
Electronic Prescriptions for Controlled Substances

Under the authority of the Controlled Substances Act of 1970, the Drug Enforcement Administration (DEA), Office of Diversion Control (OD) regulates the manufacture and distribution of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and to ensure that there is a sufficient supply for legitimate medical uses. The DEA's regulations currently prohibit the electronic transmission of controlled substance prescriptions. The DEA is working to modify its regulations to allow for the secure electronic transmission of controlled substance prescriptions. The Electronic Prescriptions for Controlled Substances (EPCS) project is expected to bring numerous benefits to both the healthcare community and the patients they serve. These benefits include:

Reduce medical mistakes—There have been numerous reports concerning the impact of prescription mistakes. Some reports estimate that prescription drug errors kill over 7000 patients each year in the United States. The DEA understands that automating and electronically transmitting prescriptions not only benefits the health care industry in terms of cost reduction and increases in efficiency, but such a system also provides tangible benefits to the patient community.

Improve healthcare efficiency—Electronic prescriptions not only reduce the amount of time spent processing prescriptions in the pharmacy; they also improve practitioner efficiency when these systems are linked to patient records and drug utilization review. By prescribing electronically, practitioners get fewer callbacks and patients receive their prescriptions faster.

Reduce prescription forgery—Pharmacists are routinely faced with the problem of determining the validity of controlled substance prescriptions—has the prescription been altered or is it a forgery? EPCS prescriptions will be secured using strong digital signatures thereby enabling pharmacists to quickly determine whether a prescription has been altered or if the prescriber is DEA-registered.

An Allowance Not a Mandate

The DEA understands that businesses must weigh the advantages of any new technology against the implementation costs, and understand the expected return on investment. Since some DEA registrants may not wish to take advantage of the new

regulations, the DEA will leave current regulations and current processes in place—the DEA will not force pharmacies or practitioners to use EPCS. Adoption of EPCS standards will be the only allowance for the electronic transmission of controlled substance prescriptions from practitioner to pharmacy. Participating practitioners will not be prohibited from issuing prescriptions manually.

How Will Electronic Prescriptions Be Secured?

To combat the risk that the use of electronic prescriptions could create new ways for diversion to occur, the DEA will require that this class of electronic prescriptions be digitally signed using Public Key Infrastructure (PKI) technology. This technology will bring to the process the following advantages: (1) reduce the amount of paper in the process (2) speed transaction times (3) lower costs per transaction and (4) introduce security services into the process. The following paragraphs explain the underlying security technology that makes this possible.

What is a Digital Signature?

Frequently, the last business processes to be automated are those that require a “wet signature.” In the electronic world, PKI can replace the traditional approach with a more robust method that delivers both message integrity and nonrepudiation. The solution combines a “document fingerprint” with public key cryptography. Public key cryptography provides a mechanism for encrypting information. It is an important tool used in creating a digital signature. The encryption algorithm is asymmetric—that is, it uses two distinct keys, or numbers. The owner keeps one key private and makes the other public. What one key encrypts, only the other can decrypt. Because neither key can be derived from the other, there is no vulnerability in sharing the public key.

Signing a document—First, the sender’s computer runs the document through a complex algorithm to generate a fixed-length message digest—the unique document fingerprint. If even one letter in the document changes, the fingerprint also changes. Now the sender can use his or her private key to encrypt the digest. The encrypted digest, called a “digital signature,” is then sent along with the message.

Verifying a signature—Upon receiving the digitally signed document, the recipient uses the sender’s public key to decrypt the signature and obtain the original message digest. If the signature can be decrypted with the sender’s public key, then only the sender could have sent it (the sender’s private key was used to encrypt the digest). This provides the service of

nonrepudiation. The recipient then calculates a new message digest and compares this with the one that has just been decrypted. If they match, the document has not been changed. This provides the service of message integrity. This process is instantaneously and transparently performed by PKI-enabled systems.

What is a Certification Authority?

A Certification Authority (CA) is an entity that issues digital certificates to applicants. It also makes certificate status information available to relying parties. In this capacity, it acts as a credible and neutral trusted third party. Subscribers implicitly trust any information that is digitally signed by the CA. The CA performs a number of important duties, including:

Enrollment—Before issuing a digital certificate, the CA verifies the identity of the applicant to ensure that the digital certificate is being “bound” to the correct individual and not to an impostor. Depending on the intended application, some CAs require in-person enrollment while others may allow enrollment over the web. Such procedures are defined in the Certificate Policy (CP).

Revocation—Digital certificates can be revoked for a number of reasons including loss or compromise. The CA lists these untrusted certificates on a Certificate Revocation List (CRL) in the same way that credit card companies once published lists of invalid credit cards. The CRL is digitally signed by the CA and is valid for a specified time period.

Publishing certificates and CRLs—The CA publishes public certificates and CRLs to a network directory. Think of this as computerized white pages. Subscribers are not vulnerable if their certificates are published. The worst thing that can happen is that someone would be able to encrypt a message for the subscriber.

What is a Digital Certificate?

By digitally signing the subscriber’s public key, the CA transforms a user’s public key into a form that other subscribers can trust, namely a digital certificate. The X.509 standard defines the information a certificate must contain, such as the user’s name, the user’s public key, and the certificate’s validity period.

The Need for a Certificate Policy

While technology provides the mechanism to solve the security issues facing electronically transmitted prescriptions, policy ensures that the technology is implemented correctly and managed appropriately. The policy framework is as important as the technology itself.

A Certificate Policy defines the level of assurance their PKI provides. The assurance level results from many operational decisions the CA has made, ranging from due diligence in the enrollment process to how often CRLs will be posted. All policies are not the same; the business application guides the development of the policy. The policy identifies the set of obligations the management and subscriber communities must fulfill. For example:

Securing the private key—For true nonrepudiation, (assurance that the prescription was sent from a doctor and not the office staff), the doctor must not share this private key with anyone.

Accepting a signed prescription—Upon receipt of a digitally signed prescription, relying parties must ensure that the digital certificate used to digitally sign the message has not expired. Relying parties must also verify that the digital certificate is not on a CRL. If it is on the CRL, the message should be ignored. Finally, the signature must be verified to ensure that the document has not been modified. Computer systems can be programmed to perform all of these functions automatically.

Elements of the EPCS Framework

The EPCS framework is being designed to provide trust services to the over 800,000 DEA registered practitioners and the 50,000 pharmacies nationwide. The framework will consist of both government and commercially operated systems. The EPCS framework is made up of the following five elements: 1) Root CA, 2) Subordinate CAs (either commercial or institutionally operated), 3) EPCS-enabled Electronic Prescription Systems, 4) participating DEA registered practitioners, and 5) EPCS participating pharmacies. These elements are shown in Exhibit 1.

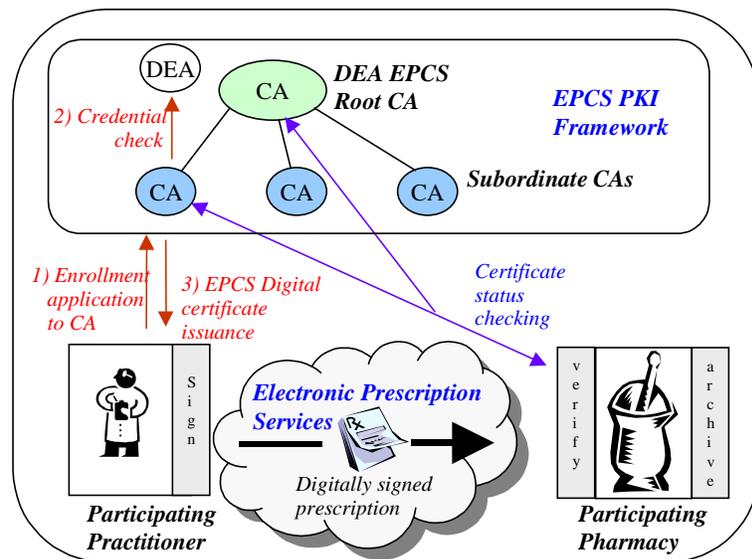


Exhibit 1.

EPCS Root Certification Authority

The DEA developed the EPCS framework after carefully considering a number of PKI-architecture alternatives. The architectures were evaluated with respect to a number of factors including PKI interoperability and regulatory enforceability.

While the DEA has the authority to take action against registrants, it was unclear how DEA regulations would apply to commercially or institutionally operated CAs. In the event that a CA operates in an improper manner—inconsistent with the DEA's EPCS Certificate Policy—the DEA desires the ability to terminate the CA's ability to issue EPCS certificates and to revoke all certificates issued by it. By operating a root CA, the DEA would have a mechanism to do this. While such a step would be drastic, it would only occur after discussions between the DEA and the CA, or after some form of legal action.

The architectures were also evaluated to determine how well they facilitated interoperability between participating PKIs. By operating a Root CA, the DEA can ensure that a participating practitioner's EPCS digital certificate will be universally trusted by all EPCS participants—regardless of the Subordinate CA they enrolled with.

DEA's current role as a registrar naturally positions it to perform a similar—yet reduced—role in the EPCS environment. Therefore, the DEA anticipates that it will implement the EPCS Root Certification Authority as shown in Exhibit 1. Under this framework, commercial or institutional Subordinate CAs that agree to operate in accordance with the DEA's Certificate Policy—and who receive approval from the DEA—would be granted the authority to issue EPCS Digital Certificates to DEA registered practitioners and institutional authorized practitioners. To facilitate this, the EPCS Root CA will issue certificates to DEA approved Subordinate CAs.

The DEA would define the EPCS Certificate Policy (CP) to define strict standards and obligations that will be followed by approved EPCS CAs and by participating practitioners, pharmacies and prescription software vendors. As the regulatory authority for the EPCS system, the DEA would retain its ability to revoke digital certificates issued under EPCS.

Subordinate Certification Authorities

Subordinate certification authorities are envisioned to operate under the DEA's EPCS root CA. This does not preclude commercial organizations from setting up a Certification Authority exclusively for EPCS.

Responsibilities of EPCS Subordinate CAs

Comply with the DEA's EPCS Certificate Policy—The EPCS CP will define the set of PKI policies that ensure that participants maintain a high level of assurance. The policy defines the requirements for identity proofing. CA operation must be performed in accordance with the EPCS CP.

Issue EPCS Certificates to DEA registered practitioners—The EPCS-defined enrollment process for practitioners is designed to ensure that the CA can only issue digital credentials to DEA registered practitioners. Registered practitioners will be able to apply for an EPCS certificate either in-person or online. It is anticipated in the case of on-line enrollment that the practitioner must first submit a signed copy of a DEA provided registration form along with proof of DEA registration. A DEA approved CA will issue an EPCS digital certificate to a DEA registered practitioner only after the CA has approved the application.

Publish up to date certificate status information—The CA will be required to publish a Certificate Revocation List (CRL) on a regular basis as defined in the EPCS Certificate Policy. The CRL identifies the EPCS digital certificates that have been revoked by the CA.

Maintain a CRL archive—The CA will be required to maintain an archive of all CRLs published.

Perform an annual accreditation—Subordinate CAs will be required to perform a yearly third-party accreditation to validate that the CA is operating in compliance with DEA's EPCS standards. The results of the audit must be sent to the DEA.

Electronic Prescription Applications

Today, there are numerous commercial systems that allow practitioners to transmit prescriptions electronically. Under the DEA's current regulations, these systems are prohibited from electronically transmitting controlled substance prescriptions. The DEA anticipates that once its revised regulations are in place, third party electronic prescription vendors will PKI-enable their system to support digitally signed electronic prescriptions for controlled substances to comply with the newly established standards.

Vendor Obligations

Electronic prescription systems typically provide services to practitioners and pharmacists. The following obligations would be pertinent:

Support EPCS digital signatures—The system would have to provide the practitioner with the ability to digitally sign all electronically transmitted controlled substance prescriptions using the practitioner’s EPCS digital certificate. The system should automatically prompt the practitioner. The system will be required to transmit the practitioner’s EPCS digital certificate along with the prescription transaction.

Yearly audit—The vendor will be required to perform a yearly third-party audit of their application to ensure that the software correctly performs the required practitioner obligations.

EPCS Participating Practitioners

Only DEA registered practitioners will be eligible to obtain EPCS digital certificates. EPCS digital certificates will be valid for one year and will allow the practitioner to electronically transmit prescriptions for all schedules of controlled substances. Practitioners enrolled in EPCS will also be able to use their EPCS digital certificate to transmit prescriptions for non-controlled substances. However, since the DEA registration-based EPCS digital certificate exists solely to certify the holder’s registration status to the relying party for the controlled substance prescription transaction, healthcare professionals not registered to handle controlled substances will not be authorized to obtain DEA sanctioned EPCS digital certificates for the purpose of certifying their identities to third parties.

Practitioner Obligations

The following bullets identify the EPCS participating practitioners’ obligations.

Apply for an EPCS digital certificate—Practitioners will be required to submit a properly documented application to an EPCS approved CA of their choice. DEA registered practitioners will be permitted to prescribe controlled substances electronically only after the application has been approved and the CA has issued a digital certificate to the practitioner.

Safeguard the private key—The practitioner will be obligated to protect the EPCS private key on a smartcard or other physical device under the sole control of the practitioner.

Notify CA in event of lost or stolen private key—EPCS participating practitioners will be obligated to notify the issuing EPCS-approved CA within 24 hours of the loss of the private key storage device.

EPCS Participating Pharmacies

As relying parties to the electronic prescription transaction, pharmacies participating in the EPCS program will not receive EPCS certificates. However, the electronic prescription system they use will be required to be EPCS-compliant. This means that the software must perform the EPCS-defined relying party obligations—identified below—prior to accepting the controlled substance electronic prescription. Vendor's of PKI-enabled pharmacy software, and pharmacies who develop their system's in-house, will be required to perform a yearly audit of their application to ensure that the software correctly performs the pharmacy obligations.

Its important to note that the EPCS was not developed as a reporting system—it merely provides a PKI framework that will support the secure and trusted electronic transmission of controlled substance prescriptions between practitioners and pharmacy systems. However, since the prescription will be transmitted in an electronic form, this should make transaction reporting easier when required by state laws or regulations.

Pharmacy Obligations

The following bullets identify a few of the key EPCS pharmacy obligations that must be performed prior to dispensing an electronically transmitted prescription for a controlled substance. These obligations can either be performed 1) in the pharmacy at the time of dispensing or 2) automatically upon receipt of the prescription by whatever intermediate system is employed to connect the pharmacy's computer system to the electronic prescription service provider. In the second case, the verification will be transparent to the pharmacist.

Prescription signature verification—Verify that the electronic prescription has not been altered or that it is a forgery. The pharmacy must reject fraudulent prescriptions and prescriptions that have been tampered with.

Validate practitioner's status—Check the status of the practitioner's EPCS digital certificate to ensure that the practitioner is still a DEA registrant by verifying that the practitioner's EPCS digital certificate is not listed on the CRL. The pharmacy must also verify that the practitioner is authorized to prescribe the appropriate schedule of controlled substances. The pharmacy must reject the prescription if the practitioner's digital certificate has been revoked, or if the practitioner does not have the proper privileges to prescribe the class of medication.

Maintain an archive for 2 years—The pharmacy must maintain an electronic archive of all controlled substance prescriptions

received. DEA regulations regarding the management of electronic records will be part of the Notice of Proposed Rule Making for EPCS.

Electronically sign the prescription record—For valid EPCS prescriptions, the pharmacist must electronically sign the electronic prescription so that the pharmacist can be bound to the act of filling the prescription.

DEA's Efforts to Date

The following bullets identify the work that has been performed to date.

Gathering Security Requirements

The DEA's contractor interviewed over 60 Healthcare stakeholders regarding their perspective on security requirements for electronic prescriptions for controlled substances. The results of this effort are documented in the *Certificate Policy Requirements Analysis*.

This document can be found on the Office of Diversion Control's web site at <http://www.deadiversion.usdoj.gov>.

Industry IT Infrastructure Review

The DEA is sensitive to the significant investment that the healthcare community has made in Information Technology. To ensure that any electronic prescription framework was consistent with Industry IT architectures and configurations, the DEA's contractor conducted extensive interviews with industry representatives to identify how the framework could be designed to minimize any impact on Industry while at the same time leveraging existing infrastructure. The results of this effort are documented in the *Industry IT Infrastructure Analysis*.

This document can be found on the Office of Diversion Control's web site at <http://www.deadiversion.usdoj.gov>.

PKI Interoperability Testing and Product Review

Since the DEA will be operating the EPCS Root Certification Authority, it is critical that the system be interoperable with widely available Commercial Off The Shelf (COTS) PKI products and with PKI service organizations. The DEA conducted extensive PKI interoperability tests to ensure that the platform DEA chooses for the root certification authority is the most interoperable product available. These tests represent the most comprehensive testing performed in industry to date and

underscore the DEA's commitment to ensuring Industry acceptance of the EPCS framework.

Concept of Operations

From the outset, DEA has solicited industry opinions on how such a PKI framework would operate. As a part of this process, the DEA is developing a Concept of Operations to provide a clear picture of the EPCS PKI framework would be designed and how it will operate. The results of this effort will be posted on the DEA's web site at <http://www.deadiversion.usdoj.gov>.

Ongoing DEA Efforts

Moving forward, the DEA is currently involved with the following additional tasks.

Developing Regulations

The DEA is working to develop the Federal regulations that will establish the EPCS framework. These regulations represent a significant evolution in the way prescriptions will be transmitted and promises to bring benefits to the public as well as to the health care community. The DEA plans to issue a notice of proposed rulemaking in late 2000 or early in 2001.

Implementing the EPCS Root Certification Authority

The DEA is working in parallel with DEA's regulatory activities, to establish the EPCS root certification Authority. Significant Lab testing has already been performed that demonstrates the viability of the design.

Industry Input and Comments

The DEA continues to actively solicit Industry comments concerning the EPCS framework. The DEA is also holding industry meetings to share project status information and to help industry stakeholders to prepare for the new regulations.

Pilot Partnerships

The DEA is working with the Department of Veterans Affairs (VA) to evaluate the effectiveness of this concept in a controlled, VA outpatient pharmacy environment. During the PKI Pilot test period, the DEA will exempt participating VA pharmacies from the requirements of 21 CFR §1304, which would ordinarily preclude using digital signatures for controlled substances in lieu of written signatures.