



# Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

## 1. What is the difference between Badge Renewal and Smartcard Certificate Update?

A badge nominally has a 5-year lifetime. When the badge is near expiration, a **Badge Renewal** process is triggered, which requires the badge holder to go to the badging office to get a replacement badge. The badge has digital certificates on it, which have up to a 3-year lifetime. Badges will typically need a **Smartcard Certificate Update** once during the lifetime of the badge, up to 60 days prior to the expiration of the initial 3-year certificates that were issued when badge was first received.

## 2. Why does my smartcard need to have certificates updated?

Per regulations, a user's certificates on the badge are limited to 3 years. A badge will need to have updated certificates encoded before the current certificates expire. Your PIV authentication certificate needs to be current, and not expired, for use with NASA systems and applications that require smartcard login.

## 3. How will I know if my PIV certificate is about to expire?

NASA's IDMAX system will send expiration warning notifications to the card holder starting at 60 days before the current badge certificates are due to expire.

## 4. What are the options for getting a Smartcard Certificate Update?

Smartcard certificate update is supported on most Windows systems with ActivClient 7 installed. Mac and Unix systems users will need to get either temporary access to a properly configured Windows system or go to the center badging office to have their card updated.

## 5. If for some reason there are issues while performing the automatic certificate update procedure, whom do I contact?

Please call the ESD @ 1-877-677-2123.

## 6. Do I need to know my smartcard PIN to perform the Smartcard Certificate Update?

Yes. If you do not know the PIN, you will need to go to the Badging Office for a PIN reset.

## 7. Where is my Center Badging Office?

See PIV Badge PIN Reset (Badging Office Information) page for details of center locations and support hours. (<https://icam.nasa.gov/documents/11201/55651/Badging+Offices+By+Center.docx/ce84d199-3ee8-647d-e554-14ca5d324634>).

## 8. What will I be unable to do, if my smartcard authentication certificate expires?

Once your smartcard authentication certificate expires:

- You will not be able to login or unlock your Windows system with your smartcard, however your NDC AUID/password will continue to work if you have a PIV logon exemption
- You will not be able to log into web applications that require smartcard login



## Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

### 9. What configuration is needed on my system after I receive a New Badge or after a Smartcard Certificate Update is performed?

Here are some important action items you need to be aware when getting a new card or updated certificates on an existing card:

- The first desktop smartcard login with a new card, or after the card has been updated, must occur while the computer is connected to the internal NASA network.
- Those with a NASA MDM managed mobile device **MUST** re-enroll the device in MDM once the badge is updated with new certificates, or a replacement badge is received. Additional information on that process can be found on the Mobile Device Registration FAQ: <https://mdr.nasa.gov/faqs>
- Mac users that use email Signing and Encryption **MUST** manually reconfigure Outlook for Mac to use the latest certificate on the card. See item #12 in this FAQ for Mac Outlook reconfiguration instructions.
- Windows users, the reconfiguration of Outlook to use the latest certificates for encrypted emails is automatically configured by Entrust; no action is required. To clear the previous cached certificates to prevent them from showing up when using browsers, run the “**PIV Cache Cleaner**” application found in ICAM folder under All Programs on NDC Windows systems, then reinsert your updated smartcard.

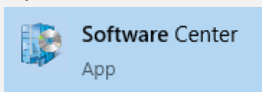
### 10. Can I perform a Smartcard Certificate Update remotely?

Yes, for remote users, it is advised to access the VPN before completing the PIV smartcard remotely. Once you are on the VPN you will be able to run the Self Service PIV Updater utility. Refer to question 11 for complete instructions.

### 11. How do I use Windows to perform a Smartcard Certificate Update?

For a card update procedure to succeed there must be a card update already pending for your badge. You would have been notified by IDMAX that an update is needed to your card. If you received such a notification and if you are using a EUSO managed Windows computer, you can perform the update by the following steps:

- Open Software Center from the Start Menu



- Find PIV Updater and click on the icon





# Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

- Click Install

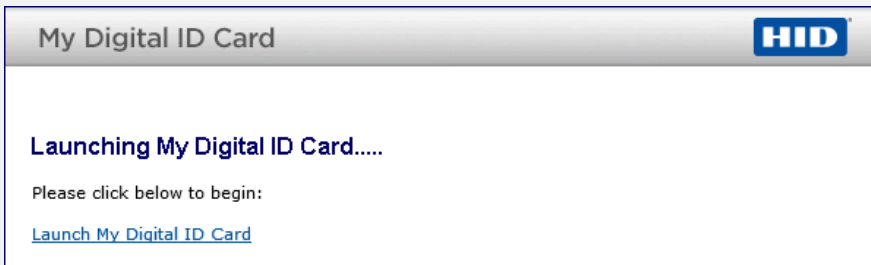


PIV Updater  
Published by CSET

**Install**

Application for updating PIV certificates. PIV is the standard badge for full time employees and contractors.

- PIV Update website will open automatically, click *Launch My Digital ID Card*



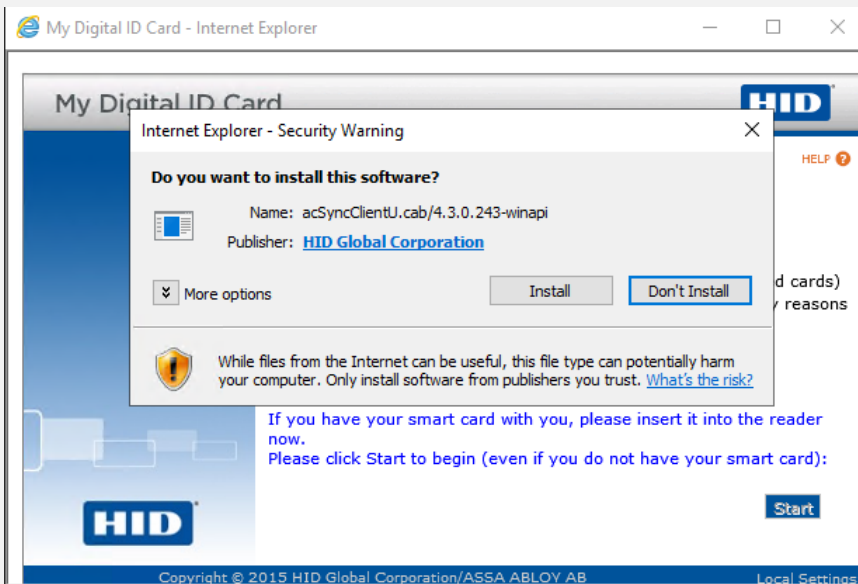
My Digital ID Card **HID**

Launching My Digital ID Card.....

Please click below to begin:

[Launch My Digital ID Card](#)

- Click Install



My Digital ID Card - Internet Explorer

My Digital ID Card **HID**

Internet Explorer - Security Warning

Do you want to install this software?

Name: acSyncClientUI.cab/4.3.0.243-winapi  
Publisher: [HID Global Corporation](#)

More options

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. [What's the risk?](#)

If you have your smart card with you, please insert it into the reader now.  
Please click Start to begin (even if you do not have your smart card):

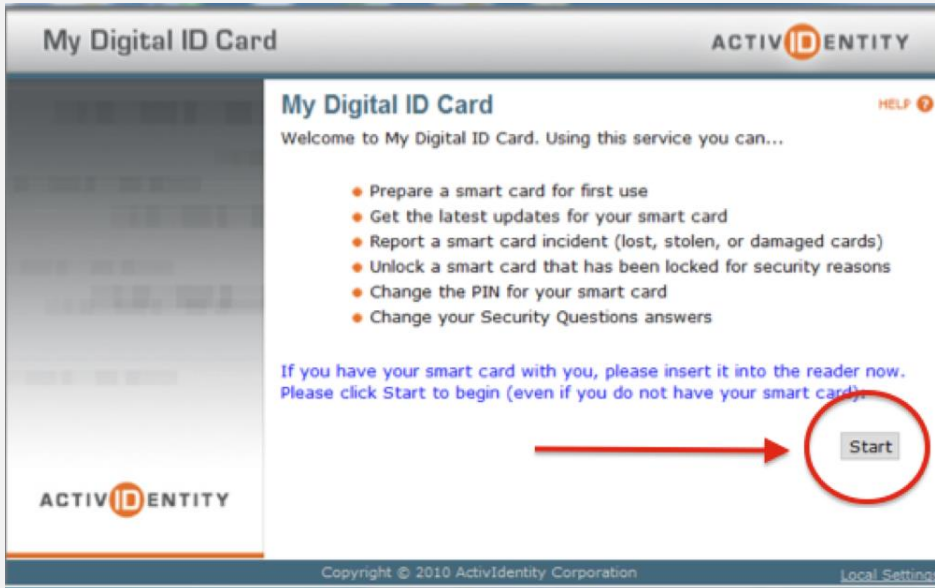
**Start**

Copyright © 2015 HID Global Corporation/ASSA ABLOY AB Local Settings

## Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

- Click **“Start”**. If you cannot see the **“Start”** button, this is due to the zoom level of Internet Explorer being too high. To correct reduce the zoom level, by pressing the **“Control”** and minus **“-“** key at the same time.



- Enter your PIN, click Continue



- The Card Management System will then perform the smartcard update until complete. It typically takes about 5 to 10 minutes. **Wait patiently** - Do not remove the smartcard until the utility completes.
- Once complete click **“Done”**. If you experience a failure, schedule an appointment with your local badging office to assist you in fixing your PIV card or you can try to complete the following:
  - If another card update is required due to a failure, you can use the PIV Updater application to relaunch the smartcard update process to the Card Management System (CMS). To run the application a second time, simply click Uninstall on the PIV Updater application. Once uninstalled,

## Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

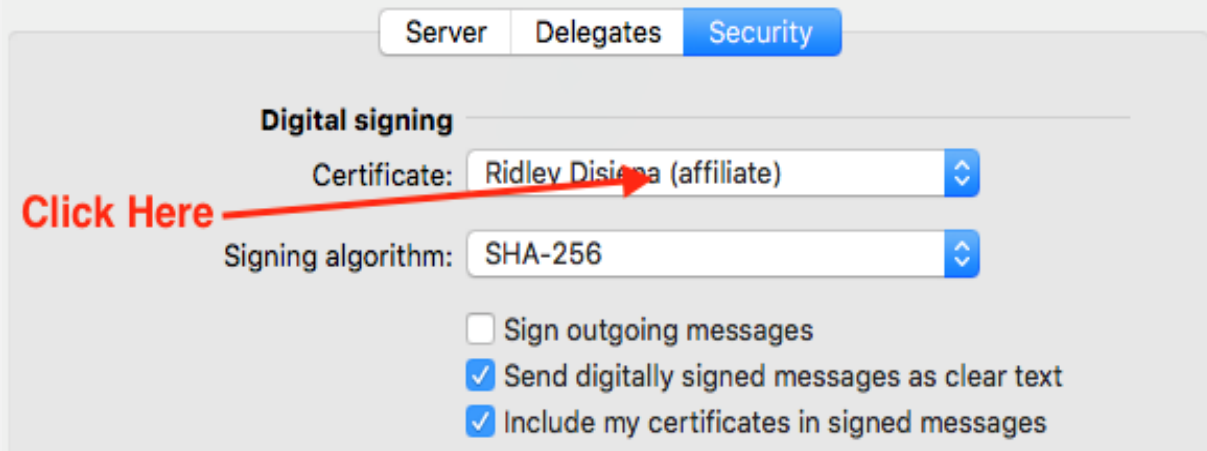
click **Install**, the interface to the CMS website will launch automatically and you will be able to perform the required steps again.

- **Laptop Users:** After updating the certificate on the smartcard, an updated cached credential needs to be stored so the smartcard can be used when the network is not available. While still connected to the NASA network either directly or via VPN, screen lock your system and log back in with your updated smartcard prior to disconnecting from the network and logging off the VPN. This ensures your new credential is cached. Failure to do so will keep you from being able to logon to your laptop until you return back to a NASA Center. This can and should be performed as soon as the card update is complete.

### 12. How do I reconfigure Outlook for Mac to use my new certificates?

With your card in the reader, Launch Outlook for Mac:

- Select **Tools**, then **Accounts**. In the Accounts window, click on the **Advanced** button and select the **Security** Tab.
- To configure the signing certificate, click on the Certificate pop-up under the **Digital signing** section and select your certificate.
- To select your Signing certificate, click on the **Certificate** dialog under the Digital signing section.



- Click the **Choose a Certificate**. The signing certificate will likely be the second one listed, but to verify that it is the correct certificate, click **Show Certificate**. Scroll about halfway down in the certificate details to the **“Extension Key Usage”** section and verify that it lists usage of **“Digital Signature, Non- Repudiation”**. Only the correct certificate will show that certificate usage. Once that correct certificate is selected, click

# Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

OK.

The screenshot shows the 'Accounts' window with the 'Security' tab selected. The 'Digital signing' section is active, and the 'Choose An Identity' dialog is open. The dialog shows a list of certificates for 'Ridley Disiena (affiliate) (U.S. Government)'. A red box highlights the 'Key Usage ( 2.5.29.15 )' extension with 'Critical YES' and 'Usage Digital Signature, Non-Repudiation'. A red arrow points to the 'OK' button. Text overlays include 'Scroll about halfway down' and 'Find Key Usage: Correct cert will have Non-Repudiation'.

- Set the **Signing algorithm** to SHA-256 and check the boxes for **Send digitally signed message as clear text** and **Include my certificates in signed messages**
- To select your Encryption certificate, click on the **Certificate** dialog under the **Encryption** selection and select your encryption certificate. You may see more than one certificate listed. It should be the topmost choice. To verify you may click "Choose a Certificate" and Show Certificate to see certificate details. Pick the certificate with the latest expiration date.
- Set the **Encryption algorithm** to AES-256



## Smartcard Certificate Update and New Badge FAQ

Last Updated: 03/17/2020

- Do not select a **Client authentication** certificate, it should show “**None Selected**”. The security Configuration tab should look like this when the configuration is complete. Click OK,

Server Delegates **Security**

**Digital signing**

Certificate: Ridley Disiena (affiliate)

Signing algorithm: SHA-256

Sign outgoing messages

Send digitally signed messages as clear text

Include my certificates in signed messages

**Encryption**

Certificate: Ridley Disiena (affiliate)

Encryption algorithm: AES-256 (more secure)

Encrypt outgoing messages

**Certificate authentication**

Client certificate: None Selected

Cancel OK

- Outlook is ready to use your recently updated certificates.