RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Prescribing of Controlled Substances

(BEPC)

EPCS Token Acquisition and Provisioning Guide

Version 1.0
August 2019

Office of Information Technology
Division of Information Resource Management

Table of Contents

Document Revision History

Version	Date	Author	Description	Sections
1.0	8/2019	GDIT SESS team	Initial Release	All

1.0 Introduction

Purpose of This Guide

The Electronic Prescribing of Controlled Substances (EPCS) project implements the Drug Enforcement Administration (DEA) regulations that give providers the ability to electronically prescribe outpatient controlled substances, whether the orders are sent to the local Outpatient Pharmacy at the site or electronically transmitted to Surescripts.

The regulations require each provider to be individually configured with specific information, such as the number that gives them the authority to prescribe controlled substances (DEA or Department of Veterans Affairs [VA] number), any schedules for which they can or cannot prescribe, and the authorization to electronically prescribe controlled substances.

In addition, two-factor authentication for both provider credentialing and the digital signing of controlled substance prescriptions must be instituted at the site. This second factor of authentication is performed with a cryptographic token.

This guide is intended to assist sites and individuals with the acquisition and provisioning of the devices required for two-factor authentication and digital signing.

2.0 Tokens

2.1 What Is a Token

A token is a physical device that can be used to confirm an individual's identity. For two-factor authentication and digital signing in the Resource and Patient Management System (RPMS) Electronic Health Record (EHR) application, these tokens take the form of either a standard Personal Identity Verification (PIV) card or a USB (Universal Serial Bus) device containing a SIM (Subscriber Identity Module) chip that stores certificates. A personal identification number (PIN) must be entered to use the token for digital signing.

2.2 Approved Tokens

The EPCS application has been certified for use with only the following three tokens:

1. PIV cards issued through the Indian Health Service (IHS) that contains certificates issued by the Health and Human Services Federal Public Key Infrastructure (HHS-FPKI). This is the standard PIV card issued to IHS employees and contractors.

2. IdenTrust USB Token: An HID ActivKey SIM (HID USB Token) with an IGC Basic Assurance Unaffiliated Hardware 2 Year Certificate issued by the third-party credential service provider (CSP) IdenTrust.

3. WidePoint ORC USB Token: An HID ActivKey SIM (USB Cryptographic Token) with a Certificate: 1 Year ECA Medium Token Assurance Identity/Encryption Certificate Pairs issued by the third-party credential service provider WidePoint ORC.

2.3 Who Needs a Token

There are two types of users who will need to have a token:

- Providers who will issue and digitally sign controlled substance orders that will be electronically submitted to a pharmacy.
- Users serving in the Provider Access Administrators role. These are the users who will use two-factor authentication to verify that a provider meets the qualifications to electronically prescribe controlled substance orders.

Users serving in both the Provider and Provider Access Administrator roles do not need separate tokens but can use the same token for both roles.

A provider working at multiple sites may not need to obtain multiple tokens. A provider who works at multiple sites may use the PIV card for EPCS at all the sites as long as each site has card readers that are able to read the PIV card. Likewise, a provider that works at multiple sites may use the same USB cryptographic token for EPCS at each of the sites as long as all sites will support the use of the USB ports. The provider will need to work with each site to determine if the token that they have will be supported at all sites where they work.

Finally, the certificates on the token are assigned to a specific individual and thus cannot be transferred from one user to another.

2.4 Choosing a Token

To simplify the process of acquiring and maintaining tokens, it is recommended that, if possible, sites pick only a single token type for two-factor authentication and digital signing. However, there is no requirement that only a single type be used, and any combination of approved tokens may be used at a site.

There may also be circumstances where a site decides to use multiple tokens types. For instance, a site may use PIV cards for staff who already have them but also acquire USB Cryptographic tokens for temporary employees who may not be issued a PIV or for staff who are waiting for a PIV to be issued.

For sites where staff already possess a PIV card and computer systems are equipped with card readers, this is the simplest and most cost-effective option since the issuance and maintenance procedures will already be instituted. However, PIV cards are only available to IHS employees and contractors. Personnel at non-federal sites will not be able to obtain a PIV.

For sites that will acquire USB cryptographic tokens for some or all users, the site will need to acquire tokens from one or both of the two approved USB token providers listed in Section 2.2. Sites will need to research both USB token providers to determine which USB token to purchase. Factors used to determine which token to acquire should include cost, renewal period of the certificates on the token, acquisition option, and identity-proofing process. Sections 4.0 (IdenTrust) and 5.0 (ORC) of this document include additional information on the processes for acquiring tokens and certificates for each CSP, which may be helpful for the site's decision-making process.

The contact information for both CSPs follows:

- IdenTrust
  6623 Dumbarton Circle
  Fremont, CA 94555
  (415) 486-2900
  https://identrust.com

- IdenTrust product literature: https://www.identrust.com/sites/default/files/resources/identrust-igc-basic-assurance-unaff-hw-cert-ds-en_5.pdf
- WidePoint Cybersecurity Solutions Corporation (formerly ORC, Inc.)
  11250 Waples Mill Road
  South Tower, Ste 210
  Fairfax, VA 22030
  800-816-5548
  https://www.orc.com
- ORC product literature: https://eca.orc.com/pricing/

2.5 Acquiring and Preparing USB Cryptographic Tokens

The acquisition and preparation of PIVs will continue to use existing Homeland Security Presidential Directive 12 (HSPD12) processes. The rest of this section is for those sites that will use USB cryptographic tokens for some or all of the site users. The general process for acquisition and preparing USB cryptographic token is:

1. Purchase tokens.
2. Distribute tokens or vouchers to the users.
3. Users follow vendor-specific instructions for identity proofing and to acquire certificates.
4. Site administrators prepare workstations for USB Token use. This step can happen concurrently with the previous three steps.
5. Users load certificates onto USB Tokens.

These steps may be completed prior to the installation and configuration of the EPCS software. In that way, the users can be configured to use EPCS as soon as EPCS is available.

2.5.1 Acquisition and Distribution

Detailed instructions for procuring USB tokens, including web links and prices, are provided in Sections 4.0 and 5.0 of this document. If tokens or vouchers are purchased by the area's or site's acquisition team, the tokens or vouchers will need to be distributed to the users.

The vendors for cryptographic tokens will provide generic documentation that outlines how individuals acquire a cryptographic token. To assist providers with setting up their tokens, each site should consider modifying or augmenting the generic documentation with additional information, such as site-specific contacts, a site-specific URL provided by the portal, site branding, and any other site-specific information.

As all tokens are identical in appearance, each site should consider labelling the tokens in some manner (e.g., affixing a label or using a permanent marker) to identify the provider to whom the token belongs.

2.5.2 Obtaining Certificates

USB tokens do not initially contain any certificates. After doing some form of identity proofing, the signing certificate is provided by the vendor. Like the purchasing of tokens, the process of identity proofing, obtaining certificates, and installing certificates is also vendor specific. This information should be provided by the vendor when the tokens are purchased. See Sections 4.0 and 5.0 of this document for more information.

2.5.3 Prepare Workstations for USB Token Use

This does not need to be done by individual users but will need to be done by site administrators to prepare the workstations that will either provision and/or will read the tokens.

- Obtain and install the Certificate Authority Trust Anchor.
- Prepare workstations to read from a USB Token.
- Install HID ActivClient software.

The process to do these items is documented in Section 6.0.

2.5.4 Load Certificate onto the Token

Using the vendor-supplied instructions, each user will need to load the certificate onto their token.

2.6 Assign Digital Signing Certificates to Users in RPMS

The signing certificate on the PIV or the USB cryptographic token will need to be associated to the user in the RPMS using the EHR application. If a provider works at multiple sites, the token will need to be assigned to the user at each of the RPMS databases where the user works. This process is done after the EPCS Software is installed and configured and is not covered in this manual. This is discussed in more detail in the *EHR-EPCS Supplemental User Guide* (patch 25).

3.0 Token Maintenance and Lifecycle

3.1 Custodian

If a site is handling the purchase of the USB cryptographic devices, the site will need a way to track the distribution of the initial USB cryptographic devices as well as replacement of misplaced or damaged devices and device acquisitions for new staff. Sites may also want to also assist their users for the initial administration and renewal of certificates. It is recommended that sites using USB cryptographic devices assign a staff member as a "custodian" to track these events and ensure that prescribers maintain the ability to prescribe controlled substances electronically.

Since a user can use the same token at multiple sites, the token should be tracked by the site that issued the token to the user, which may be the user's primary site or the first of the sites where the provider works that becomes EPCS enabled.

3.2 Certificate Renewals

The certificates on a USB token will expire after one to two years, depending on which CSP is used. When a certificate nears its expiration the certificate issuer should contact the individual to whom the certificate was issued, with instructions for renewal. However, it is highly recommended that a custodian monitors upcoming certificate expirations to ensure renewals occur in a timely fashion.

For both digital signing certificate on a PIV or USB token, it is important that the individual work with the EPCS Provider Profile Admin and EPCS Provider Access Admin to register the new certificate in RPMS before the old certificate expires. Otherwise the EPCS application will attempt to use the old certificate to sign, and the signing attempt will fail once the old certificate expires.

3.3 When a Token Holder Departs or Is Terminated

For sites using PIV cards, the handling of the departing individual's PIV card and associated certificates will follow existing HSPD12 processes.

The individual's EPCS profile in the RPMS database should be deactivated immediately. See the *EHR-EPCS Supplemental User Guide* for more information on this process.

3.3.1 Single-Site Providers with a USB Token

Cryptographic tokens are tied to a single user and cannot be reissued to another user. If a provider will no longer work at a site, consider one of the following approaches:

- Let the provider retain the token and remove the token from the site's inventory. The provider may have a use for the token at another location.

- Reclaim the cryptographic token and physically destroy it per site and/or OIT policy.

3.3.2 Multi-Site Providers with a USB Token

If a provider will no longer work at what is considered the provider's primary site, the primary site should consider transferring the token to the provider's new primary site to become part of its inventory record. It will be up to the last site a provider works with to determine whether to reclaim the token or let the provider retain the token.

3.4 When a Token Is Inoperative

If a token becomes inoperative due to damage or internal failure it will need to be replaced. As part of incident response, sites will need to deactivate the individual's EPCS profile in the RPMS database until a new device can be acquired. See the *EHR-EPCS Supplemental User Guide* for more information on this process.

If the individual has retained possession of the inoperative device and its whereabouts are accounted for, it may be possible to replace the hardware and load the existing certificates onto the new device instead of revoking and replacing the certificates. This determination will be made by the organization responsible for the issuance of the device and certificate.

> **Note:** This option is only available if the provider has retained possession of the token and can account for its whereabouts. Otherwise, procedures for a lost or stolen device should be followed.

3.4.1 Inoperative PIV Card

Sites will need to use existing processes to contact the HSPD12 Team.

3.4.2 Inoperative USB Token – IdenTrust

The site will need to contact IdenTrust at Helpdesk@IdenTrust.com to explain the circumstances of the hardware token damage and to determine if a certificate revocation is necessary. IdenTrust will provide guidance on loading the existing or replacement certificates onto the replacement device.

3.4.3 Inoperative USB Token – WidePoint ORC

The site will need to contact ORC at pkihelp@orc.com to explain the circumstances of the damage to the device and to determine if a certificate revocation is necessary. ORC will provide guidance on loading the existing or replacement certificates onto the replacement device.

3.5 When a Token Is Misplaced

If a token is lost or stolen, and it is clear that the individual cannot account for its whereabouts or that the device will not be recovered, report the incident immediately to the site's designated incident response staff.

As part of the incident response, sites will need to deactivate the individual's EPCS profile in the RPMS database until a new device and certificate can be acquired. See the *EHR-EPCS Supplemental User Guide* for more information on this process.

Sites will also need to initiate the certificate revocation process for the certificates on the misplaced device.

3.5.1 Misplaced PIV Card

The site will need to use existing processes to contact the HSPD12 Team to submit a request to revoke the digital signing certificate. The issuance of a replacement device and certificates will follow established processes.

3.5.2 Misplaced USB Token – IdenTrust

The site will need to contact IdenTrust at Helpdesk@IdenTrust.com to initiate a request to revoke the digital signing certificate and replace the device and certificate.

3.5.3 Misplaced USB Token – WidePoint ORC

The site will need to contact ORC at pkihelp@orc.com to initiate a request to revoke the digital signing certificate and replace the device and certificate.

3.6 Unlocking a Locked Token

If an incorrect PIN is entered six time in a row, the token will become locked. The token is no longer usable until it is unlocked. There are two methods to unlock a token.

3.6.1 Use the Unlock Code

The documentation issued with the physical token includes an unlock code. Copy and properly escrow this code so that it is available in the event there is a need to unlock the token.

> **Note**: Neither IdenTrust nor ORC has a copy of this code nor a way to recover this code.

To unlock a token:

1. Go to a workstation that has ActivClient installed.

2. Insert the token into an available USB port.
3. Launch the ActivID ActivClient User Console:
    a. From the menu select **Tools**, **Unlock Card.**
    b. Follow the prompts and enter the unlock code.
    c. Once successfully unlocked, follow the prompts to set a new PIN.
    d. Memorize the new PIN and optionally escrow in a secure location.

3.6.2 Replace the Digital Certificate

The replacement process effectively wipes the token and re-downloads the certificates. This process can take up to a week and involves coordinating with the Credentialing Service Provider. To initiate the replacement process, contact the vendor and follow the directions provided.

- ORC help desk at ecahelp@orc.com or call (800) 816-5548
- IdenTrust help desk at support@identrust.com or call (888) 248-4447

3.7 Found Tokens

If a token has been found and there is no label on the token, the user can be identified by examining the certificates on the token, which includes the username and email address.

4.0 IdenTrust Tokens

This section is included as a reference for the acquisition and provisioning of IdenTrust tokens. This information, referenced documents, and referenced links are accurate at the time of the document's publication. However, any of this information and detail may become deprecated and changed by IdenTrust at any time without forewarning so adjustments to these procedures and instructions may need to be made.

4.1 Approved Product

The EPCS application completed DEA certification using the following IdenTrust product combination:

- USB Token: HID USB Token
- Certificate: IGC Basic Assurance Unaffiliated Hardware 2 Year Certificate
- Certificate Renewal Period: 2 years
- The IdenTrust product literature can be obtained at: https://www.identrust.com/sites/default/files/resources/identrust-igc-basic-assurance-unaff-hw-cert-ds-en_5.pdf

4.2 Purchasing New Tokens and Certificates

IdenTrust offers multiple options to acquire cryptographic tokens. Each site will need to determine which methods it wants to use to acquire the cryptographic tokens.

- Procurement staff at a site can bulk purchase vouchers using either a purchase order (PO) or credit card for the cryptographic tokens. The site will issue a voucher number to the provider to use to acquire a token.
- Individual providers may also pay for a token with a credit card at the time they register for a token. Sites will need to determine if they will require the use of an organizational credit card, reimburse the provider for the credit card purchase, or if the purchase will be an out-of-pocket charge for the provider. Sites will need to ensure that providers receive appropriate payment instructions.

These options can be reviewed under the IGC DEA Approved for EPCS Prescribing section of this link https://www.identrust.com/certificates-portfolio.

No matter which method is used, there is certain information that must be supplied to make sure that DEA certified solution is purchased.

- When selecting the certificate type, select **IGC Basic Assurance Unaffiliated Hardware 2 Year Certificate**. Since the options on this screen are similar, make sure you ***do not*** select either an Unaffiliated Software Certificate or Hardware Certificate w/ Mobile Authentication. Also, do not select a one-year or three-year certificate.
- When selecting the Hardware Type, choose the **HID USB Token**. Make sure you do not select any other hardware device.
- The link to make a bulk purchase of vouchers using a purchase order is difficult to find on the IdenTrust website. It can be found under the **Disclosures and Refund Policy** section of the Voucher purchase page.
- If an individual provider is purchasing the token and is prompted for the eHR/eMR vendor, choose the **Vendor Program Is Not Listed** option.

4.3 Obtaining and Installing Certificates

If vouchers were purchased during the purchase process, the individuals will use the link on the voucher to start the process of obtaining the digital signing certificate online. Follow the instructions provided.

> **Note:** There is a section that will ask for a social security number, a driver's license number, and a credit card number. The credit card number is used here for identity proofing. This number should be one that belongs to the individual. It will not be charged. A separate section will ask for the payment information if a voucher was not used.

IdenTrust uses remote identity proofing via an online process, which can be found at https://www.identrust.com/sites/default/files/resources/Identity_Verification_Document_Requirements_IGC.pd_.pdf.

If IdenTrust is unable to complete remote identity proofing online, they may request some additional documentation or provide a set of forms to complete and be notarized.

Some common issues that lead to unsuccessful remote identity proofing include:

- Using a cell phone instead of a land line for a phone number. Many cell carriers reject inquiries regarding identity.
- Using nicknames instead of full legal names.
- A credit card number to use for identity proofing was not supplied.

> **Note:** It is important that the user track any security information (e.g., PIN, unlock code, security questions) as it may be needed if the user is unable to use the certificate on the token at a later time.

4.4 Renewing Certificates

Certificates need to be renewed every two years. IdenTrust should provide a notification via email when it is time to renew the certificate. Follow the instructions provided in the email to renew. The same form is used to acquire renewal certificates as the new tokens.

> **Note:** While it is possible to order vouchers for both new tokens and renewal certificates at the same time, it is recommended to order new hardware separately from renewal certificates. This will avoid any confusion when completing the order form.

As with the initial purchase, renewing can also be done using vouchers (PO or credit card) or direct purchase by the provider. Whatever method is chosen, make sure that you indicate that this is a renewal and the user(s) already have the hardware device.

5.0 ORC Tokens

This section is included as a reference for the acquisition and provisioning of ORC tokens. This information, referenced documents, and referenced links are accurate at the time of the document's publication. However, any of this information and detail may become deprecated and changed by ORC at any time without forewarning, so adjustments to these procedures and instructions may need to be made.

5.1 Approved Product

The EPCS application completed DEA certification using the following ORC product combination:

- USB Token: USB cryptographic token
- Certificate: 1 Year ECA Medium Token Assurance Identity/Encryption Certificate Pairs
- Certificate Renewal Period: 1 year
- The ORC product literature can be obtained at https://eca.orc.com/pricing/.

> **Note:** ORC requires the ActivClient software to provision the certificates. Remember to include a license with each token. ActivClient is not required to carry out multi-factor authentication or to digitally sign a controlled substance medication order. Federal or other sites that already have ActivClient installed may not need to order this product.

5.2 Purchasing New Tokens and Certificates

ORC offers a single acquisition process, whether ordering one token or multiple tokens. The information provided herein was accurate at the time of publication.

To order tokens and vouchers, send an email to pkihelp@orc.com to request a quote. Note the following information in the email:

- The quantity being acquired.
- The following products:
  - Certificate: 1 Year ECA Medium Token Assurance Identity/Encryption Certificate Pairs
  - USB Token: USB cryptographic token
  - ActivClient
- The method of payment that the site intends to use. A site can acquire vouchers and tokens using a credit card, corporate check, or purchase order.
- A shipping address and contact for ORC to use to send the tokens.

ORC will return a quote. Follow the directions on the quote to confirm the order and submit payment.

After the site receives the tokens, the site will issue the tokens and ORC instructions to the individual users.

5.3 Obtaining and Installing Certificates

The ORC instructions will provide the steps necessary to obtain and load the digital certificates onto the token. As part of obtaining the certificate, you need to conduct identity proofing. ORC requires forms to be completed, notarized, and submitted to ORC.

> **Note:** It is important that the user track any security information (e.g., PIN, unlock code, security questions) as it may be needed if the user is unable to use the certificate on the token at a later time.

Prior to installing the certificate, the workstation must be prepared to read and use the token. See Section 6.0 for these steps.

5.4 Renewing Certificates

Certificates will need to be renewed every year. The same process is used to acquire renewal certificates as the new tokens.

> **Note:** While it is possible to order vouchers for both new tokens and renewal certificates at the same time, it is recommended to order new hardware separately from renewal certificates. This will avoid any confusion between vouchers for new tokens and vouchers for certificate renewals.

6.0 Preparing for USB Token Use

6.1 Obtain Certificate Authority Trust Anchor

Each credential service provider has instructions to download and install one or more sets of root certificates. The purpose for these root certificates is to provide a trust anchor for the certificates issued by the credential service provider. This will typically include two sets. One set is the primary and intermediate certificate authorities for the credential service provider's Certificate Authority (CA). The second set provides the primary and intermediate certificate authorities for the Federal Bridge Certificate Authority.

Instead of having each user pull down these certificates, use the instructions provided by the credential service provider to pull down the certificates and store in a designated location. To obtain the CA Trust Anchor:

1. Establish a designated secure location to store the root certificates.
2. Download the root certificates for the selected credential service provider and store in designated location:
   - For ORC: https://eca.orc.com/caCerts/ECA_Root_CA_4.cer and https:/eca.orc.com/caCerts/ECA_ROOT2.cer.
   - For IdenTrust: https://www.identrust.com/support/downloads and navigate to the IGC Root Certificate Download – for Device and TLS/SSL Certificates.

6.2 Install Certificate Authority Trust Anchor

Once the Certificate Authority Trust Anchor has been obtained, it can be installed on all systems but for EPCS to function correctly, it must be installed on the following systems:

- Workstations that will be used by the EPCS Provider Profile Admin role to associate providers' tokens with their EPCS profiles.
- Workstations that will be used by the EPCS Provider Access Admin role to activate providers' EPCS profiles.
- Workstations that will be used by providers to digitally sign controlled substance medication orders.

To install the CA Trust Anchor:

1. Identify the impacted servers and workstations.
2. From each server or workstation, access the location where the root certificate was stored and double click the certificate.
3. This will launch the certificate import wizard.

4. Follow the directions and store in the Trusted Root Certificates store.

Alternatively, the certificates can be pushed out using group policy. See the Microsoft article "Distribute Certificates to Client Computers by Using Group Policy" (https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy) for further information.

6.3 Prepare Workstations to Read from USB Tokens

The HID ActivKey SIM used by ORC and IdenTrust is technically a USB smartcard reader and SIM smartcard. Workstations that will be used by providers for digitally signing controlled substance medication orders and by the EPCS Provider Access Admin to credential providers shall allow access to the token.

6.3.1 Identify Impacted Workstations

The ability to connect the USB token is not required at all workstations. The ability to attach the USB token is only required where providers will digitally sign controlled substance medication orders, where the EPCS Provider Profile Admin will associate the token to providers EPCS profiles, and where the EPCS Provider Access Admin will use multi-factor authentication to activate a provider's EPCS profile.

6.3.2 Whitelist USB Tokens

> **Note:** In general, a site will want to use the same methods/utilities that are used to lock down the use of peripheral devices to whitelist the cryptographic tokens. The following provides an overview of the common methods used to restrict and whitelist devices. A site should assess its own configuration prior to utilizing the instructions that follow.

The device shows up in Windows Device Manager as two components. Under **Smart card readers**, it displays as **Microsoft Usbccid Smartcard Reader (WUDF)**. Under **Smart cards**, it displays as **ActivID ActivClient (HID Global Crescendo C1150)**.

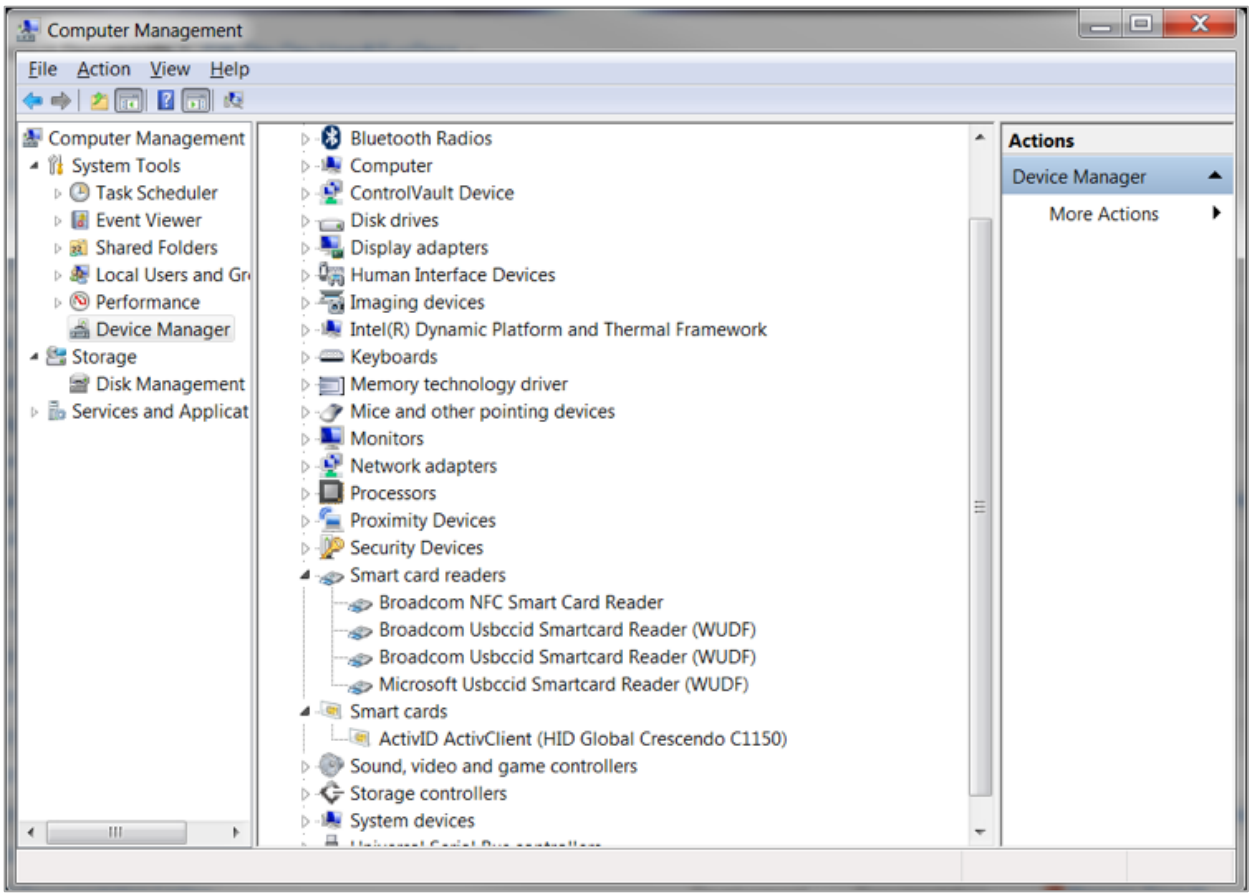

Figure 6-1: ActivKey SIM in Device Manager

If a site has locked down the ability to plug in certain devices, the ActivKey SIM device shall be added to the device whitelist in the workstation's configuration. In general, the site will want to review the steps originally used to lock down the devices. If a site is using device management utility, such as USB Device Control that is part of the enterprise version of Symantec End Point Protection or Microsoft InTune, the device management utility should be used to whitelist the USB token.

The most common mechanism to lock down which devices are allowed to run on a workstation is Group Policy (GPO). While not detailed instructions, the following outlines the group policies that are involved. The site shall determine whether to use Domain GPOs or Local GPOs based on how it manages group policies.

In general, there are two policies that control the installation of devices. Both are under the Device Installation Restrictions policy. The "Prevent Installation of Devices not described by other policies" does not allow a user to activate the drivers for a device that is not whitelisted. The "Allow installation of device that match any of these device IDs" provides the means to specify the whitelist.

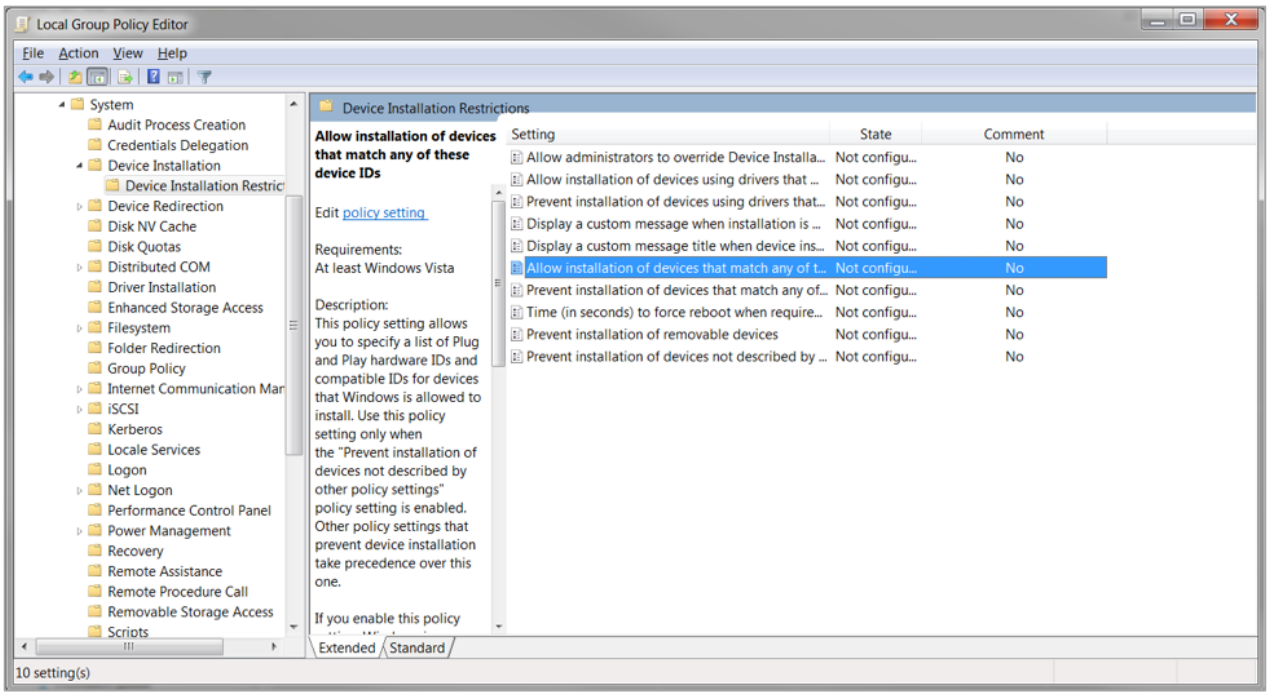

Figure 6-2: Device installation restriction in group policy editor

Both of the above policies would be enabled and the device ID of the ActivKey SIM would be added to the whitelist. The device ID can be found using **Windows Device Manager** under **Details | Hardware IDs**.

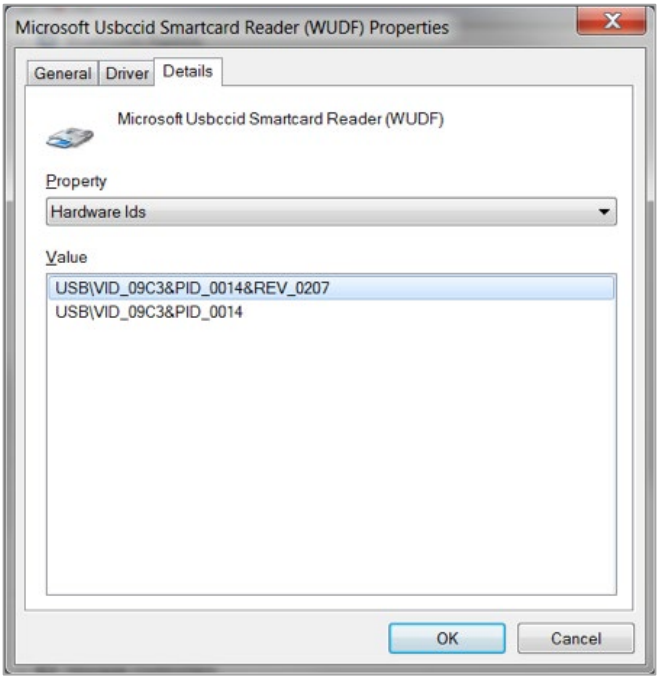

Figure 6-3: Device manager and Hardware IDs

These are added to the whitelist.

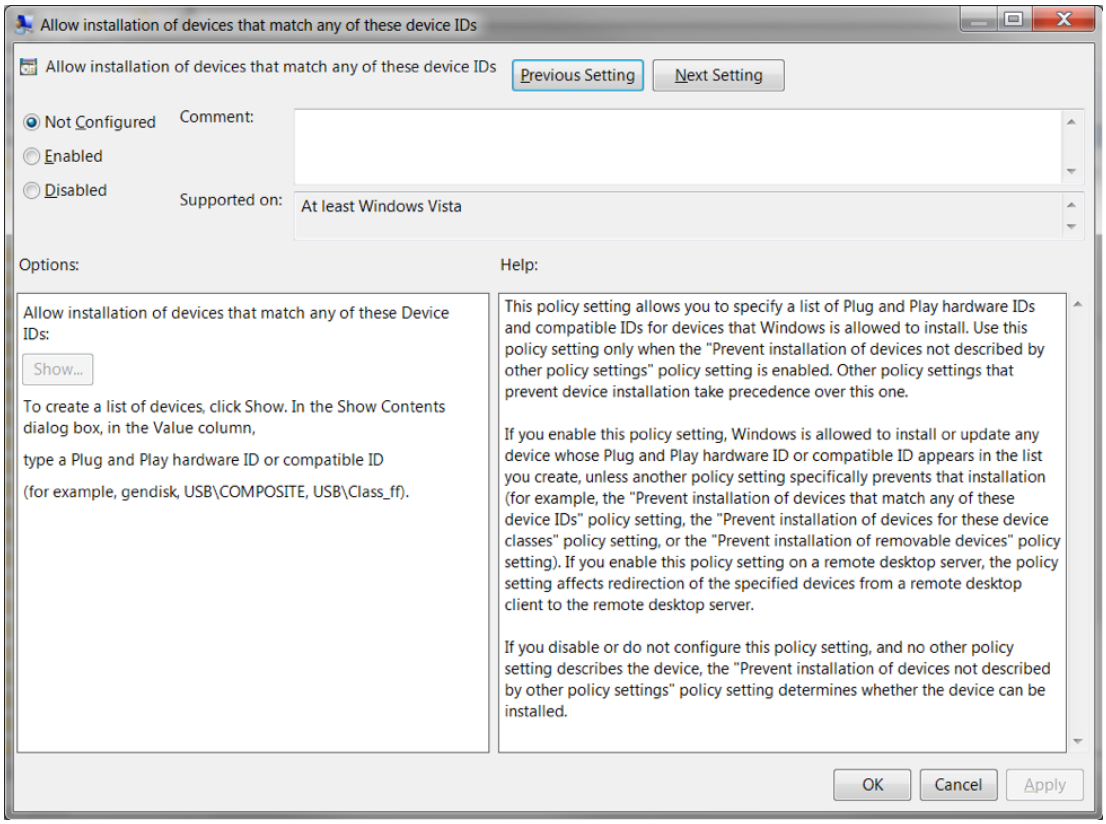

Figure 6-4: Adding device to whitelist

6.3.3 Device Installation GPO

Sites may have implemented restrictions that prevent non-admin users from installing devices. This GPO takes the approach that is often used to allow non-admin users to install printer drives.

This uses the policy System/Driver Installation, and allow non-administrators to install device drivers for these classes:

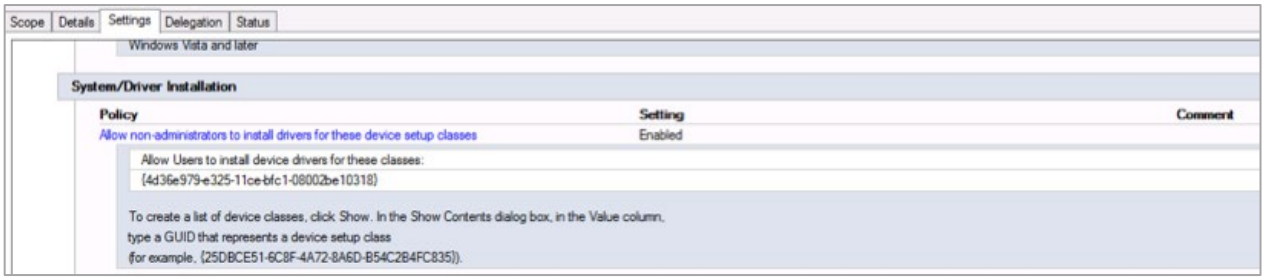

Figure 6-5: GPO non-admin device install

Since the HID ActivKey SIM installs as a smart card reader, the smart card reader class must be added to the list of allowed devices.

Smart Card Readers
Class = SmartCardReader
ClassGuid = {50dd5230-ba8a-11d1-bf5d-0000f805f530}

This class includes smart card readers.

6.3.4 Pass-through for Virtual Desktops and Thin Clients

If a site is using virtual desktops, the previous steps shall be conducted for the virtual desktop. It will also be necessary to allow the remote desktop access to the token. Remember that the token shows up as a SmartCard. The actual mechanism to pass-through the token will vary based on the actual remote desktop protocol being used. The following shows how to enable pass-through for a Remote Desktop Protocol (RDP) client:

1. Open the RDP configuration file.
2. Select the **Local Resources** tab.
3. Select the **More** button toward the bottom.

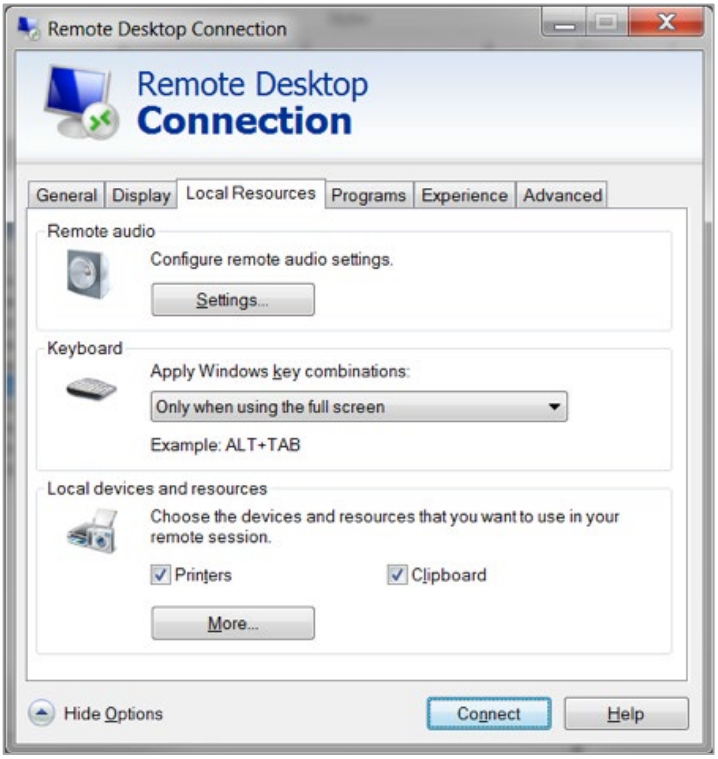

Figure 6-6: Remote Desktop Connection dialog, Local Resources

4. Ensure that the **Smart cards** check box is checked, then click **OK**.

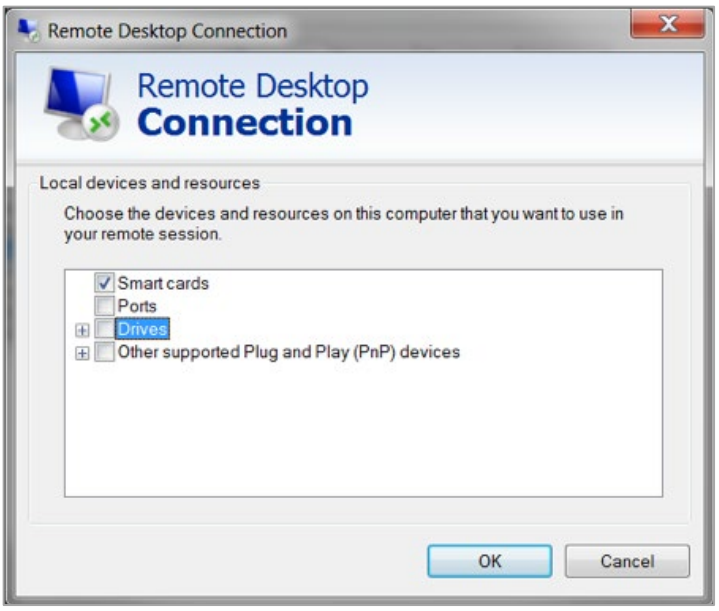

Figure 6-7: Remote Desktop Connection dialog, Local devices and resources

6.4 Install HID ActivClient Software

Both ORC and IdenTrust use the HID ActivClient Software to provision the certificates onto the token. It is also used when an individual renews the certificate on the token. The ActivClient software does not need to be installed on each workstation. It only needs to be installed on workstations that will be used to initially provision or renew the certificates token with the credential service provider. Sites should consider designating and configuring a set of workstations for those purposes.

Notes: If a site already has ActivClient installed, such as for use with PIV, it is not necessary and not recommended to install the ActivClient from the credential service provider.

Windows 10 Users: There is an identified issue where Windows 10 will recognize the ActivKey smartcard reader, but not the SIM smartcard. This issue was addressed in ActivClient version 6.2.01.198. However, for Windows 10, it is recommended to use at least ActivClient version 7.1.0.210, which is the version that ships with the tokens. Any Windows 10 workstation that has ActivClient installed should be at least at this version. This includes workstations that will be used to digitally sign controlled substance medication orders that have ActivClient installed.

To install the ActivClient software:

1. Validate that the workstation has had Trust Anchor established per instructions in Sections 6.1 and 6.2.
2. Validate that the workstation has been configured to allow connection of USB token per instructions in
3. Identify the workstations that will be used to provision tokens with the credential service provider.
4. Obtain the ActivClient software from the selected credential service provider.
5. Follow directions provided to install ActivClient on each of the identified workstations.
6. Verify whether the workstation is able to browse to the credential service provider's portal. If not, process a request to unblock the URL.
    - For ORC: https://eca.orc.com/order/token-certificate-requirements
    - For IdenTrust: www.identrust.com/install

Glossary

Authentication

Verifying the identity of the user as a prerequisite to allow access to the information application.

Certification Authority

Organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

Credential

Object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Credential Service Provider

Trusted entity that issues security tokens or electronic credentials to subscribers. The CSP may be an independent third party or may issue credentials for its own use.

Digital Certificate

Data record that, at a minimum:

- Identifies the certification authority issuing it;
- Names or otherwise identifies the certificate holder;
- Contains a public key that corresponds to a private key under the sole control of the certificate holder;
- Identifies the operational period;
- Contains a serial number and is digitally signed by the certification authority issuing it.

Digital Signature

Record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Electronic Prescription

Prescription that is generated on an electronic application and transmitted as an electronic data file.

Identity Proofing

Process by which a credential service provider or certification authority validates sufficient information to uniquely identify a person.

Private Key

A confidential cryptographic key that is used to create a digital signature for the respective owner.

Public Key

A cryptographic key that can be obtained and used to verify a digital signature.

Public Key Infrastructure

Structure under which a certification authority verifies the identity of applicants; issues, renews, and revokes digital certificates; maintains a registry of public keys; and maintains an up-to-date certificate revocation list.

Resource and Patient Management System

A decentralized integrated solution for management of both clinical and administrative information in these healthcare facilities. Flexible hardware configurations, over 50 software applications, and network communication components combine to create a comprehensive clinical, financial, and administrative solution; a solution that can stand alone or function in concert with other components as needed. Professionals in American Indian, Alaska Native, and private sector health facilities use RPMS every day to efficiently manage programs, maximize revenue generation, and most important, to provide high-quality care for patients.

Token

Something a person possesses and controls (typically a key or password) used to authenticate the person's identity.

Acronym List

Acronym	Meaning
CA	Certification Authority
CSP	Credential Service Provider
DEA	Drug Enforcement Administration
EHR	Electronic Health Record
EPCS	Electronic Prescribing of Controlled Substances
GPO	Group Policy
HHS-FPKI	Health and Human Services Federal Public Key Infrastructure
HSPD12	Homeland Security Presidential Directive 12
IHS	Indian Health Service
PIN	Personal Identification Number
PIV	Personal Identity Verification
PO	Purchase Order
RDP	Remote Desktop Protocol
RPMS	Resource and Patient Management System
SIM	Subscriber Identity Module
URL	Uniform Resource Locator
USB	Universal Serial Bus
VA	Department of Veterans Affairs

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/helpdesk/

Email: support@ihs.gov