RESOURCE AND PATIENT MANAGEMENT SYSTEM

Electronic Prescribing of Controlled Substances

(BEPC)

Frequently Asked Questions

Version 1.0
August 2019

Office of Information Technology
Division of Information Resource Management

Table of Contents

1.0 Introduction

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 do electronic prescribing of 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 USB (Universal Serial Bus) cryptographic token or Personal Identity Verification (PIV) card.

This guide is intended to assist sites and individuals with frequently asked questions about tokens, certificates, EPCS credentialing, and the EPCS Monitoring Service.

2.0 Tokens

Q: Who should get a token?

A: There are two user roles that need tokens. The first are providers who will create and sign controlled substance orders. The second are users in the EPCS Provider Access Administrator role. Users in this role verify that providers meet all the criteria to electronically prescribe controlled substance orders.

Q: How many tokens should a site acquire?

A: The site should acquire a token for each provider who will electronically prescribe controlled substance orders and one token for each user in the EPCS Provider Access role. Additional considerations:

- If a user is in both roles, they only need one token.
- If a user has a token from another site, they do not need to purchase another token. They can use the token at each site if the sites have the proper equipment to read the token – smart card reader or USB port.
- Tokens are specific to an individual and cannot be shared.

Q: What token should be selected?

A: The Resource and Patient Management System (RPMS) EPCS application has been certified for use with only the following three tokens.

- PIV cards issued through the Indian Health Service (IHS) that contain 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.
- IdenTrust USB Token: A 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.
- WidePoint ORC USB Token: A 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.

Only these three tokens can be used for the certified EPCS solution. Determining which tokens to use involves many factors. Please review Sections 2.0, 4.0, and 5.0 of the *EPCS Token Provisioning Guide* to assist in making this determination.

Q: Can a site use more than one token type?

A: Yes, any combination of approved tokens can be selected. For tracking purposes, it might be best to select the minimal number of token types. However, a site may use PIV as the primary token type but also use USB cryptographic tokens for temporary employees.

Q: If a provider works at multiple sites, does the provider need a token for each site?

A: No. As long as each site supports the equipment (smart card reader or USB port) needed to use the token, it can be used at multiple sites. The provider will need to go through the EPCS credentialing process at each site.

Q: Can a user switch token types?

A: Yes. A user can switch from user one token to another. For instance, a provider may use a USB token while waiting for the processing of a PIV card. When the PIV card arrives, the provider will need to be re-credentialed via the EPCS Credentialing option. The Provider Profile Administrator will want to select the digital signing certificate from the PIV card and the Provider Access Administrator would verify the user with the PIV digital signature. After this is done, the user would use the PIV to digitally sign control substance orders and would no longer use the USB token. The USB token can be used at other sites, however.

Q: Can a user use multiple tokens at the same time at a site?

A: No, only a single token can be used at a given time at a site. The EPCS Credentialing component only allows one digital signing certificate to be entered; so whatever certificate is entered and verified in the EPCS Credentialing component is the one that should be used to digitally sign controlled substance orders at that site.

Q: Can a user use different tokens at different sites?

A: Yes. A user could use PIV at one site and a USB token at a different site, depending on how the user is credentialed via EPCS at each site.

Q. Do I need to wait until EPCS is installed and configured before acquiring a USB cryptographic token and digital signing certificate?

A: No. It is actually recommended to start acquiring USB cryptographic tokens early in the EPCS implementation process so that they are ready when the EPCS application is installed and configured.

Q: Can a USB cryptographic token be re-issued to another user?

A: Generally, no. Similar to PIV, the digital signing certificate that is loaded onto the token is user specific; so once the digital signing certificate has been loaded, the token cannot be re-issued to another user. However, if the token was issued to the user but the digital certificate has not been loaded, the token may be transferable. If the user has started the identity-proofing process but the digital signing certificate has not been downloaded from the CSP, you would need to contact the CSP to see if the process can be stopped and re-initiated with a different user.

Q: Is there anything special I need to do if I have a PIV card?

A: No. PIVs will continue to be managed through the normal Homeland Security Presidential Directive 12 (HSPD12) processes and the EPCS credentialing process is the same for both PIV and USB cryptographic tokens.

Q: Bad Tokens

A: USB cryptographic tokens should have a lifespan of at least five years. However, they could fail earlier, especially if subject to rough treatment. To determine if a token is failing, attempt to view the token using ActivClient or Device Manager.

Q: What software needs to be installed for the token?

A: ActivClient software needs to be installed to process the initial token setup (load certificates onto the token and to reset a token's PIN), but this software is optional on workstations where controlled substance orders will be signed.

Q: For USB tokens and certificates, can the token and certificate only be used on the machine that was used to load the certificate?

A: No, once the certificate is loaded it can be used on any machine as long as the USB token is plugged in.

Q: Are there special consideration for IdenTrust certificates?

A: IdenTrust expects that identity proofing process and installation of the digital signing certificate to be done on the same machine with the same user profile.

Q: Is installing the certificates on a USB token acceptable on a Virtual Machine (VM)?

A: Yes, if certain conditions are met:

- USB pass-through is enabled.
- The user profile persists on the VM. If the user profile is issued each time a user logs in, then it will not work

Q: What should be done if I am not home when IdenTrust delivers the token to my home address?

A: Once shipping is confirmed, go to the FedEx website and use the tracking number to have the token held at one of the FedEx depots (e.g., copy shop, grocery store) for pickup outside of work hours.

Q: Will there need to be firewall changes to download the digital signing certificate?

A: Generally no; however one alpha site experienced an issue with obtaining certificates inside their network and instead obtained them from an external network outside the firewall. If the certificate retrieval website is not accessible from within your network a firewall exception may need to be added.

Q: When do I need to renew certificates?

A: Certificate renewal is as follows:

- IdenTrust digital signing certificates need to be renewed every two years.
- ORC digital signing certificates need to be renewed every year.

- PIV digital signing certificates need to be renewed as determined by Health and Human Services (HHS) requirements.

Q: Is there certificate renewal fee?

A: For USB tokens there is a certificate renewal fee. The amount is determined by the Credential Service Provider at the time of renewal. PIV cards continue to follow established HSPD12 procedures for certificate renewal.

Q: How do I know when a certificate will expire?

A: The EPCS software will check the expiration date whenever the token is used for two-factor authentication. A 'soon to expire' warning has been added to the PIN prompt for an expiration date of 30 days or less.

In addition, for USB cryptographic tokens, the Credential Service Provider who issued the token and certificate should send an email prior to the expiration of the certificate. For PIV, notification is done as is currently done.

Q What action must be taken once the certificate on the token or PIV card is renewed or extended?

A: Once the certificate on the cryptographic token or PIV card is renewed, the new certificate needs to be assigned to the provider, which means the provider's EPCS certification record has to re-credentialed.

Via the new EPCS credentialing component of the Electronic Health Record (EHR), a Provider Profile Administrator should update the EPCS certification record with the new digital signing certificate and a Provider Access Administrator needs to validate the new changes made to the provider's account via the new EPCS credentialing component of EPCS.

Q: As the EPCS Profile Access Administrator, I have a lot of digital signing certificates in my certificate store. How do I clear them out?

A: The EHR Supplemental User Guide for EPCS (patch 25) has detailed instructions for this process.

3.0 EPCS Credentialing

Q: What is an EPCS Provider Profile Administrator?

A: The EPCS Provider Profile Administrator is the user who enters a provider's EPCS credentials (e.g., DEA number and expiration, digital certificate, etc.) via the new EPCS credentialing component of EPCS.

Q: What is an EPCS Provider Access Administrator?

A: The EPCS Provider Access Administrator is the user who validates a provider's EPCS credentials via the new EPCS credentialing component of EPCS. Per the DEA regulations, this user will need to use two-factor authentication as part of the validation process.

Q: Can a single user have both the EPCS Provider Profile Administrator and the EPCS Provide Access Administrator roles?

A: Yes. However, as part of the DEA regulations, the same user cannot utilize both roles for the same provider record. In other words, a user cannot both edit and validate the same provider's data.

Q: Can a provider also have the EPCS Provider Profile Administrator and/or EPCS Provider Access Administrator role?

A: Yes. However, a user cannot edit or validate his or her own EPCS credentialing record.

Q: Does a user in both a Provider and EPCS Provider Access Administrator role need two tokens?

A: No, a user can use the same token for both roles.

Q: Can a pharmacist also have the EPCS Provider Profile Administrator and/or EPCS Provider Access Administrator role?

Q: Yes. If a pharmacist also has the EPCS Provider Access Administrator role, the pharmacist will need a token.

Q: How are EPCS Provider Profile Administrators entered?

A: A user is assigned the EPCS Provider Profile Administrator role via the XUEPCSEDIT key.

Q: How are EPCS Provider Access Administrators entered?

A: A user is assigned the EPCS Provider Access Administrator role via the XUZEPCSVERIFY key. In addition, the digital signing certificate must be associated with the user. This is done via the SEARCH VERIFIER button in the new EPCS credentialing component of EHR. See the EHR Supplemental User Guide for EPCS for more information.

Q: What provider data can the EPCS Provider Profile Administrator enter?

A: The EPCS Provider Profile Administrator can enter the following information for a provider:

- Authorized to Write Med Orders parameter
- EPCS Status — Active or Inactive
- Provider's DEA number and DEA expiration date
- Provider's VA number
- Provider's DEA X number
- The controlled substance schedules the provider is licensed to order.
- The digital signing certificate from the provider's token.

If the provider does not have a DEA number or VA number, the EPCS Provider Profile Administrator will get a warning but is allowed to continue.

See the EHR Supplemental User Guide for more information.

Q: Does the provider need to meet the EPCS Provider Access Administrator?

A: Yes. The EPCS Provider Access Administrator will need to have the provider's token in order to associate the provider's digital signing certificate with the provider in RPMS.

Q: Can multiple EPCS Provider Profile Administrators edit an incomplete provider EPCS credential record?

A: No. Only one EPCS Provider Profile Administrator can edit an EPCS provider credential record at a time. If there are pending changes to a provider's EPCS credential record and additional changes must be made before validating the changes, either the EPCS Provider Profile Administrator who made the original changes must make the additional changes or the pending changes must be deleted and all desired changes re-entered.

Q: Can any EPCS Provider Profile Administrator delete pending changes to a provider EPCS credential record?

A: Yes. This will allow deletion of an incomplete EPCS credential record in instances where an EPCS Provider Access Administrator leaves the site or is temporarily unavailable.

Q: I have been credentialed in EPCS. Why am I getting an invalid certificate message when trying to sign a controlled substance?

A: If the user gets a "Your signing certificate's status has not updated recently and cannot be validated" or a "Your signing certificate is not currently valid" Windows message when signing a controlled substance order, it may be due to one of the following reasons:

- The BMXNet listener is not running.
- The EPCS Monitoring Service is not running.
- The EPCS Monitoring Service is not able to validate the certificate because it cannot reach the Certificate Revocation List distribution points. Review the EPCS Monitoring Service log to see if the status of the certificates is being validated.

See Section 4.0 for reviewing and resolving these issues.

4.0 EPCS Monitoring Service

Q: What is the EPCS Monitoring Service?

A: The EPCS Monitoring Service is a Windows service that can connect to one or more RPMS databases to perform the following functions:

- Validating the system time for the RPMS database is within five minutes of the National Institute of Standards and Technology (NIST) time clock.
- Validating that the certificates used by the providers are valid to perform digital signing of controlled substance orders.

Both of these functions are required per the DEA regulations.

Q: Where should the EPCS Monitoring Service be installed?

A: This Windows service needs to be installed on a Windows server that can have outbound connections to the internet and that can connect to the RPMS database(s) that it is monitoring. Examples of servers that can be used for installation are the Windows server that hosts the RPMS database or a separate Windows application server that has hosts the EHR Repository or the BPRM practice management Standalone Application Server (as long as these servers can communicate with the RPMS database via BMXNet and can connect to the internet).

Q: Does the EPCS Monitoring Service require firewall changes?

A: For the EPCS Monitoring Service to perform its core functions, the EPCS Monitoring Service will also need access to the internet to reach the NIST time server and the Certificate Revocation List (CRL) Distribution Points that are used to validate the certificates.

The IHS Network Operations and Security Center (NOSC) has adjusted the firewall/proxy rules for the IHS Intranet, so if your RPMS environment is behind the IHS Intranet, the firewall should not need any changes.

For RPMS environments that are not behind the IHS Intranet, follow the instructions in the EPCS Configuration Guide to check and open the firewall.

Q: How do I stop the EPCS Monitoring Service?

A: On the Window service where the EPCS Monitoring Service is running, go to **Start** (Windows key) | **Administrative Tools** | **Services** | **BEH EPCS Monitoring Service**. Stop the BEH EPCS Monitoring Service. The command **net stop "BEH EPCS Monitoring Service"** can also be used.

Q: How do I stop the EPCS Monitoring Service?

A: On the Window service where the EPCS Monitoring Service is running, go to **Start** (Windows key) | **Administrative Tools** | **Services** | **BEH EPCS Monitoring Service**. Start the BEH EPCS Monitoring Service. The command **net start "BEH EPCS Monitoring Service"** can also be used.

Q: What happens if the BMXNet listener is not running?

A: The EPCS Monitoring Service requires that the BMX listener is running. If it is not running, the digital signing certificates cannot be validated. If the digital signing certificates have not been validated for eight hours, providers will no longer be able to order controlled substances electronically and will need to resort to paper.

To check if the BMXNet listener is running, go to the BMXMENU and use the **View** option to confirm if it is running. It is not running, use the STRT option to start the BMXNet Listener.

If the BMXNet listener was restarted, stop and start the EPCS Monitoring Service using the instruction above. Restarting the EPCS Monitoring Service will cause all certificates to be immediate checked instead of waiting for the next four-hour cycle.

Q: How do I monitor the EPCS Monitoring Service?

A: The EPCS Monitoring Service has a log folder containing general logs (log.log) and error logs (error.log) in the path **C:\Program Files (x86)\Indian Health Service\BEH EPCS Monitoring Service\logs**. These logs should occasionally be monitored for errors.

5.0 Miscellaneous

Q: What happens when a provider's DEA number is about to expire?

A: A provider will be notified thirty days prior to the expiration of the DEA number and can submit the renewal paperwork in that thirty-day window. As long as the provider submits the renewal paperwork prior to the actual expiration, the site is able to keep the DEA active on a day-to-day basis while the DEA processes the request, which may take up to six weeks. Each site will need to identify a procedure for addressing the situation when the provider's original DEA Expiration Date has lapsed prior to the receipt of the renewal.

Once the DEA completes the processing of the request, the new DEA expiration should be entered via the EPCS Credentialing component. If the provider fails to submit the paperwork before the expiration date or if the DEA number is not renewed, the provider can no longer submit controlled substance orders using EPCS. These providers must be inactivated for EPCS by either changing their EPCS status to inactive or setting the DEA Expiration Date back to the original Expiration Date via the EPCS Credentialing component.

Q: Where is a listing of the EHR message popup windows related to two-factor authentication and digital signing?

A: See Appendix A of the EHR Supplemental User Guide for EPCS.

Glossary

Authentication

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

Certification Authority

The 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

An 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

A trusted entity that issues or registers tokens and issues electronic credentials to individuals. The CSP may be an independent third party or may issue credentials for its own use.

Digital Certificate

A 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

A record that is 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.

Identity Proofing

The process by which a CSP or certification authority validates sufficient information to uniquely identify a person.

Private Key

The key of a key pair that is used to create a digital signature.

Public Key

The key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure

The structure under which a certification authority does the following:

- 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	Term Meaning
CRL	Certificate Revocation List
CSP	Credential Service Provider
DEA	Drug Enforcement Administration
EHR	Electronic Health Record
EPCS	Electronic Prescribing of Controlled Substances
HHS	U.S. Department of Health and Human Services
HSPD12	Homeland Security Presidential Directive 12
IHS	Indian Health Service
NIST	National Institute of Standards and Technology
NOSC	Network Operations and Security Center
PIN	Personal Identification Number
PIV	Personal Identity Verification
RPMS	Resource and Patient Management System
USB	Universal Serial Bus
VA	U.S. Department of Veterans Affairs
VM	Virtual Machine

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