
- I will comply with the instructions described to me today for my Identification Number (PIN) or other required method for controlling access to my private keys and will not disclose same to anyone, leave it where it might be observed, nor write it on the token itself;
- I will protect the contents of my PIV card at all times, by treating my PIV card as valuable personal property and keeping my PIN from disclosure as described above;

Primary SMITH
UPN
smith.james@cdc.gov
Certificate Expiration Date
01-JAN-2014

SEARCH VERIFY PIN ENCODE SIGNATURE FINISH


Deloitte Card Management Client
2.4.7.12
Production Version

Enter Your PIN

James Smith Enter your PIN

PIN

Deloitte Card Management Client

 Digital signature was created successfully

Press Start Over to perform another operation or Exit to close the application.

- Applicant selects **“I Agree”**
- Enters PIN and selects **“OK”**
- Select **“OK”**



Alternate Logon Token (ALT) Recycle

ALT Recycle: Search

Deloitte Card Management Client
2.4.7.12
Production Version

Lifecycle Workstation

Enter Last Name or HHSID

Select
**“Recycle
Cards”** to
remove any
remaining
certificates and
prepare the
card for
issuance.

Recycle Cards

PIN Reset

Recycle Cards

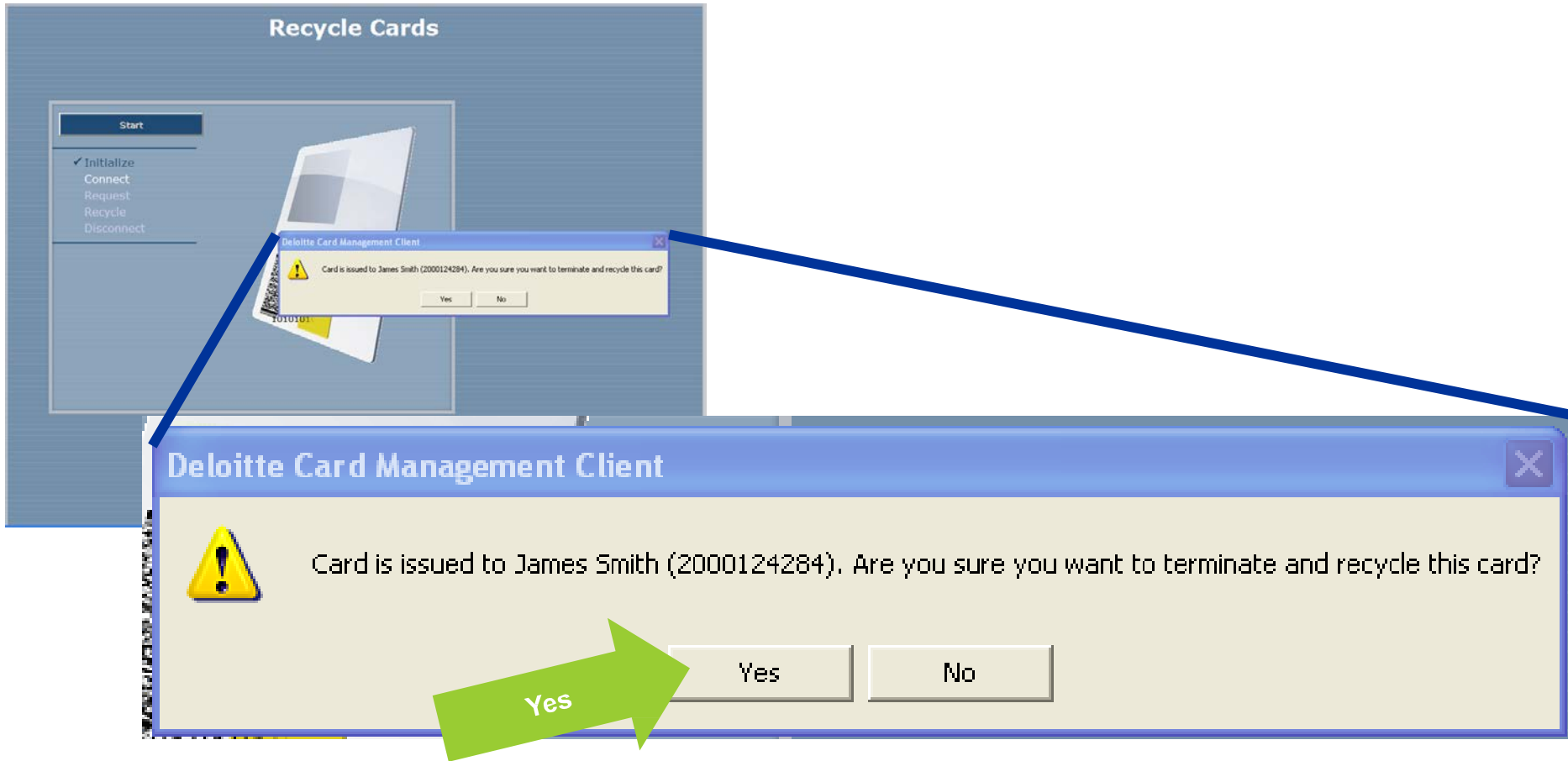
Exit

ALT Recycle



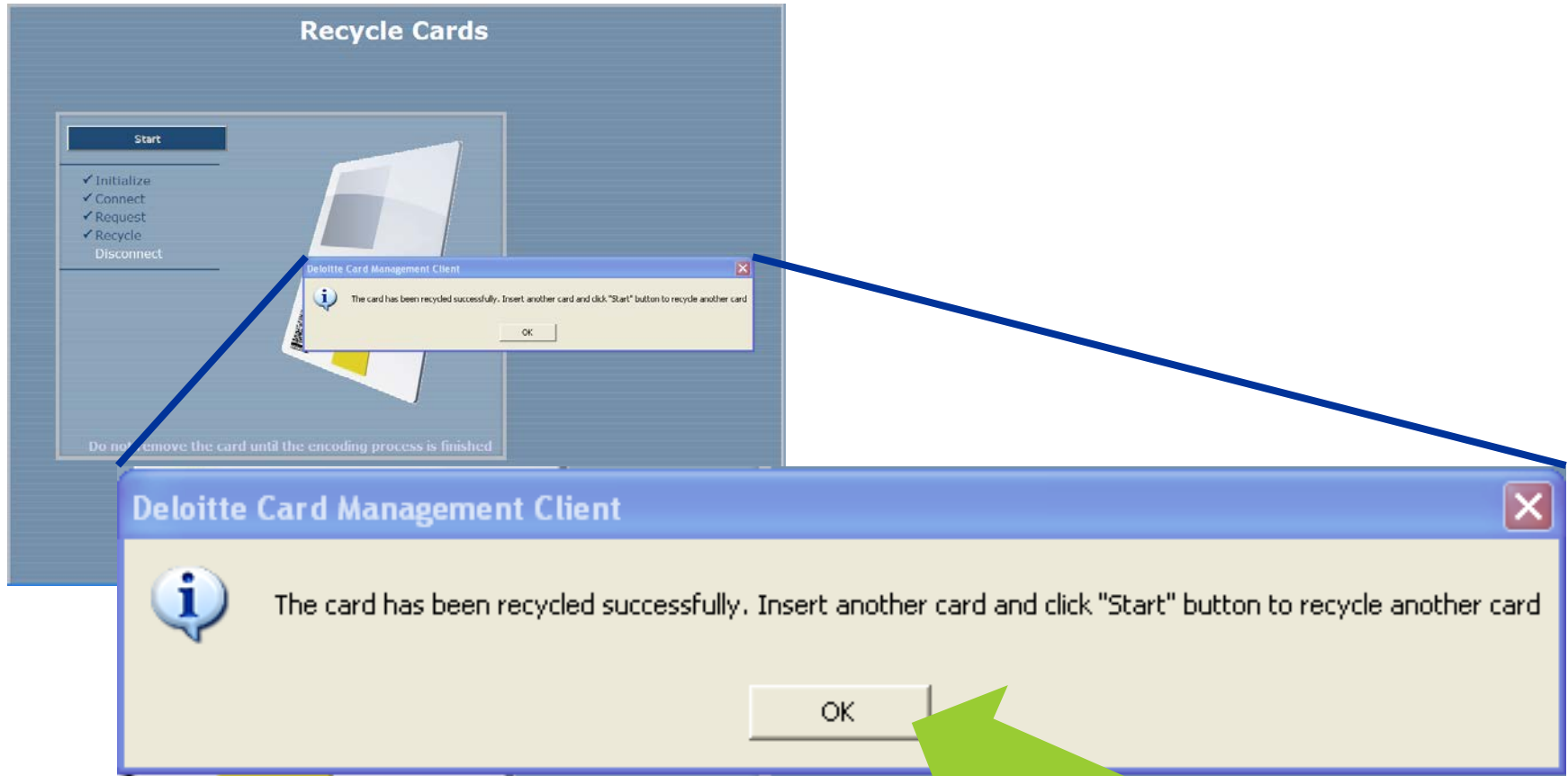
Select **“Start”** to begin recycling the card

ALT Recycle



- Once recycling begins, it will warn you if the card is issued to another user.
- Select **“Yes”** to terminate and recycle the cardstock.

ALT Recycle



- Once complete, a new window will notify that the card has been successfully recycled and ready for issuance.
- Select **“OK”** to return to the IWS to recycle another card.