

---

## **Public Key Infrastructure Analysis**

### **Electronic Prescriptions for Controlled Substances Concept of Operations**

**Prepared for**

**Drug Enforcement Administration  
Office of Diversion Control  
600 Army Navy Drive  
Arlington, Virginia 22202**

**In response to  
Assist 5C-A-JMD-0072-DO-220**

**October 26, 2000**

**Prepared by  
PEC Solutions, Inc.**

---

## Table of Contents

	page
<b>Section 1—Introduction.....</b>	<b>1-1</b>
1.1 Overview and Background.....	1-1
1.2 Mission of the Office of Diversion Control.....	1-1
1.3 Description of the Concept of Operations.....	1-2
1.4 General Information.....	1-2
1.5 Document Organization.....	1-3
<b>Section 2—Current Environment.....</b>	<b>2-1</b>
2.1 Practitioner and Pharmacy Responsibilities.....	2-1
2.1.1. Practitioner Responsibilities.....	2-1
2.1.2 Pharmacy Responsibilities.....	2-2
<b>Section 3—Overview of Public Key Infrastructure (PKI).....</b>	<b>3-1</b>
3.1 Introduction.....	3-1
3.2 Benefits.....	3-1
3.3 Security.....	3-1
3.4 Fundamentals of Public Key Infrastructure.....	3-1
3.4.1 Terms and Definitions.....	3-1
3.4.2 Public Key – The PK in PKI.....	3-2
3.4.3 Infrastructure – The I in PKI.....	3-7
3.4.4 Essential Documents of a PKI.....	3-9
3.4.5 PKI Management Functions.....	3-10
<b>Section 4—EPCS PKI Design Concept.....</b>	<b>4-1</b>
4.1 EPCS PKI Functional Architecture.....	4-1
4.1.1 Root Certification Authority.....	4-2
4.1.2 Subordinate Certification Authorities.....	4-3
4.1.3 Controlled Substances Act (CSA) Database.....	4-4
4.1.4 Pharmacy ADP System and Electronic Prescription Archives.....	4-4
4.2 EPCS PKI Network Architecture.....	4-4
4.3 EPCS PKI Certification Authority Architecture.....	4-6
4.3.1 EPCS PKI Trust Model.....	4-6
4.3.2 EPCS PKI Certificate Policy.....	4-6
4.4 Compatible Electronic Prescription Systems.....	4-12
4.4.1 EDI Systems.....	4-12
4.4.2 Closed Proprietary Systems.....	4-12
4.4.3 E-mail Based Systems.....	4-13
4.4.4 Electronic Clearinghouse Based Systems.....	4-13

## Table of Contents

	page
<b>Section 5—EPCS PKI Operation.....</b>	<b>5-1</b>
5.1 Controlled Substances Transactions Allowed Under EPCS .....	5-1
5.2 EPCS Organizational Roles And Responsibilities .....	5-1
5.2.1 Roles and Responsibilities of the DEA.....	5-1
5.2.2 Responsibilities of DEA-approved Subordinate CAs .....	5-3
5.2.3 Responsibilities of the Practitioner .....	5-4
5.2.4 Responsibilities of the Pharmacy .....	5-5
5.2.5 Responsibilities of Third Party Organizations .....	5-7
5.3 PKI Operational Concept .....	5-7
5.3.1 Registration Concept of Operations .....	5-8
5.3.2 Applicant Identity Proofing Concept of Operations.....	5-9
5.3.3 Key Handling Concept of Operations .....	5-10
<b>Section 6—Implementation Procedures.....</b>	<b>6-1</b>
6.1 Implementation of PKI Aware Applications .....	6-1
6.1.1 Practitioner Systems.....	6-1
6.1.2 Pharmacy Systems.....	6-2
6.2 Certification of EPCS Components .....	6-2
6.2.1 Certification of Subordinate CA Systems .....	6-3
6.2.2 Certification of PKI-enabled Commercial Systems.....	6-3
6.3 Requirements for Audit of an EPCS Commercial CA.....	6-4
6.4 Requirements for Archive .....	6-4
<b>Section 7—Control and Management of the EPCS PKI .....</b>	<b>7-1</b>
7.1 Introduction .....	7-1
7.2 Policy Management Authority .....	7-1
7.2.1 Responsibilities .....	7-1
7.2.2 Cyclical and Routine Activity .....	7-2
7.2.3 Procedural Requirements .....	7-3
7.2.4 Reporting and Record Keeping Requirements.....	7-3
7.3 Operations Management Authority .....	7-3
7.3.1 Responsibilities .....	7-3
7.3.2 Cyclical and Routine Activity .....	7-4
7.3.3 Procedural Requirements .....	7-4
7.3.4 Reporting and Record Keeping Requirements.....	7-4
7.4 PKI Manager .....	7-4
7.4.1 Responsibilities .....	7-5
7.4.2 Cyclical and Routine Activity .....	7-6
7.4.3 Procedural Requirements .....	7-7
7.4.4 Reporting and Record Keeping Requirements.....	7-7

## Table of Contents

	page
<b>Section 8—Compliance With Federal Standards and Requirements .....</b>	<b>8-1</b>
8.1 Introduction .....	8-1
8.2 Electronic Signatures in Global and National Commerce Act.....	8-1
8.3 Government Paperwork Elimination Act (GPEA).....	8-1
8.4 OMB Proposed Implementation Of The GPEA.....	8-2
8.5 FDA, HHS 21 CFR Part 11 .....	8-2
8.6 HCFA, HHS 45 CFR Part 142 .....	8-3
8.7 National Conference of Commissioners on Uniform State Law (NCCUSL) .....	8-4
8.8 American Bar Association (ABA) .....	8-4
<b>Appendix A—Fundamentals of Making an Application PKI Aware.....</b>	<b>A-1</b>
<b>Appendix B—List of Acronyms .....</b>	<b>B-1</b>

## List of Exhibits

	<b>Page</b>
2-1 Pharmacy Verification Process.....	2-4
3-1 Symmetric Key Process.....	3-3
3-2 Asymmetric Key Process .....	3-4
3-3 An Example of a Hash Function Process .....	3-5
3-4 An Example of a Digital Signature Process .....	3-6
3-5 A Sample Digital Certificate .....	3-8
3-6 PKI Functions Performed.....	3-10
4-1 EPCS PKI Functional Architecture.....	4-1
4-2 EPCS PKI Network Architecture.....	4-6
4-3 Hierarchical Root CA Architecture.....	4-7
4-4 Details of EPCS Certificate Policy.....	4-8
5-1 Circumstances for Digital Certificate Revocation.....	5-3
5-2 Sample EPCS Online Registration Concept.....	5-8
7-1 EPCS PKI Management Structure .....	7-1

## Section 1 — Introduction

### 1.1 Overview and Background

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 also to ensure that there is a sufficient supply for legitimate medical uses. *Title 21, Code of Federal Regulations, Parts 1300-1316* sets forth in detail the authority and responsibilities of DEA in this area. The Government Paperwork Elimination Act of 1999 (Title XXII of Public Law 105-277) mandates that Federal agencies allow for the option of electronic submission of required records and for the use of electronic signatures when practicable.

The DEA plans to modify their regulations to permit the electronic transmission of controlled substance prescriptions between practitioners and pharmacies using PKI technology to secure the electronic transaction. This technology will bring to this 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 electronic security services into the process.

The electronic security services include: (a) *confidentiality of communications*- only authorized persons will be able to read encrypted communications; (b) *authentication of sending party*- the recipient will be able to positively identify the sender of a communication and subsequently to demonstrate to a third party, if required, that the sender was properly identified; (c) *integrity of communications*- it will be possible for the recipient of a message to determine if the message content was altered in transit; (d) *non-repudiation*- the originator of a message can not convincingly deny to a third party that the originator sent it.

### 1.2 Mission of the Office of Diversion Control

*Title 21, Code of Federal Regulations, Parts 1300 to 1316*, defines the registration, record keeping, inventory, order processing, prescribing, and miscellaneous activities as they relate to controlled substances. Persons who wish to participate in a controlled substance business activity, i.e. manufacturing, distributing, dispensing, research, narcotic treatment programs, import, export, are required to register with the DEA unless otherwise exempted from registration described in §1301.22. Registrants fall into two categories, A-Type registrants and B-Type registrants.

The electronic prescription project focuses on specific A-Type registrants—retail pharmacy and practitioner. The project will review the relationships and processes as they pertain to controlled substance prescriptions. The project will ultimately determine how

the DEA's regulations can be modified to allow for the electronic transmission of controlled substance prescriptions through the use of a PKI.

### 1.3 Description of Concept of Operations

#### Concept of Operations Task 2.2.4

The purpose of this document is to provide a conceptual overview of how the security services of authenticity, integrity and non-repudiation can be achieved for electronically transmitted prescriptions for controlled substances using PKI-based digital signatures. It defines how the Electronic Prescriptions for Controlled Substances (EPCS) Framework will operate from the perspective of patients, practitioners, pharmacists, third parties, and administrators. DEA regulations define responsibilities of the A-Type registrants that participate in this process and these responsibilities are further addressed pertaining to an electronic prescription system. Implementation of the EPCS can be achieved through several architectural designs. This Concept of Operations document provides typical implementation of the EPCS and addresses critical issues in the form of obligations that are related to any EPCS that is fielded. Registration, operations and implementation guidelines are discussed. Finally it provides a basis for implementing the EPCS pilot. This document's target audience includes representatives of the medical and pharmaceutical professions and DEA decision makers.

### 1.4 General Information

This deliverable—the *Electronic Prescriptions for Controlled Substances, Public Key Infrastructure (PKI) Concept of Operations*—has been prepared by PEC Solutions, Inc for the Drug Enforcement Administration's Office of Diversion Control. It is the fifth deliverable under contract ASSIST 5C-A-JMD-0072-DO-220, Public Key Infrastructure Analysis, Task 1. Other documentation produced under this task includes the following documents, which may be referenced in this document:

- **Reference 1:** The *EPCS PKI Program Plan*, dated August 11, 1999, establishes the project goals and requirements and defines the approach that was used to accomplish the PKI Pilot.
- **Reference 2:** The *PKI Certificate Policy Requirements Analysis*, dated March 13, 2000, examines the current commercial business processes, identifies stakeholder requirements, and analyzes issues that affect the level of assurance at which the EPCS PKI will be operated.
- **Reference 3:** The *Information Technology Infrastructure Study*, dated May 26, 2000, presents details of the stakeholders network topologies and applications for the purpose of integrating the PKI into the VA Outpatient Pharmacy Environment as a pilot program.

- **Reference 4:** The *PKI Solution Review* is a survey of the PKI marketplace that identifies a set of Commercial-Off-The-Shelf (COTS) hardware and software candidates for the PKI Pilot.

## 1.5 Document Organization

The remainder of this document is organized as follows:

- **Section 2 Current Environment:** describes the current regulations for the dispensing of DEA controlled substances and the responsibilities of the parties involved in those transactions.
- **Section 3 PKI Overview:** presents an overview of PKI and the benefits that can be derived from PKI-based digital signatures.
- **Section 4 EPCS PKI Design Concept:** presents the concept of operations for the EPCS PKI architecture. It discusses the information flow within the PKI architecture from a functional and a network perspective.
- **Section 5 EPCS PKI Operation:** presents the concept of operations for the daily operation of the EPCS PKI, including organizational roles and responsibilities
- **Section 6 Implementation Procedures:** presents some of the details about the implementation of the EPCS PKI, including the types of modifications and additions that will be required to existing practitioner and pharmacy ADP systems to incorporate PKI.
- **Section 7 Control and Management Structure of EPCS PKI:** outlines the control and management structure of the EPCS PKI.
- **Section 8 Compliance with Federal Standards and Requirements:** summarizes the enacted Federal legislation that 1) supports the use of PKI for digital signature and 2) gives legal guidance for the use of digital signatures.
- **Appendix A - Fundamentals of making an application PKI Aware**
- **Appendix B – List of Acronyms**

## Section 2 — Current Environment

The regulations pertaining to the dispensing of DEA controlled substances (Title 21, Code of Federal Regulations, part 1300 to 1316) and the responsibilities of the parties involved in these transactions are derived from the Controlled Substances Act of 1970 (CSA). These regulations set forth the registration, record keeping, inventory, ordering, prescribing, and other miscellaneous activities as they relate to controlled substances. Persons who wish to participate in a controlled substance business activity, i.e. manufacturing, distributing, dispensing, research, narcotic treatment programs, import, and export, are required to register with the DEA unless otherwise exempted from registration as described in §1301.22

### 2.1 Practitioner and Pharmacy Responsibilities

The dispensing process begins with the practitioner. Practitioners prepare and issue prescriptions for controlled substances in accordance with CFR §1306. The prescription is then conveyed to the pharmacy for dispensing. The following paragraphs outline the responsibilities of the parties under the current regulations.

#### 2.1.1 Practitioner Responsibilities

*The following are the practitioner responsibilities with respect to registration:*

- **Register with DEA.** Practitioners desiring to prescribe or dispense controlled substances (Schedules II-V) must be registered with the DEA in the applicable dispensing category (practitioner, hospital/clinic, etc). The practitioner receives a DEA registration number (CFR §1301 describes the registration process). Registration is required for practitioners in each state where they wish to prescribe controlled substances or at any physical site where they intend to store controlled substances. In some instances, a practitioner will practice under multiple DEA registrations if he/she practices in more than one state.

*The following are the practitioner responsibilities with respect to prescribing controlled substances:*

- **CFR §1306.11.** “All prescriptions for controlled substances shall be dated as of, and signed on, the day when issued and shall bear the full name and address of the patient, the drug name, strength, dosage form, quantity prescribed, directions for use and name, address and registration number of the practitioner.”
- **Schedule II substance prescription requirements.** A Schedule II controlled substance prescription must be in written form and bear the manual signature of the practitioner. Schedule II prescriptions for a resident of a long-term care

facility may be sent to the pharmacy via facsimile and the facsimile will serve as the original prescription. This procedure also applies to prescriptions for narcotic substances for patients in hospice care or for those receiving compounded substances. However, in an emergency, a pharmacy can accept oral prescriptions for a Schedule II controlled substance, within certain limitations.

- **Schedule III -V prescriptions.** Schedule III -V prescriptions can either be written, faxed, or called into the pharmacy.

### 2.1.2 Pharmacy Responsibilities

*The following are the pharmacy responsibilities for registration:*

- **Register with DEA.** Each pharmacy location must be individually registered. The actual location is registered, not the pharmacists at the location. (CFR §1301).

*The following are the pharmacy/pharmacist responsibilities with respect to verifying and dispensing controlled substances to the patient:*

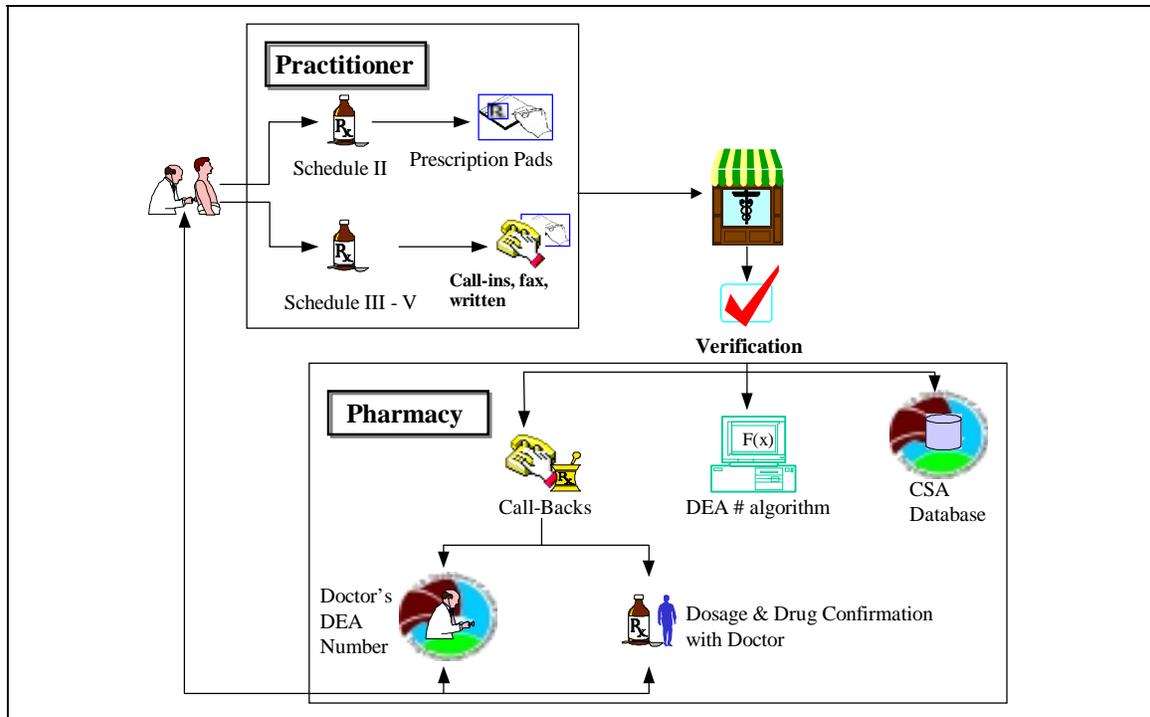
- **Prescription authentication.** As stated in CFR §1306.04, pharmacists have a corresponding responsibility equal to that of the prescribing practitioner. The pharmacist must ensure that the proper substance at the correct dosage reaches the intended patient for a legitimate medical purpose. Prior to dispensing, the pharmacist must be assured of the authenticity of a prescription. After verifying the prescription, the pharmacist dispenses the medication.
- **Registered practitioner validation.** A pharmacist must make a reasonable effort to determine that the prescription came from a registered practitioner. Pharmacists utilize a number of tools to validate prescriptions for controlled substances.

*Some common mechanisms used in the prescription validation process are listed below:*

- **Call the Practitioner back**—Information required on the prescription is confirmed including the DEA number, substance prescribed, and dosage.
- **DEA's Controlled Substance Act (CSA) database**—The DEA maintains a database of valid DEA registration numbers including the registrant's name and the schedules they are permitted to prescribe. This information is available through the Department of Commerce in various media formats including CD-ROM and on-line access. Some pharmacies have integrated this database into their computer system to assist in the validation process.

- **Check the DEA number**—The DEA number is constructed using a special algorithm. Many pharmacy systems are programmed to accept the DEA registration number and run the number through the algorithm to see if it matches the format. This verification process only determines if the number follows the DEA format. It does not determine if the practitioner is registered.
- **Familiarity with community practitioner**—Pharmacists often become familiar with the prescribing habits of local community practitioners. If a pharmacist receives a suspicious prescription that is deemed out of the “regular” prescribing habits of a known practitioner, the pharmacist may use other tools to help determine the validity of the prescription.
- **Signature file**—If there is question as to the validity of the Practitioner’s signature on the prescription, signatures on filled prescriptions can be reviewed in an attempt to compare signatures. Some pharmacies maintain a paper file of practitioner signatures to assist in the verification process.
- **Phone trees**—Structured phone trees are a common tool used by pharmacies to notify one another of a “bad” doctor, patient, or other person involved in diversion. In addition, messages are often sent via electronic mail and facsimile to pharmacies warning them of some possible techniques and persons involved in diversion.
- **Miscellaneous**—There are some additional indicators of diversion that a pharmacist must pay particular attention to:
  - Practitioner is writing more controlled substance prescriptions than other practitioners in the same specialty.
  - Practitioner writes prescriptions for stimulants and depressants at the same time for the same patient.
  - A patient returns too frequently to the physician or visits a variety of physicians in order to obtain the drugs and quantities desired.

Exhibit 2-1 is a diagram of the verification and dispensing processes at the pharmacy.



**Exhibit 2-1. Pharmacy Verification Process**

## Section 3 — Overview of Public Key Infrastructure (PKI)

### 3.1 Introduction

The section provides an overview of Public Key Infrastructure. It is presented at this point in the Concept of Operations as an aid to the reader because many of the terms and concepts of PKI will be used in subsequent sections.

### 3.2 Benefits

Electronic ordering systems for controlled substances and controlled substance prescription systems have the capability to (1) reduce the amount of paper, (2) speed transaction times, (3) lower costs per transactions, (4) improve accuracy of entries, (5) improve data archive and retrieval, and (6) improve overall system effectiveness and efficiency.

While these systems can provide the above benefits, they do not alone provide a sufficiently secure infrastructure to permit their employment in every environment.

### 3.3 Security

PKI technology adds the following security services to an electronic ordering system:

- **Confidentiality** - only authorized persons have access to data.
- **Authentication** - establishes who is sending/receiving data.
- **Integrity** - the data has not been altered in transmission.
- **Non-repudiation** - parties to a transaction cannot convincingly deny having participated in the transaction.

### 3.4 Fundamentals of Public Key Infrastructure

The sections below introduce the key concepts involved in cryptography and PKI. The reader already familiar with this information may skip this section and proceed to Section 4.

#### 3.4.1 Terms and Definitions

- **Key** – aka cryptographic key, an input parameter that varies the transformation performed by a cryptographic algorithm.
- **Secret key** - a key used in a symmetric cryptographic transformation where the key is protected from being known by any system entity except those who are intended to know it.

- **Private key** – the non-publicly disclosable component of a pair of cryptographic keys used for asymmetric cryptography.
- **Public key** – the publicly-disclosable component of a pair of cryptographic keys used for asymmetric cryptography.
- **Encryption** – cryptographic transformation of data (plaintext) into a form (ciphertext) that conceals the data’s original meaning to prevent it from being known or used.
- **Decryption** – cryptographic transformation of data (ciphertext) that restores encrypted data to its original state (plaintext).
- **Hash algorithm (or hash function)** – an algorithm that computes a value based on a data object (such as a message or file; usually of variable length; possibly very large), thereby mapping the data object to a smaller data object (the “hash result”) which is usually a fixed-size value.
- **Message digest** – the fixed size result of hashing a message.
- **Secret key (conventional) cryptography** – a synonym for “symmetric cryptography.”
- **Symmetric cryptography** – a branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption).
- **Asymmetric cryptography** – a modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.
- **Public key cryptography** – synonym for “asymmetric cryptography.”

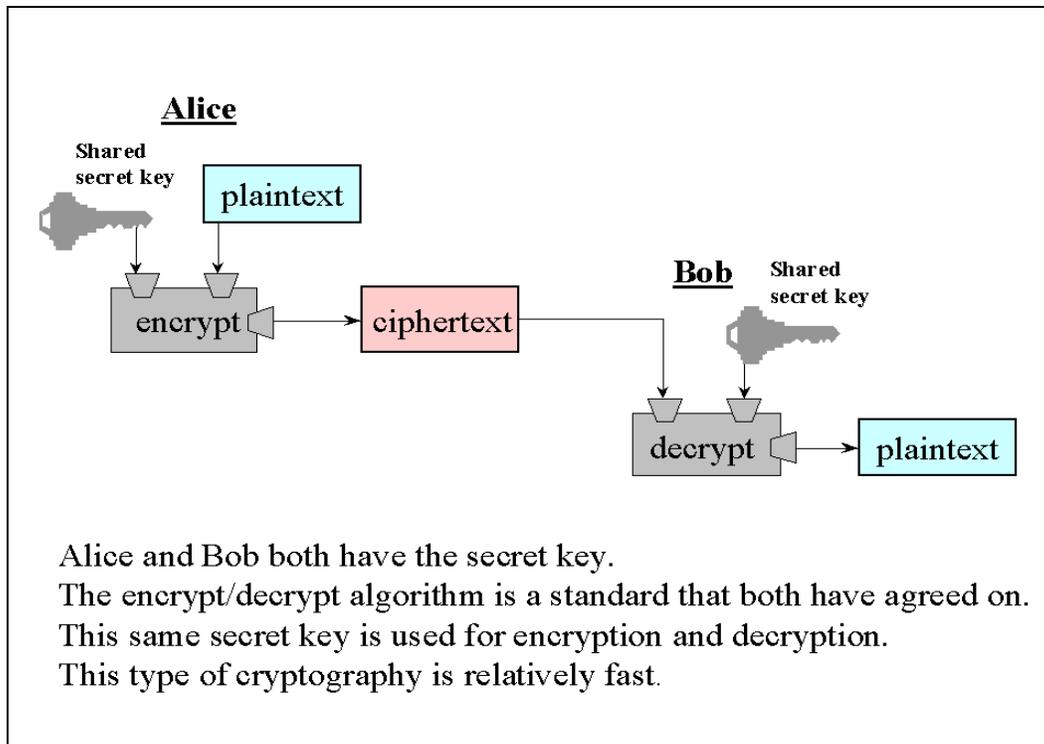
### 3.4.2 Public Key – The PK in PKI

- **Cryptography**

Cryptography deals with the transformation of ordinary text (plaintext) into a coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. Historically, before the advent of mechanical or electrical computers, the transformation was performed by hand and included, for example, the procedures of substitution and transposition. Whether performed by hand or by computer, these procedures, or transformations, are mathematical in nature. The transformation procedure is known as the cryptographic algorithm.

In a computer environment, the encryption and decryption algorithm uses a cryptographic key to perform these mathematical transformations. The key functions as an input parameter to vary the transformation of plaintext to ciphertext and vice versa.

When the cryptographic system uses a single key for both encryption and decryption, the key is known both as a symmetric and secret key. Exhibit 3-1 illustrates the symmetric key cryptography process.



**Exhibit 3–1. Symmetric Key Process**

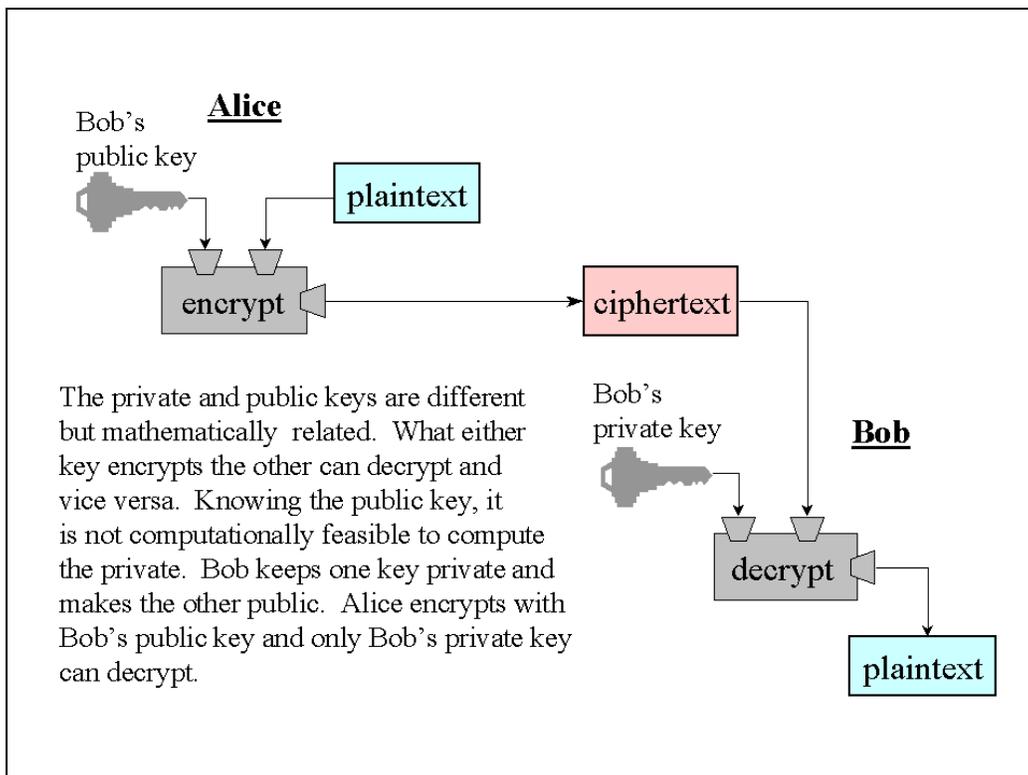
A disadvantage of a symmetric key system is that as cryptographic systems increase in scope and complexity, that is, as the number of participants increase, it becomes increasingly difficult and prohibitively expensive to manage the safe distribution of the secret key or keys.

- **Public Key Cryptography**

Public key cryptography, known as asymmetric cryptography, is a modern branch of cryptography in which the cryptographic algorithms employ a pair of keys. Public key cryptography is distinct from traditional, symmetric key cryptography in which the same key is used for both encryption and decryption. The two keys are the public key and the private key, and either can encrypt or decrypt data. A user gives his or her public key to other users,

keeping the private key to him or herself. Data encrypted with a public key can be decrypted only with the corresponding private key, and vice versa.

The asymmetric key system does not have the disadvantages of a symmetric key system because the public key is made widely available so that anyone can possess it. In this system only the private key needs to be kept private. Each entity can retrieve another entity's freely available public key, thus removing key distribution management complexity. Exhibit 3-2 shows the public key cryptography's use of the public and private keys.

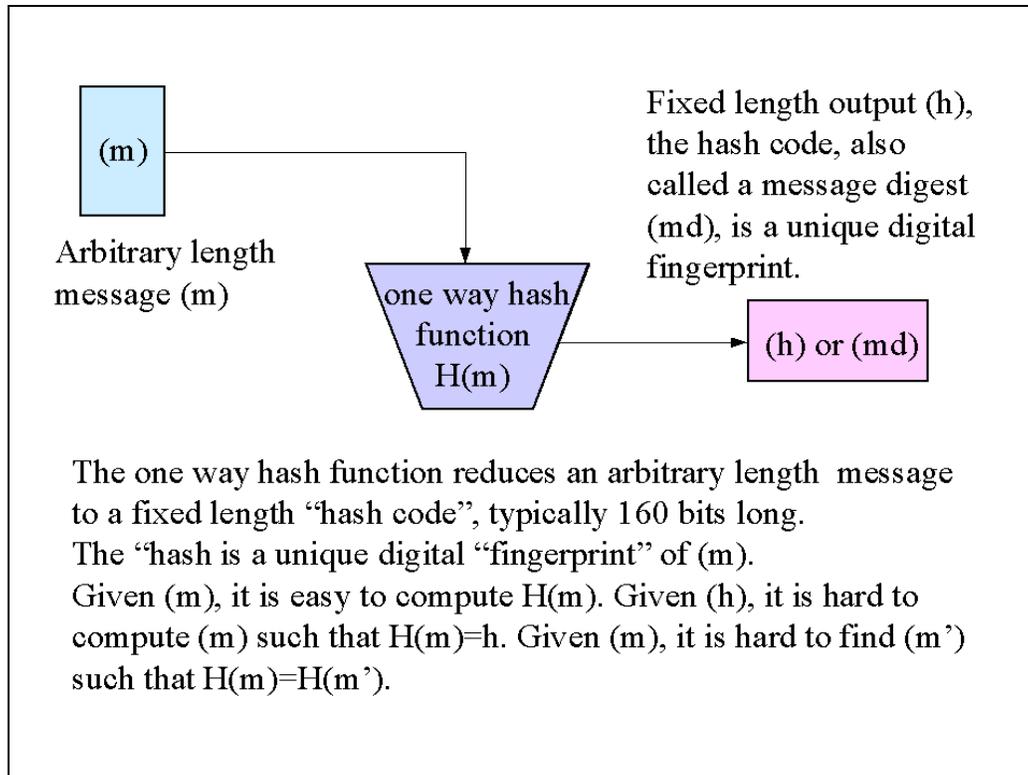


**Exhibit 3–2. Asymmetric Key Process**

- **Hash function processes**

A cryptographic hash function is a function where it is computationally infeasible to find either (a) a data object (plaintext) that maps to a pre-specified hash result (the one-way property) or (b) two data objects (plaintext A and plaintext B) that map to the same hash result (the “collision-free” property).

Exhibit 3-3 illustrates the hash process used to generate a fixed size code from any size input message, in this case an arbitrary 160 bit code.



**Exhibit 3–3. An Example of a Hash Function Process**

- **Digital Signature**

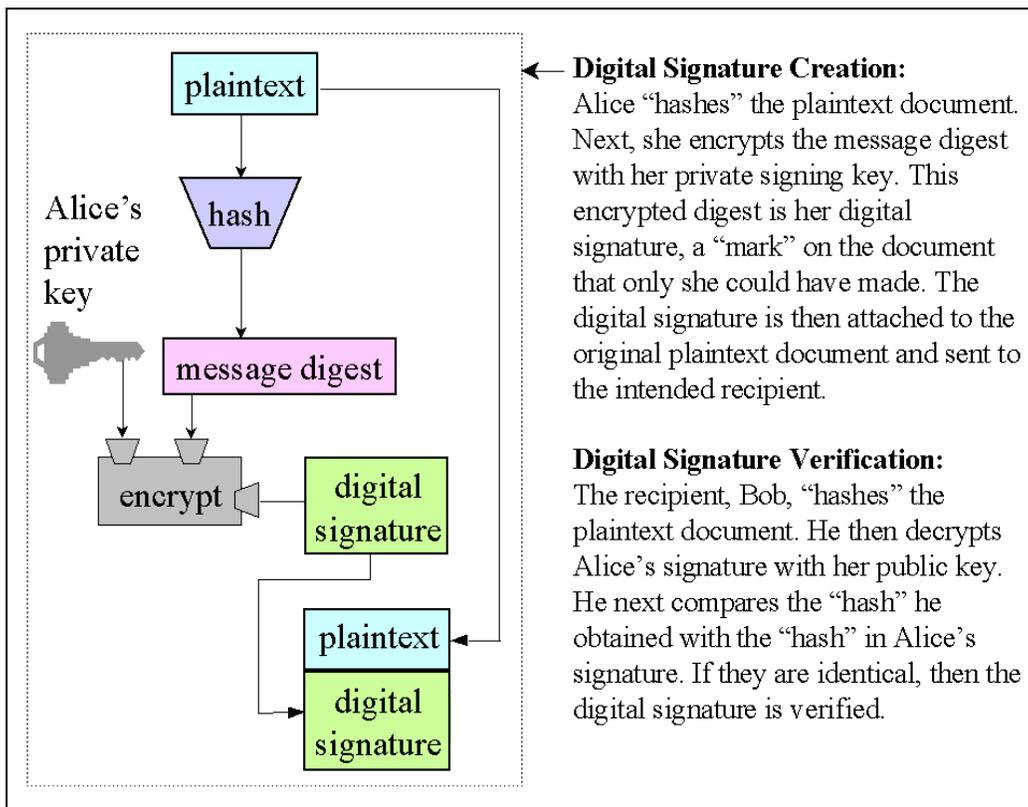
A digital signature is a public key cryptography process in which a signer "signs" a message in such a way that anyone can verify that the message was signed by no one other than himself, and that the message has not been modified since he signed it.

The digital signature process results in a bit string that allows a recipient of a message to verify the identity of the signer of the message and the integrity of the message. Any one of several digital signature algorithms can generate the bit string. These algorithms have the generic characteristic that private information is used to make a signature and public information is used to verify signatures. A private key should be unique to its owner. If the owner of a private key uses it to encrypt a digital document, that encryption may be assumed to have the same meaning as a paper signature. That is to say, it is a “mark” on the document that only the owner could have made. In many algorithms, the owner does not sign an entire document but rather a digest of a document.

A typical implementation of digital signature involves a message-digest, a private key for encrypting the message digest, and a public-key for decrypting the message digest. The digital signature procedure is as follows:

- **The sender.** The software used by the sender computes; using a standard algorithm, a “message digest” from the message. The message digest is unique to the original message in that only the original, unmodified message could have produced the message digest. The sender then encrypts the message digest with his *private key*, yielding an encrypted message digest. He sends the message and the encrypted message digest to a recipient. The two parts together form the digitally signed message.
- **The recipient.** The recipient decrypts the received message digest with the signer’s *public key*. The recipient then computes a message digest from the received message using the same algorithm as the signer. He then compares the decrypted received message digest to the computed message digest. If the two are the same, he accepts the message.

Exhibit 3–4 shows the creation of one type of digital signature.



**Exhibit 3–4. An Example of a Digital Signature Process**

The recipient knows that the signer has sent the message because only the sender’s public key will work. However, it still remains that a particular public key be unquestionably associated with a particular individual or organization. Methods of developing trust in public keys are covered in the next section.

### 3.4.3 Infrastructure – The I in PKI

**Components of the PKI infrastructure include:**

- **Certification Authority (CA)**

A certification authority (CA) is an entity that creates and then "signs" a document or file containing the name of a user and his public key. Anyone can verify that the file was signed by no one other than the CA by using the public key of the CA. By trusting the CA, one can develop trust in a user's public key.

The trust in the certification authority's public key can be obtained recursively. One can have a certificate containing the certification authority's public key signed by a superior certification authority that he already trusts. Ultimately, one need only trust the public keys of a small number of top-level certification authorities. Through a chain of certificates, trust in a large number of users' signatures can be established.

A broader application of digital certification includes not only name and public key but also other information. Such a combination, together with a signature, forms an extended certificate. The other information may include, for example, electronic-mail address, authorization to sign documents of a given value, or authorization to sign other certificates.

A logical view of a sample digital certificate is shown in Exhibit 3–5.

Digital Certificate Structural View

Certificate serial number	3082030830820271A003020102020436F2A2E3
Signature algorithm ident for CA	300D06092A864886F70D0101050500
Issuer X.500 name	3009060355040613025553, 3016060355040A130F552E532E20476F7665726E6D656E74, 301C060355040B13154465706172746D656E74206F66204A757374696365
Validity period	301E170D3939303430363139333235365A170D3032303430363230303235365A
Subject X.500 name	3009060355040613025553, 3016060355040A130F552E532E20476F7665726E6D656E74, 301C060355040B13154465706172746D656E74206F66204A757374696365, 30110603550403130A63657274746573746572
Subject X.500 serial number	300A06035504051303303030
Subject public key information	300D06092A864886F70D0101050500
Certificate Extensions	
CRL Distribution Point	30690603551D1F04623060305EA05CA05AA4583056310B30603550406130255 5331183016060355040A130F552E532E20476F7665726E6D656E74311E301C5 5040B13154465706172746D656E74206F66204A75737469610D300B06035504 03130443524C31
Key Usage	300B0603551D0F040403020520
Issuer unique identifier	301F0603551D23041830146BF3A0494A651430A3D08F8274C8DFF40575204A
Subject unique identifier	301D0603551D0E04160414EAB61B64CBA6E9EFA5BA327814D31F06EC5F09
Basic Constraints	30090603551D1304023000
Certificate format version	301906092A864886F67D074100040C300A1B0456342E3003020490
CA Signature	300D06092A864886F70D0101050500

Exhibit 3–5. A Sample Digital Certificate

- **Database**

A data storage structure where the CA keeps information required for the internal operations of the CA.

- **Repository**

A system for storing and distributing digital certificates and related information (including CPs, CRLs, and CPSs) to certificate users. The repository may be implemented as a trustworthy logically centralized database. It is often implemented as a remote server based on the Lightweight Directory Access Protocol (LDAP), an X.500 directory, or other directory.

- **Registration Authority**

The registration authority (RA) is a PKI entity whose function can be separable from the CA. The RA assists the CA in the recording or verifying of information needed by the CA to issue public-key certificates, CRLs, or other certificate management functions.

- **Timestamp Server (TS) and Data Validation and Certification Servers (DVCS)**

The TS signs a data string or file to establish that the data string or file existed at a particular point in time. A DVCS validates correctness of data and then signs it. TS and DVCS are optional PKI entities.

- **Archive**

The archive provides long term storage of the certificates, and other valuable records for archival purposes.

### **3.4.4 Essential Documents of a PKI**

**The following documents serve as a basis for the detailed implementation, planning, development and direction of operations of a PKI, as well as a basis to establish the level of security and trust model necessary to support the application of the PKI processes.**

- **Concept of Operations (CONOPS)**

The CONOPS sets forth in high level, abstract terms the purpose of a PKI. Although there is no industry standard for this document, it serves to inform an organization's decision-makers about the fundamental concepts and applicability of a PKI. It may include the business rationale for the deployment of a PKI, and may contain a Memo of Understanding (MOU) for the parts of an organization establishing the PKI. It may also include applicable portions of the Certificate Policy (CP).

- **Certificate Policy (CP)**

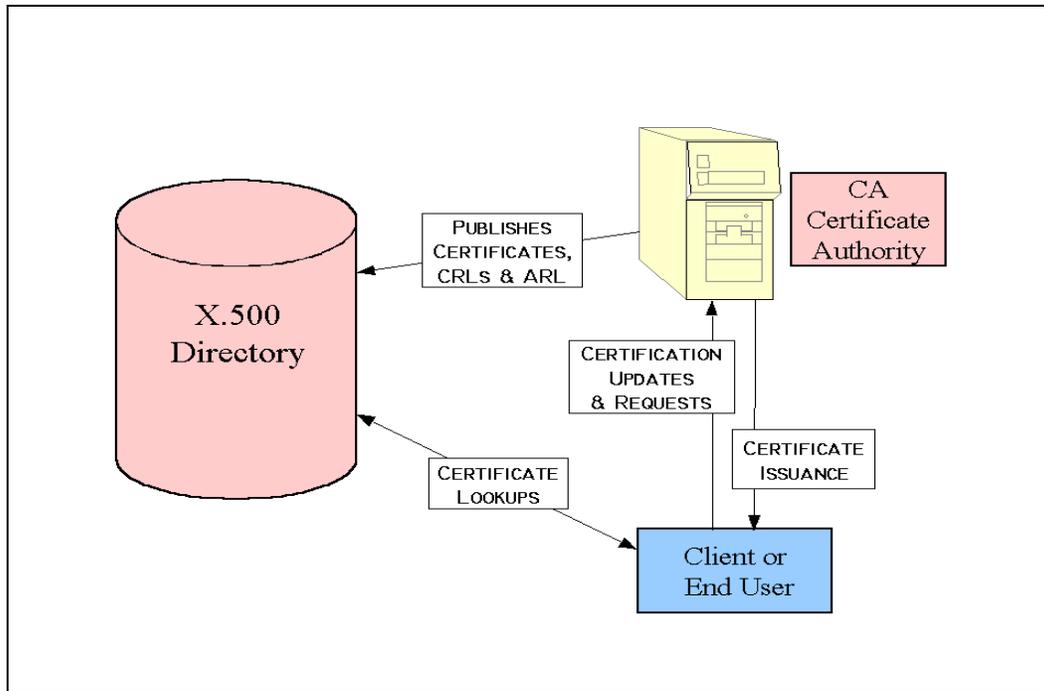
The certificate policy serves as a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application having common security requirements. RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," establishes a standard format for the development of a CP.

- **Certification Practice Statement (CPS)**

This document, more specific than a CP, describes in greater detail how the CP will be implemented. It is written to comply with RFC 2527.

### 3.4.5 PKI Management Functions

**PKI functions are performed in context of the structure of Exhibit 3–6.**



**Exhibit 3–6. PKI Functions Performed**

**The following activities further identify management functions performed in a PKI.**

- **Registration**

The process whereby an applicant, who is the subject of a certificate, makes himself known to the CA, either directly or through a RA. The applicant's name, IP address, domain name, and/or other attributes are placed in the certificate. The CA/RA registers the new applicant by verifying the data provided by the applicant in compliance with the CPS.

- **Initialization**

In the initialization phase the applicant receives the values to begin communicating with the CA or RA. These values could be the public key or Public Key Certificate (PKC) of the CA or the public/private key pair of the applicant. The initialization must be performed through a trusted channel.

- **Certification**

Certification is the process wherein the CA issues a public-key certificate for a subject's public key and returns that public-key certificate to the subject and/or posts that public-key certificate to a repository.

- **Key generation**

Depending on the CA's policy, the user's private/public key pair can either be generated by the user in his local environment, or generated by the CA. If generated by the CA, then the private key must be distributed in a secure manner to the user.

- **Key pair recovery**

There is sometimes a business case for recovery of private signing keys, for example, the user may forget his password and therefore be unable to access his private key. Where this is the case, there are two classes of key recovery techniques: key escrow and key encapsulation, with each technique having its own merits. The determination of preferred key recovery technique to be used is dependent upon the business organization's specific needs and requirements.

- **Key expiration**

Key pairs expire at the end of their period of validation. For the EPCS PKI, the validity period is one year. Each expired key pair must be replaced by generating a new key pair and issuing a new public-key certificate.

- **Key compromise**

The user's private key is subject to compromise. It is the responsibility of the user to maintain the security of this key since it is equivalent to a written signature. The private key should be considered compromised whenever it is stolen, duplicated, or whenever its security status is in doubt. A compromised private key requires the generation of a new key pair and issuing a new public-key certificate.

- **Certificate expiration**

The user's public-key certificate expires at the time of expiration of the public/private key pair. The expired certificate is replaced with a new public-key certificate when the user performs re-registration.

- **Cross-certification**

Cross-certification is the process by which a public-key certificate is issued by one CA to another CA. The public-key certificate contains the public key associated with the signing CA. An end entity in one domain can establish a trust path with an end entity in another domain through a cross-certification process. For example, Alice trusts CA-1 and Bob trusts CA-2. If CA-1 and CA-2 cross-certify, Alice and Bob will have a trusted path.

- **Revocation**

The revocation process utilizes Certification Revocation Lists (CRLs) in the following process description:

A public-key certificate has a validity period when it is issued. However, circumstances can require the CA to invalidate the public-key certificate before the end of the period; for example, due to a name change, termination of employment, or compromise of the private key. Therefore, in response to such events, the CA periodically issues a signed Certificate Revocation List of public-key certificates whose validity period may have not yet expired, but nevertheless are invalid for one reason or another. The CRLs are posted to the Repository where they are available to the users of the system. Additionally, CRLs can be distributed via un-trusted networks to other repositories, because their contents are protected from undetected alteration through the "hashing" process illustrated in Exhibit 3-3.

If, for any reason, a user's certificate appears in a CRL, then the user's certificate is considered invalid by the system. The user will be unable to successfully accomplish transactions until a new private/public key pair and public-key certificate are obtained.

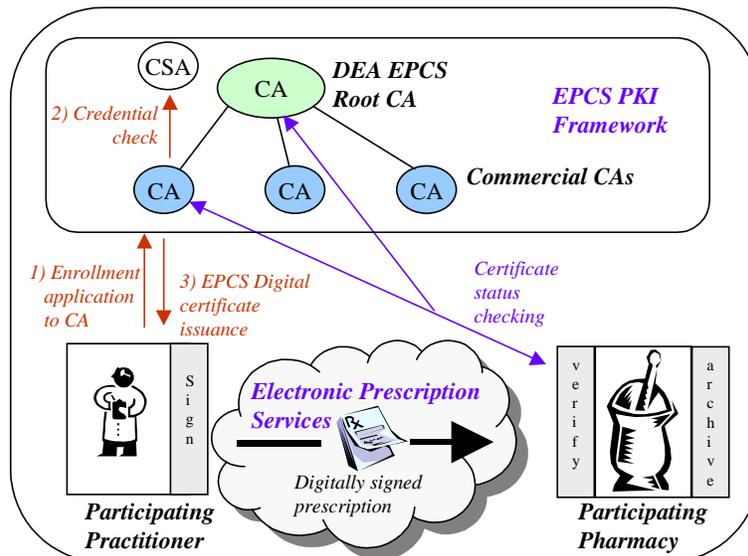
## Section 4 — EPCS PKI Design Concept

This section presents the concept of operations for the EPCS PKI architecture. It discusses information flow between PKI components from both functional and network perspectives. This section discusses:

- **EPCS PKI Functional Architecture**—A concept of operations for the information flow between the DEA Office of Diversion Control, practitioners, pharmacists, and the PKI components.
- **EPCS PKI Network Architecture**—A concept of operations for connectivity between the DEA, the practitioners, the pharmacies, and the PKI components.
- **EPCS PKI Certification Authority Architecture**—A concept of operations for the EPCS based on a hierarchical trust model.
- **Compatible Electronic Prescription Systems**—A concept of operations for the transmission of electronic prescriptions using the EPCS PKI environment.

### 4.1 EPCS PKI Functional Architecture

PKI digital signature technology will allow secure, electronically transmitted, prescriptions for controlled substances. Exhibit 4–1 depicts the major functional elements of the EPCS PKI and identifies the communication interfaces between them.



**Exhibit 4–1. EPCS PKI Functional Architecture**

The following sections detail the key elements of the EPCS PKI functional architecture:

#### 4.1.1 Root Certification Authority

The Root CA will be established by the DEA and will be operated and maintained by the DEA or by an authorized DEA contractor. The Root CA will perform the following functions in the EPCS PKI architecture:

- **Accept Applications for operation from Subordinate Certification Authorities.** Subordinate CAs wishing to offer EPCS digital certificate services to DEA authorized healthcare professionals must complete and submit an *Application for Interoperability with the EPCS Trust Hierarchy* to the DEA. The application will include a satisfactory attestation report from a recognized accrediting organization stating that the Subordinate CA is operating in compliance with the DEA's EPCS Certificate Policy.
- **Issue certificates to Subordinate CAs.** CA's whose application for operation has been approved by the DEA will be granted certificates with which the CA will be authorized to operate. Approved commercial CAs will operate in accordance with the DEA's Certificate Policy and within the DEA's EPCS trust hierarchy.
- **Publish Subordinate CA certificate status.** Relying parties will be required to check the status of an EPCS commercial CA before they accept an electronic prescription from any practitioner who has been issued a certificate from that CA. The Root CA will regularly publish this information in the form of an Authority Revocation List (ARL). In the event that the DEA determines that a Subordinate CA has failed to comply with the provisions of the DEA's Certificate Policy, an administrative action will be undertaken that will result in the revocation of the CA's certificate such that it appears on the ARL.

The Root CA's directory infrastructure will consist of the following:

- **Internet connectivity.** Relying parties will access the directory via the Internet.
- **Fault Tolerant Implementation.** The directory will provide reliable service through a fault tolerant configuration of one or more distributed directory servers at one or more locations. The exact implementation of the ARL directory structure will be discussed in subsequent documentation.
- **Accessible using Lightweight Directory Access Protocol (LDAP).** The ARL directory URL will be accessed by pharmacy automation systems using LDAP version 3.

#### 4.1.2 Subordinate Certification Authorities

DEA approved Subordinate CAs will offer digital certificate services. In doing so, each Subordinate CA will perform the following functions:

- **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.
- **Accept Applications from DEA registrants.** Registered practitioners wishing to electronically prescribe controlled substances must submit an application to the Subordinate CA. Section 5.3.1 provides a detail outline of the registration concept of operations.
- **Issue certificates to DEA registered practitioners.** As their primary duty, commercial CAs will issue EPCS certificates to DEA registered practitioners. The certificates will be signed by the Subordinate CA. Before it approves the certificate application, the Subordinate CA will access the Controlled Substances Act (CSA) database to validate information about the registrant.
- **Revoke digital certificates for cause.** While the revocation of the registrant's DEA registration would obviously result in the revocation of his digital certificate, the opposite is NOT true. A digital certificate may be revoked or invalidated by the CA for a number of circumstances unrelated to any DEA-initiated punitive action. The two "revocations" are not synonymous.
- **Publish subscriber certificates status.** Relying parties will be required to check the status the prescriber's digital certificate before they accept an electronically signed prescription from any practitioner. The commercial CA must regularly publish this information to a directory in the form of a Certificate Revocation List (CRL). The CRL is a list of certificates that the Subordinate CA has issued that have since been revoked. Once a certificate is placed on the CRL, it is no longer valid for use.
- **Maintain a database of public-key certificates.** To verify that the prescription has not been altered, a pharmacist must have a copy of the practitioner's public-key certificate (see Section 3 for more information on signature verification). The commercial CA must publish certificates that it has issued to a directory. However, electronic prescription vendors are free to implement their systems in such a way that does not force the pharmacist to access the directory to obtain the practitioner's digital certificate. The recommended approach would be for the electronic prescription system to include the prescribing practitioner's public-key certificate along with the prescription. In this case, the relying party need only access the directory to obtain the CRL to check certificate status.

- **CRL Distribution Point (CDP).** Each certificate will contain a CDP. The CDP will be in the form of a Uniform Resource Locator (URL) such that it will direct the relying party to the proper directory server where the applicable CRL can be found. The CDP will also supply the LDAP syntax for obtaining the appropriate CRL.
- **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.

#### **4.1.3 Controlled Substances Act (CSA) Database**

The CSA database will play an important role in the EPCS PKI. It is anticipated that the Subordinate CAs will securely access the CSA database when they register a participant and issue a certificate for digitally signing electronic prescriptions. The method of access will depend on the technology used for the CSA database. An advanced version of the CSA database might be connected to the Internet and accessed by Subordinate CA using Secure Sockets Layer (SSL). Alternatively, a Virtual Private Network (VPN) could be set up between the CSA database and the approved Subordinate CAs.

#### **4.1.4 Pharmacy ADP System and Electronic Prescription Archives**

The EPCS PKI will interface with, but will not replace, the functions of a pharmacy's Automatic Data Processing (ADP) system and the internal network used to link the ADP system with other pharmacy locations. The software used in the processing of prescriptions must satisfy the obligations defined in the DEA's Certificate Policy. Section 5.2.4 identifies the pharmacy's and the pharmacist's obligations.

##### **4.1.4.1 Pharmacy's Ability to Cache Revocation Lists**

Before accepting any electronically transmitted prescription for a controlled substance, pharmacy computer systems must check to ensure that the practitioner's certificate and the certificate of the Subordinate CA have not been revoked. This action can result in a directory lookup—across a network—to obtain certificate status information.

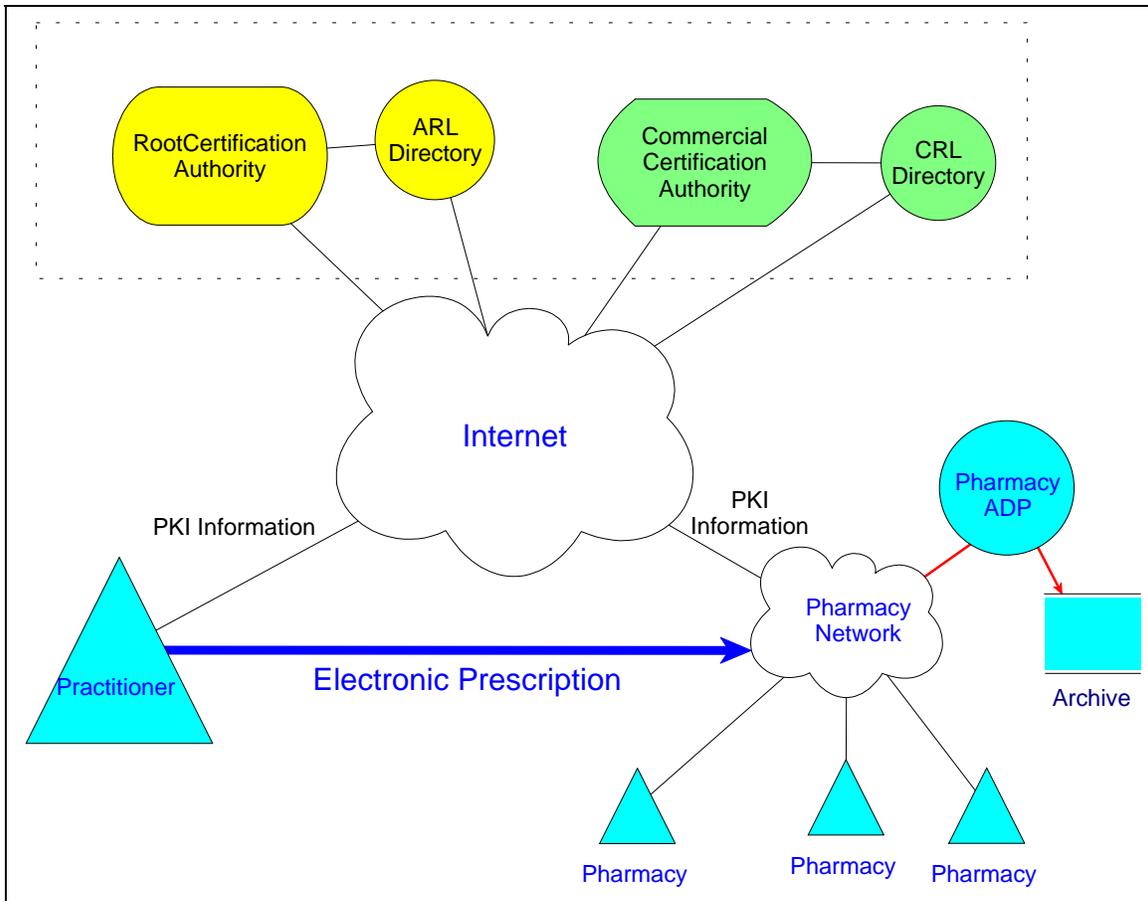
Caching a revocation list— a CRL or ARL—locally speeds the certificate status checking process by allowing relying parties to check a local copy of the revocation list. This eliminates the need for the relying party to transmit a certificate status request to the CA, conserves network bandwidth, and improves performance. Based on the large number of prescriptions that are issued, significant network traffic would result if each prescription required a new CRL check. Relying parties will be permitted to cache CRLs for a period equal to the life of the CRL. This check will be inherent in all PKI-enabled systems and will be automatic and transparent to the pharmacist. The pharmacist's computer system will use a PKI enabled application to assist him in the electronic prescription transaction process. A PKI enabled or aware application is an application that incorporates functionality that permits the application to use the security services provided by PKI.

Appendix A provides a detail look into the fundamentals of making an application PKI aware.

## 4.2 EPCS PKI Network Architecture

Although the connectivity requirements in the functional architecture in Exhibit 4–1 appear to be complex, all connectivity to the EPCS PKI can be made through the Internet. Exhibit 4–2 shows how the network architecture can be quite simple if the Internet is used as the basic connectivity between EPCS PKI components. Some of the key features of this architecture are:

- **The EPCS PKI network is separate from the electronic prescriptions network.** The architecture de-couples the EPCS PKI connectivity from the electronic prescriptions network infrastructure.
- **The EPCS PKI leverages public networks for connectivity.** This architecture will allow practitioners and pharmacists to have the required connectivity to the Subordinate CA, the ARL repository, and the CRL repository via the Internet. This eliminates the need for expensive, dedicated private lines.
- **Flexibility for transmission of electronic prescriptions.** The EPCS does not affect how electronic prescription vendors transport electronic prescriptions for controlled substances. Electronic prescription systems may use any available network (which may or may not include the Internet) for transferring the electronic prescriptions to the pharmacies. Alternatively, they may issue "smart cards" to patients—the smart card would contain the electronically signed prescription.



**Exhibit 4–2. EPCS PKI Network Architecture**

### 4.3 EPCS PKI Certification Authority Architecture

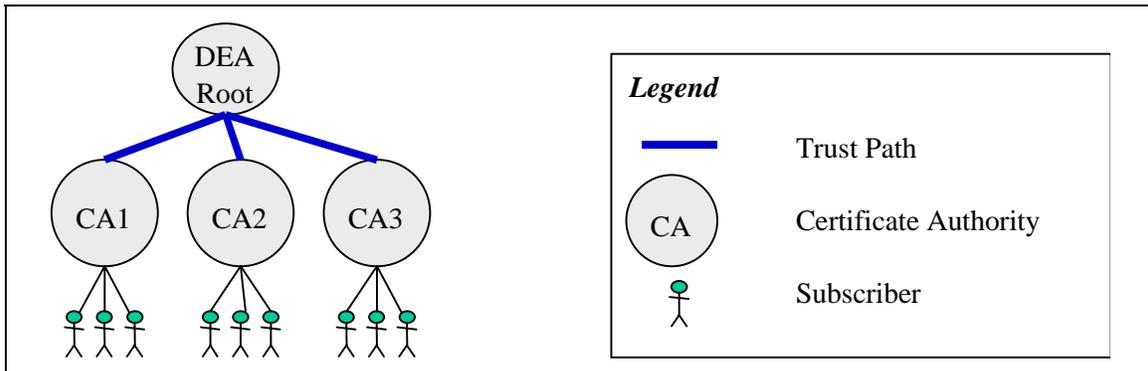
The EPCS Root CA will be operated under a policy that mandates reliability and availability to subscribers 24 hours a day 7 days a week (24x7). The paragraphs below describe the PKI trust model and the certificate policy.

#### 4.3.1 EPCS PKI Trust Model

"Trust Models" in a PKI may be either hierarchical, network, or key ring. Each of the models has certain characteristics, advantages and disadvantages (see Reference 2, *PKI Certificate Policy Requirements Analysis* dated March 13, 2000). The DEA PKI employs the hierarchical trust model. In a hierarchical trust model, end users trust the CA at the root of their hierarchy. The main characteristics of this trust model are:

- Intra-hierarchy trust.** Trust between CAs flows down from the root. Relying parties will only directly trust other users whose CA is a member of the same hierarchy. In a hierarchy, the level of trust for a CA is a function of the level of trust associated with the CA at the root of the hierarchy.

Exhibit 4–3 shows this hierarchy with the DEA CA operating as the root.



**Exhibit 4–3. Hierarchical Root CA Architecture**

### 4.3.2 EPCS PKI Certificate Policy

According to X.509, a Certificate Policy (CP) is: "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." A certificate policy is used by a certificate user to help in deciding whether a certificate is sufficiently trustworthy for a particular application. The degree to which a certificate user can trust the binding embodied in a digital certificate depends on several factors. These factors include:

- The practices followed by the CA for subscriber identity proofing
- The CA's operating policy, procedures, and security controls
- The subscriber's obligations
- The CA's obligations

The DEA's Root CA will issue EPCS digital certificates to approved commercial CAs. This will result in a single trust domain composed of Subordinate CAs operating within the DEA's hierarchy. The DEA's Certificate Policy will define the minimum provisions for CA operation that collectively contribute to the level of assurance that DEA will mandate for electronically transmitting prescriptions for controlled substances.

A complete listing of Certificate Policy Requirements for the EPCS PKI is in Section 4 of Reference 2, *The PKI Certificate Policy Requirements Analysis* dated March 13, 2000.

The EPCS PKI will be operated as a medium level assurance PKI. The EPCS CA Certificate Policy (CP) will describe fully the meaning of this medium level of security. Exhibit 4–4 provides details of the CP, which characterize a medium level policy implementation.

1	Overview	The EPCS PKI will be operated under the authority of the DEA Office of Diversion Control Policy Management Authority (PMA). The purpose of the EPCS PKI is to bring the security services of authenticity, integrity and non-repudiation to the DEA's electronic prescription process. The Certification Authority will be governed by the laws of the US and DEA regulations. The Certification Authority will be operated under a policy that emphasizes and strongly warrants reliability of the PKI and its availability to subscriber's 24 hours a day 7 days a week.
2	Policy Management Authority (PMA)	The Office of Diversion Control will establish an EPCS PKI PMA. The PMA is responsible for setting, implementing, and managing certificate policy decisions regarding the EPCS PKI. The PMA is composed of Office of Diversion Control personnel. It will meet quarterly or as required. At each meeting there will be an opportunity for PKI enrollees from Industry to present matters for consideration.
3	Operations Management Authority	The PMA will establish an OMA. The OMA will carry out the policy of the PMA and will direct the activities of the EPCS PKI Manager. The OMA is composed of DEA personnel. It will require at least 1 full time position.
4	The PKI Manager	The PKI Manager will run the EPCS PKI on a day to day basis. The PKI Manager will be subordinate to the OMA. The PKI Manager and its staff may be Office of Diversion personnel, may be contractor personnel or may be a combination of both.
5	Community and Applicability	The community of users for the EPCS PKI is limited to DEA registered practitioners and pharmacies/pharmacists. An EPCS certificate is limited in applicability to the signing of prescriptions by participating practitioners.
6	Certification Authority	EPCS Subordinate CAs are responsible for (1) issuing, signing, and managing through their life cycle, certificates binding subscribers with their signature verification key (2) promulgating certificate status through CRLs (3) ensuring adherence to the provisions of the Certificate Policy. The Certification Authority will issue and operate in accordance with the provisions of its Certification Practice Statement.

**Exhibit 4-4. Details of EPCS Certificate Policy**

7	Certification Authority obligations and warranties	The Subordinate CA warrants to Subscribers that identities of subjects of certificates are correct and that subjects do hold the corresponding private signature key. Further it warrants that relying parties who correctly perform certificate validation procedures may rely on the validity of the outcome in making identity decisions required under the Controlled Substances Act (CSA). The Certification Authority will make warranties (to be determined) regarding reliability and availability.
8	Legal and financial liability of Certification Authority	To be described fully in the Certificate Policy. The essence will be that the CA disclaims any liability of any kind whatsoever for any award, damages, or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon, a EPCS PKI certificate or its associated public/private key pair.
9	Adjudication of disputes	To be fully described in the Certificate Policy. Will describe the procedures for users and relying parties to resolve disputes with the CA.
10	Registration Authority	The Certification Authority will handle registration of PKI subscribers. There are no provisions for Registration Authority's at this time.
11	Repository	The Certification Authority will ensure that there is a repository wherein EPCS PKI certificates are published and are available to members of the community to validate signatures. The repository will be an X.500 compliant directory with LDAP access. The Certification Authority will assert a very high (to be defined) level of reliability and availability of the repository. The EPCS Certificate Policy will be published in the repository. CRLs will be published in the repository.
12	Certificates	EPCS PKI certificates will be X.509v3 for end entity certificates and X.509v2 for CRLs. End entity certificate validity period will be the same as the current DEA Registration period for a registrant. The certificates will use the appropriate FPKI/PKIX profile.
13	Subscribers	Subscribers hold certificates issued by the Certification Authority. Subscribers will be limited to fully qualified members of the community. Subscribers have obligations in the EPCS PKI Certificate Policy. The Certification Authority will ensure that the Subscriber enters into a written agreement to abide by all the terms and conditions of the Certificate Policy. An X.509 extension will be used in the certificate to classify subscribers as to the schedules of controlled substances they may manufacture, distribute, and dispense.
14	Relying Parties	Relying parties are responsible to perform checks for validity and appropriateness on each certificate presented. Relying parties are responsible to examine the Certificate Policy to understand all of their rights and obligations under the Certificate Policy.

**Exhibit 4-4. Details of EPCS Certificate Policy (Continued)**

15	Approved and prohibited applications	The Certification Authority must be satisfied that all applications that intend to use EPCS PKI certificates use the certificates <u>properly</u> . The manner in which the CA is satisfied will be described in the CP. The Certification Authority will set the minimum requirements for such applications. One of the requirements will be that the CRL is automatically checked at each transaction.
16	Revocation of certificates	The Certification Authority will revoke end entity certificates if end entity private key is lost or compromised or if certificate information changes. CRLs will be published at least every 12 hours. Certificates will be revoked for subscriber failure to abide by subscriber obligations. Certificates will be revoked if DEA registration is revoked. DEA will provide Registration revocation information to the Certification Authority daily. Subscribers will be permitted to cache CRL data daily.
17	Certification Authority trusted roles	All critical functions of the Certification Authority, those functions that impact on security policy, must be performed by at least two persons.
18	Personnel security	EPCS Root Certification Authority staff will have appropriate DEA clearances, training and experience.
19	Recorded events	The Certification Authority will record all events relating to the security of the Certification Authority.
20	Compliance inspection	External audit of the Certification Authority for Certificate Policy compliance is required every year.
21	Certification Authority records	The Certification Authority activity records will be maintained, 7 years, the statute of limitations for violations of the Controlled Substances Act.
22	Types of names	Names of certificate subjects must be x.500 Distinguished Names (DN) and the same Common Name (CN) as used in the DEA Registration process. The DEA Registration Number issued to each Registrant will be included in the DN as a Unique Identifier (UID). The address of the DEA Registrant will be included in the altName field of the certificate.
23	Key pair generation	End entities will generate their digital signature key pair. The public key will be delivered to the EPCS Certification Authority in accordance with: RFC 2510 "Certificate Management Protocols," RFC 2511 "Internet X.509 Certificate Request Message Format," PKCS # 10 "Certification Request Syntax Standard," or via an equally secure manner approved by the PMA. The key generation will be performed in a FIPS 140-1 level 1 module.

**Exhibit 4-4. Details of EPCS Certificate Policy (Continued)**

24	Cryptography	Cryptographic modules must be FIPS 140-1 validated. Cryptographic algorithms must be FIPS approved. Keys must have the equivalent of 1024 bit RSA modulus.
25	Protection of private keys	Certification Authority signing key must be in hardware FIPS 140-1 level 2; end entity private key in hardware or software. All entities are responsible for the protection of private keys and activation data.
26	Certification Authority public key delivery to end entity	The Certification Authority public key must be delivered to the end entity in accordance with RFC 2510 "Certificate Management Protocols," PKCS #7 "Cryptographic Message Syntax Standard," or via an equally secure manner approved by the PMA.
27	Application for a certificate	End entity certificates will be issued within a maximum of 48 hours of receipt of a completed application for a certificate from a DEA Registrant. The Certification Authority will not be a "choke-point" for commerce. The Certificate Policy and Certification Practice Statement will contain provisions for routine re-key and re-key after revocation.
28	Authentication of individual identity	End entity proof of identity is required. The proof of identity may be presented on-line or in person. The proof of identity will consist of (1) a copy of the DEA Registration Certificate, (2) one government issued photo ID, and (3) a proof of current employment document, may be a letter on letterhead stationary, with current work address, IP address, e-mail address and telephone number.
29	End entity proof of possession of private key	End entity will have to prove possession of private key at time of enrollment.
30	Site location, construction and physical access	The facility that houses the Certification Authority and the Repositories will meet a high standard of protection. It will be located in an area sufficiently remote from other activity or traffic. The facility will be of reinforced construction, locked, alarmed, and guarded or under surveillance 24x7. Access will be limited to authorized personnel and authorized and escorted visitors. There will be high quality security storage containers within the facility for the storage of sensitive materials.
31	Disaster recovery	The Certification Authority will operate a "hot" running spare co-located with the Certification Authority and repository. There will be a remote alternate site ready to assume the Certification Authority function in 6 hours. The remote and alternate sites will have the same level of protection as the principal sites. Disaster recovery planning will include a high degree of protection in the areas of power; air conditioning; water; fire; media storage. The Certificate Policy and Certification Practice Statement will address procedures to be followed in the event of Certification Authority signing key compromise.

**Exhibit 4-4. Details of EPCS Certificate Policy (Continued)**

32	Network security	The Certification Authority will be protected from attack through the network to which it is attached through a combination of network security methods.
33	Computer security	The appropriate level of functionality will be achieved through a combination of operating system, PKI software and physical safeguards.
34	Fees	EPCS PKI end entities will pay charges (to be determined) to the CA for services; possibly a fixed enrollment fee and a fee for accesses to the directory.

**Exhibit 4-4. Details of EPCS Certificate Policy (Concluded)**

#### **4.4 Compatible Electronic Prescription Systems**

It is required that the obligations defined by the DEA's EPCS Certificate Policy be enforced in the prescription software systems used by practitioners and pharmacists for the electronic transmission of controlled substance prescriptions. This section summarizes the alternative methods of electronically transporting electronic prescriptions from the practitioner to the pharmacy. Note that the following architectures are independent of the EPCS PKI network infrastructure discussed in the previous sections. The following sections outline some examples of how electronic prescription systems are implemented. Although the implementation of networks for electronic prescriptions is left to the end users, the following are identified as compatible approaches.

##### **4.4.1 EDI Systems**

Electronic data interchange (EDI) networks designed specifically for electronic prescriptions are commercially available today. These networks may use a proprietary client software, which use X.509 certificates for authentication, digital signature, and encryption. Clients are often run on handheld systems from various vendors.

##### **4.4.2 Closed Proprietary Systems**

Closed systems would be special cases of electronic prescription delivery networks. These systems may be based on a pharmacy chain business ADP system or a hospital system.

- **Sending prescriptions.** In some of these systems, there is a central ADP system and terminals are put into each brand pharmacy. In a hospital system, physicians log on to the closed system and create the electronic prescription.
- **Filling prescriptions.** No actual transfer of the electronic prescription takes place, since it is created on the same system on which it is filled. An example of this type of system is the Veterans Administration's Computerized Patient Record System (CPRS) for VA Hospitals. Pharmacists use the same system to fill outpatient prescription orders. The Central ADP system would need to provide a connection to the Internet for purposes of accessing the EPCS PKI

infrastructure components. The architecture for a closed system may require additions to the electronic prescription software modules that enforce the DEA's Certificate Policy for the EPCS system.

#### 4.4.3 E-mail Based Systems

Direct e-mail could be used to transfer the electronic prescription once it is created and digitally signed. This type of network for the EPCS might work as follows:

- **Sending prescriptions.** The patient would select a pharmacy to fill the prescription. This can be done at the time the prescription is created, or the patient can phone the practitioner later. The practitioner's office would e-mail the prescription directly to the selected pharmacy. Existing government regulations are in place to guarantee the privacy of patient information. Encryption is identified as an acceptable technique to safeguard patient privacy. The type of encryption and its requirements are beyond the scope of this Concept of Operations.
- **Filling prescriptions.** When the patient arrives at the selected pharmacy, the pharmacist would look in the pharmacy's e-mail inbox for the prescription.

There is one problem with the e-mail approach. If for one reason or another (such as insurance problems) the pharmacy cannot fill the prescription that has already been e-mailed to it, there is an issue as to how the prescription gets to another pharmacy. Forwarding the electronic prescription to another pharmacy via e-mail leaves questions open as to multiple fillings.

#### 4.4.4 Electronic Clearinghouse Based Systems

An electronic clearinghouse could be used to deliver the electronic prescriptions to the patient. This type of network for the EPCS might work as follows:

- **Sending prescriptions.** A practitioner would upload an electronically signed prescription for controlled substances to a central clearinghouse. The clearinghouse could be a third party, or associated with a pharmacy chain. The methods for uploading the electronic prescription include e-mailing the electronic prescription to the clearinghouse or filling out a form on the clearinghouse Web site. If a Web site is used, Secure Sockets Layer (SSL) encryption might be used to insure patient confidentiality during the transfer.
- **Filling prescriptions.** The patient would go to a pharmacy participating in the electronic clearinghouse. The pharmacy would do the usual insurance checks on the patient and then download the electronic prescription from the electronic clearinghouse. The clearinghouse would delete the electronic prescription (or mark it as "used") so that the patient cannot re-use it at another pharmacy.

To further ensure integrity, the practitioner's office may give the patient a piece of paper with a transaction number on it, which he would present at the time of filling the prescription.

## Section 5 — EPCS PKI Operation

The roles and responsibilities of the EPCS PKI participants are described in this section. The PKI operational concept—also provided in this section—explains the proposed subscriber registration process and the methods of application, enrollment, certification and private key safeguarding.

### 5.1 Controlled Substances Transactions Allowed Under EPCS

The following is the key prescription related process that will be allowed under the EPCS PKI program:

- **Electronic prescriptions for controlled substances.** Only DEA Authorized practitioners and agents as defined by CFR §1301.22 in possession of EPCS digital certificates for the purpose of prescribing controlled substances can perform this activity. The types of controlled substances that the practitioner can prescribe are defined by the practitioner’s registration and may not include the entire range of substances.
- **Electronic prescriptions for non-controlled substances.** Practitioners enrolled in EPCS may also use their EPCS digital certificate to transmit 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.

### 5.2 EPCS Organizational Roles and Responsibilities

The following paragraphs describe the responsibilities of the various participants in the EPCS program. All participants must adhere to the General Provisions listed in Section 4 of Reference 2, The *PKI Certificate Policy Requirements Analysis* dated March 13, 2000 that define participant obligations.

#### 5.2.1 Roles and Responsibilities of the DEA

During the initial research into the feasibility of EPCS, the DEA concluded that PKI-based digital signatures would be acceptable for this process, provided that they are used in a PKI environment in which certificates trace their hierarchy to a DEA established “Root” Certification Authority. The DEA will have the following responsibilities for the EPCS PKI framework:

Establish DEA Regulations:

- **DEA will modify its regulations.** The modifications will allow the electronic transmission of controlled substance prescriptions in accordance with standards set forth in the regulations.
- **DEA will issue a Certificate Policy and Certification Practice Statement.** These two documents will further define the strict standards and obligations that must be followed by approved EPCS Subordinate CAs and by participating practitioners, pharmacies, and prescription software vendors.

Operate a Root CA:

- **DEA will establish a “Root” CA.** DEA will establish and maintain the Root CA. The Root CA adjudicates applications from Subordinate CAs and will sign certificates for approved Subordinate CAs.
- **DEA will generate and maintain a list of accredited Subordinate CAs.** This list will be posted on a DEA Web Site.
- **DEA will establish and maintain an Authority Revocation List (ARL).** The Root CA will maintain an ARL for purpose of identifying those Subordinate CAs who’s authority to issue EPCS digital certificates has been revoked.

Establish Guidelines for Subordinate CAs:

- **DEA will establish criteria to accredit Subordinate CAs.** DEA regulations will require that Subordinate CAs wishing to issue certificates valid for controlled substance prescriptions agree to operate in accordance with the DEA’s Certificate Policy (CP). The CP defines the level of assurance at which the CA must operate.
- **The DEA will require periodic CA audits.** The DEA will require that the Subordinate CA regularly submit proof of compliance with the DEA EPCS CP in order to achieve and maintain accreditation.

Establish guidelines for electronic prescription software:

- **DEA will provide guidelines for EPCS PKI software.** The DEA's certificate policy defines the set of relying party obligations that must be satisfied in any implementation of an electronic system for prescribing controlled substances. Software vendors that implement electronic prescription systems must provide systems that meet these standards. Pharmacists and other relying parties who use these systems must maintain an adequate, readily accessible, electronic

archive to provide the DEA with the ability to audit electronic prescriptions when necessary to ensure that the obligations have been met.

### 5.2.2 Responsibilities of DEA-approved Subordinate CAs

DEA approved CAs will issue EPCS digital certificates to DEA registered practitioners after an application process has been completed and approved by the CA. The EPCS-defined enrollment process is designed to ensure that the CA can only issue digital credentials to DEA registered practitioners.

- **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**—Registered practitioners can 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.
- **Promptly revoke practitioners’ certificates when necessary**—In the event that an EPCS certificate shall need to be revoked, the Subordinate CA must perform this operation with 4 hours of notification. Exhibit 5–1 identifies the set of circumstances under which an end-entity's digital certificate shall be revoked.

Revocation Circumstance	Description
<b>Loss of DEA Registration</b>	Since a registrant's DEA registration serves as the basis for the digital certificate, loss of DEA registration-either voluntarily or through administrative action-would remove the basis and therefore require that the certificate be revoked.
<b>Change of DEA registration information (Registrants only)-</b>	This could occur due to change of location, name change, etc. The old digital certificate would be revoked and a new one issued that would include the updated registrant information.
<b>Change of affiliation (Agents only)-</b>	Since agents are permitted to prescribe under the registration of the employer, this authorization must not "follow" an agent who changes jobs. Institutions must notify the CA when agents terminate their employment.
<b>Forgotten digital certificate access control password</b>	Access to the private key is guarded by a password. Forgetting this password effectively prevents the practitioner from using the key. The only remedy is to revoke the digital certificate and issue a new one.

**Exhibit 5–1. Circumstances for Digital Certificate Revocation**

Revocation Circumstance	Description
<b>Lost or stolen token</b>	The digital certificate must be stored on a hardware device that is under the sole control of the practitioner. A lost or stolen private key could be used for unauthorized purposes if the access control password could be obtained

**Exhibit 5–1. Circumstances for Digital Certificate Revocation (Concluded)**

- **Publish up to date Certificate Status Information**—The CA must 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. A CRL must remain in the archive for 2 years.
- **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.

**5.2.3 Responsibilities of the Practitioner**

A prescription—digitally signed using this digital certificate—will indicate to any relying party, upon successful certificate validation, that the sender is authorized by the DEA to prescribe controlled substances. With this, the practitioner participating in the EPCS program will have the following responsibilities:

*Application, Enrollment, and Revocation:*

- **The practitioner will register with DEA.** The current DEA registration process will not change. All practitioners must register with the DEA to obtain a DEA number required for the dispensing of controlled substances.
- **The practitioner will obtain an EPCS digital certificate from an approved EPCS Subordinate CA.** Practitioners will apply for and, if approved, will receive an EPCS digital certificate from an approved Subordinate CA operating under the DEA’s Certificate Policy. A separate application must be made for each DEA registration held by a practitioner. EPCS certificates will be valid for one year.
- **Agents or employees of registrants can obtain EPCS certificates.** CFR 1301.22 provides guidelines for exemption of registration for agents or employees of DEA registered institutional practitioners (hospitals, and other

institutions). These exempt agents and employees may prescribe, dispense, or administer under the hospital's or institution's DEA number—provided that they are permitted to prescribe, dispense, or administer in the jurisdiction of their practice. These exempt practitioners must have an internal authorization code assigned to them by the hospital or institution.

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

Use of Digital Signatures:

- **The practitioner will use software that operates in accordance with the DEA Certificate Policy.** The practitioner may use a computerized system for creating and digitally signing electronic prescriptions for controlled substances. The software must provide a mechanism for the practitioner to perform all EPCS obligations
- **Private Key Safeguarding.** The private signing key must be protected through the use of two factor authentication and must be under the sole-control of the practitioner at all times.
- **The practitioner will digitally sign the electronic prescription.** To be valid, an electronically transmitted prescription for a controlled substance must include the digital signature of the practitioner. The electronic prescription application must be compatible with the private key safeguarding mechanism.

#### 5.2.4 Responsibilities of the Pharmacy

As stated in CFR §1306.04, pharmacists have a corresponding responsibility equal to that of the prescribing practitioner. The pharmacist must ensure that the proper substance at the correct dosage reaches the intended patient for a legitimate medical purpose. Prior to dispensing, the pharmacist must be assured of the authenticity of a prescription. After verifying the prescription, the pharmacist dispenses the medication.

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 is not being 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.

Pharmacies participating in the EPCS program will have the following responsibilities:

Processing digital Signatures:

- **Pharmacy must verify the digital signature**—To ensure that the prescription or refill request had not been altered in transit, the pharmacy’s computer system will be required to check the digital signature to verify that the signed hash is the same as the hash computed independently by the sender’s computer system. This check will be inherent in all PKI-enabled systems and will be automatic and transparent to the pharmacist.
- **Pharmacy must verify the status of the certificate**—For prescription verification purposes it is required that the pharmacy’s computer system perform a certificate status check to ensure that the certificate used to sign the transaction is indeed a valid one. Status checking must be performed using a recent copy of the Certificate Revocation List (CRL). This check will be inherent in all PKI-enabled systems and will be automatic and transparent to the pharmacist. (Status checking will not be required on refills since the DEA bases the validity of the refill on the validity of the original prescription (for Schedules III-V only).
- **Pharmacy must verify the prescriber’s ability to prescribe substances within a particular DEA schedule**—Some DEA registrants are not authorized to prescribe all schedules of controlled substances. Pharmacists who receive an electronically transmitted controlled substance prescription will be required to check the accompanying certificate to ensure that the prescriber is authorized by the DEA to prescribe on the appropriate schedule for the drug prescribed. This check will be inherent in all PKI-enabled systems and will be automatic and transparent to the pharmacist.
- **Pharmacy must check the status of the issuing Subordinate CA**—For prescription verification purposes it is required that the pharmacist’s computer system perform a certificate status check to ensure that the EPCS commercial CA’s certificate used to sign the practitioner’s certificate is still valid and has not been revoked by the EPCS root CA. This check will be inherent in all PKI-enabled systems and will be automatic and transparent to the pharmacist.
- **The pharmacist must electronically sign the prescription**—Pharmacists can use a PIN number/UserID combination to “electronically” sign the prescription record. The signing action is required to be performed as a *separate act* to capture the significance of the operation. Therefore, regardless of signing technology used—either PKI-based digital signature or a more

general electronic signature—the signature procedure must be performed as a separate act. The application cannot automatically generate the pharmacist's signature without notifying the pharmacist. The application will be required to reflect the same ceremony associated with the application of a wet signature. The exact electronic signature mechanism will depend on the software that the pharmacy is using.

- **The pharmacy must maintain an electronic archive of the electronic prescription for two years**—Section CFR 1304.22 defines the information that must be recorded by the pharmacist. Paper copies can not be used to replace this electronic archiving process. The pharmacy must maintain an electronic archive of all controlled substance prescriptions received electronically— including prescriptions, which are deemed to be invalid due to alteration or due to revocation or expiration of the practitioner's EPCS digital certificate.

### 5.2.5 Responsibilities of Third Party Organizations

In addition to the primary parties involved in the EPCS transactions—the practitioner and the pharmacy—there are other parties who will have involvement with electronic prescriptions. Some of these parties and their responsibilities are listed below.

- **Communications Network Provider.** The networks transporting the electronic prescription will vary from system to system. The transport may be a proprietary electronic data interchange (EDI) network, a closed system, or a public network such as the Internet. Prescriptions transmitted electronically must adhere to Government regulations regarding patient privacy. Public key encryption can be used, but the key pairs used for this purpose need not be obtained through a DEA accredited CA.
- **Electronic Prescription system vendors/providers.** Software and/or systems for creating the electronic prescriptions for controlled substances must perform all functions as required by the DEA Certificate Policy. Fields in the electronic prescription will include all required information, including the practitioner's DEA number. The application may follow the SCRIPT format endorsed by the National Council for Prescription Drug Programs (NCPDP).
- **Accrediting Firms.** Qualified Third parties may be contracted with for the purpose of obtaining DEA accreditation for the EPCS PKI enabled electronic prescription framework. DEA regulations may also require additional audits on a periodic basis. See Section 6 for more details of the audit procedures.

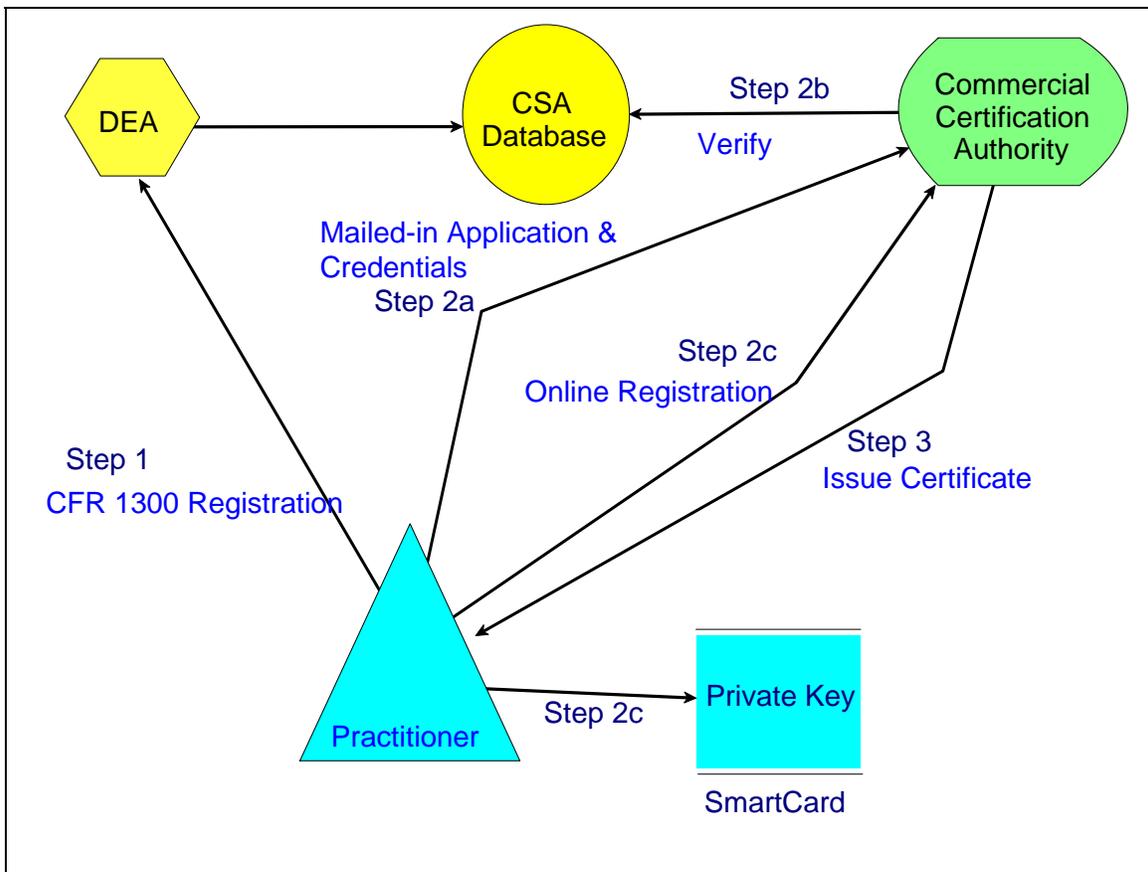
### 5.3 PKI Operational Concept

The following section provides more detail on the daily operation of the EPCS PKI.

### 5.3.1 Registration Concept of Operations

“Registration” has two contexts in the EPCS PKI. They are:

- **DEA Registration.** This registration is in accordance with CFR 1300. The existing procedure will not change.
- **CA Registration.** This is the process whereby a practitioner first submits an application to a CA —either directly or through a registration authority (RA), prior to that CA issuing a certificate for that user. A primary trust requirement is that the CA issues the certificate to the same person who registered—not an imposter. There are several methods of providing a linkage between the DEA Registration and the CA Registration. One method is shown in Exhibit 5–2. The linkage is through the registrant’s e-mail address.



**Exhibit 5–2. SAMPLE EPCS Online Registration Concept**

The procedure is outlined below:

- **Step 1—DEA Registration.** The practitioner registers with the DEA and obtains a DEA registration number. As part of the registration process, the

DEA mails (US Mail) a hardcopy of the registration to the applicant that he may use to apply for an EPCS digital certificate.

- **Step 2a—Initial Application.** The practitioner begins the registration process by obtaining an EPCS subscriber application from the Subordinate CA. Upon completion, the practitioner will have the application notarized. The applicant will also include identification information and the practitioner's DEA registration number with the application. The practitioner will forward the notarized subscriber application form via mail (US Mail) along with proof of DEA registration to the CA. The practitioner also supplies his e-mail address on the form used by the Subordinate CA. At this point, the registration process will be deferred until the Subordinate CA receives and verifies the paperwork.
- **Step 2b—Identity proofing.** The EPCS Subordinate CA checks the validity of the practitioner's information against the CSA database. The Subordinate CA could do this online. There may be some delay between the DEA registration and when a certificate can be issued. Following the validity check, a one-time userid and password will be issued via separate channels (US Mail and e-mail) to allow the applicant to access the CA's system for key pair generation. The Subordinate CA-generated userid will be sent via US Mail and the password will be sent via e-mail.
- **Step 2c—Key pair generation and Certificate request.** The practitioner accesses the registration system using the one-time userid and password. During this step, software on the practitioner's computer generates a key pair. The private key would be generated—and stored—on a "smart card." The public key is sent to the Subordinate CA in the form of a PKCS10 certificate request.
- **Step 3—Certificate Issuance.** The Subordinate CA sends the EPCS digital certificate (or a link to the certificate) via e-mail or via the online session. The practitioner's EPCS-enabled prescription application will be pre-loaded with the DEA's root CA certificate. This will be used to verify that the certificate issued by the Subordinate CA is valid.

There may be other ways to accomplish the registration, but the above procedure can be considered an acceptable baseline for purposes of this Concept of Operations. At this time, an SSL has not been determined as being necessary for the above process.

### 5.3.2 Applicant Identity Proofing Concept of Operations

Identity proofing is the process by which a Subordinate CA checks an applicant's credentials, generates a certificate from the applicant's public key, and returns that certificate to the applicant's client system and/or posts that certificate in a repository. The EPCS Certificate will have the following information about the registrant:

- Authority to prescribe specific schedules
- Business address
- Email address
- DEA Registration Number
- Employer's DEA number (When an Agents' authority is based on the institution's registration)

### 5.3.3 Key Handling Concept of Operations

The following is the concept of operation for handling the public/private key pairs used in the EPCS PKI:

- **Public key in transaction.** For the facilitation of required record keeping, the practitioner's public-key certificate must be transmitted with the signed electronic prescription transaction and must be kept by the pharmacy.
- **Archiving certificate.** The pharmacy will be required to archive the entire transaction, including the sender's public-key certificate, so that the validity of the electronic signature can be repeated at a later audit.
- **Key expiration.** All EPCS key pairs need to be changed regularly with a new key pair, and new certificates issued. For the EPCS PKI, the validity period is 1 year.
- **Key compromise.** The practitioner must protect the private key using a device that is under the sole control of the practitioner.

## Section 6 — Implementation Procedures

This section presents guidelines for those organizations interested in implementing electronic prescriptions systems for controlled substances. These systems must interface with the EPCS and provide a mechanism for satisfying the relying-party obligations defined in the DEA Certificate Policy (See Sections 4 & 5). The sections below discuss:

- The types of modifications and additions that will be required to existing practitioner and pharmacy ADP systems to incorporate PKI.
- The requirements for auditing the applications participating in the EPCS PKI.
- The requirements for archive

### 6.1 Implementation of PKI Aware Applications

As discussed in the Section 4, modifications to existing pharmacy and practitioner ADP systems will probably be required for these systems to be used for electronic prescriptions for controlled substances. The sections below discuss the implementation of the EPCS framework.

#### 6.1.1 Practitioner Systems

The following functions must be integrated into an electronic prescribing system for compliance with the DEA's Certificate Policy.

- **Private Key Protection Services.** The private signing key must be stored in a hardware device that is under the sole control of the practitioner. Client software must require a physician to authenticate before access to the private signing key is granted. Authentication can consist of either a password or a biometric.
- **Standardized Formatting.** The office automation system should present a prescription form for the practitioner to fill out. The software should format the message in a commercial standard form such as SCRIPT, with all DEA required information. After the form has been completed, the PKI software will ask the practitioner to digitally sign the form. The PKI software must use the practitioner's private key for this purpose.

The output of the above procedure will be an electronic, digitally signed prescription for a controlled substance. The method of transporting the prescription to the pharmacy is left to the vendor. As detailed below, there is a wide range of options for the actual transfer of the electronic prescriptions to the pharmacy. The following list is not intended to recommend a solution but is included to show the flexibility of the EPCS to accommodate a number of different industry or institutional implementations.

- **Proprietary network.** The electronic prescription can be sent via a proprietary network owned by a particular electronic prescription vendor.
- **Smart Card.** In the future, patients could be issued "smart cards" capable of carrying electronic prescription information to the pharmacy. The technology must insure that once the electronic prescription is read by the pharmacy, it cannot be re-used at another pharmacy.
- **Electronic Clearinghouse.** The electronic prescription can be entered into a third party clearinghouse network for download by a pharmacy. The electronic clearinghouse may be Internet-based, providing for universal connectivity. It also provides for portability, allowing a practitioner to access his account from the hospital or his office.
- **E-mail.** The electronic prescription can be e-mailed to the pharmacy. This implementation does have disadvantages: 1) The patient must select the pharmacy in advance. 2) The pharmacy selected may not be able to fill the prescription, and this presents a problem since it now has the prescription in its e-mail system.

### 6.1.2 Pharmacy Systems

In most cases, pharmacies already employ ADP systems to support the functions of filling prescriptions. The DEA understands that it would be desirable that the same system is used for receipt and processing of electronic prescriptions. The functionality that will be required for the pharmacy ADP system to participate in the EPCS is outlined below.

- **Receive electronic prescriptions.** The hardware, software, and network connectivity required to receive the electronic prescriptions will vary according to the actual implementation.
- **Verify the digital signature.** The pharmacy ADP system must be modified so that it can open the message and check the prescription's digital signature against the enclosed certificate and current CRL and ARL.
- **Check certificate status (practitioner AND subordinate CA).** The pharmacy ADP system will need a connection to the Internet to download the current CRLs (published by subordinate CAs) and ARLs (published by the EPCS root CA).
- **Archive electronic prescriptions.** The pharmacy ADP system must archive the messages as required by DEA (see sections below for more detail).
- **Reasonability checks.** The pharmacy ADP systems may already perform other functions such as checking DEA registration numbers, practitioner

names, DEA authorization, etc. in response to information entered by the pharmacist.

## **6.2 Certification of EPCS Components**

This section describes the Certification/Accreditation procedure for certificate authorities and software applications that wish to operate under EPCS PKI. The purpose of the certification/accreditation process will be to assure that CA and software applications follow the requirements of DEA EPCS Certificate Policy.

### **6.2.1 Certification of Subordinate CA Systems**

A Subordinate CA operating under the EPCS Root CA will be required to abide by the guidelines set forth in the EPCS Certification Policy. Before DEA approves a Subordinate CA for operation, the CA must first demonstrate that the following elements of the PKI operation are conducted according to EPCS standards:

- \* Key Generation and Management
- \* Physical Security
- \* Network Security
- \* Operational Practices
- \* Validation Practices
- \* Compliance and Testing

To assure that subordinate CAs operate according to the EPCS Certificate Policy they will be required to undergo Certification and Accreditation by a third party auditor to obtain a report on compliance with WebTrust for Certification Authorities principles and criteria. AICPA/CICA WebTrust for Certification Authorities—developed by the American Institute of Certified Public Accounts (AICPA)—is an accreditation process developed specifically for organizations acting as CAs.

The Standard for Attestation Engagements was issued as a new standard for reporting business activities of certification authorities. The attestation report will provide third party assurance on compliance with specified requirements. The report covers the CA business practice disclosure, service integrity (key life cycle management controls, certificate life cycle management controls), and environmental controls.

### **6.2.2 Certification of PKI-enabled Commercial Systems**

The DEA's certificate policy defines the set of relying party obligations that must be satisfied in any implementation of an electronic system for prescribing controlled substances. Software vendors that implement electronic prescription systems must

provide systems that meet these standards. The vendor will be required to perform a yearly audit—conducted by a third party— of the application to ensure that the system correctly performs the required practitioner obligations. Pharmacists and other relying parties who use these systems must maintain an adequate, readily accessible, electronic archive to provide the DEA with the ability to audit electronic prescriptions when necessary to ensure that the obligations have been met.

### 6.3 Requirements for Audit of an EPCS Commercial CA

The EPCS commercial CA will be certified initially by an external auditor capable of performing Information Technology audits and will have a periodic external audit performed to assure that it operates according to the EPCS Certificate Policy and the EPCS Certification Practice Statement.

- **Frequency of Audit**—To demonstrate compliance with EPCS Certificate Policy, CAs are expected to provide an attestation report from a third party auditor on a yearly basis or at any time that a significant change is made to their operations.
- **Qualification for Auditor**—An independent auditor qualified to perform an audit on a CA will conduct the audit.
- **Results of Audit**—Results of the CA audit will be presented to DEA to determine the CA's accuracy and compliance with EPCS Certificate Policy.

### 6.4 Requirements for Archive

Pharmacies participating in the EPCS PKI must archive the electronic prescription records for the length of time now required by the regulations for paper prescriptions. Steps must be taken to insure the integrity of the electronic prescriptions during the required archive period. These steps include:

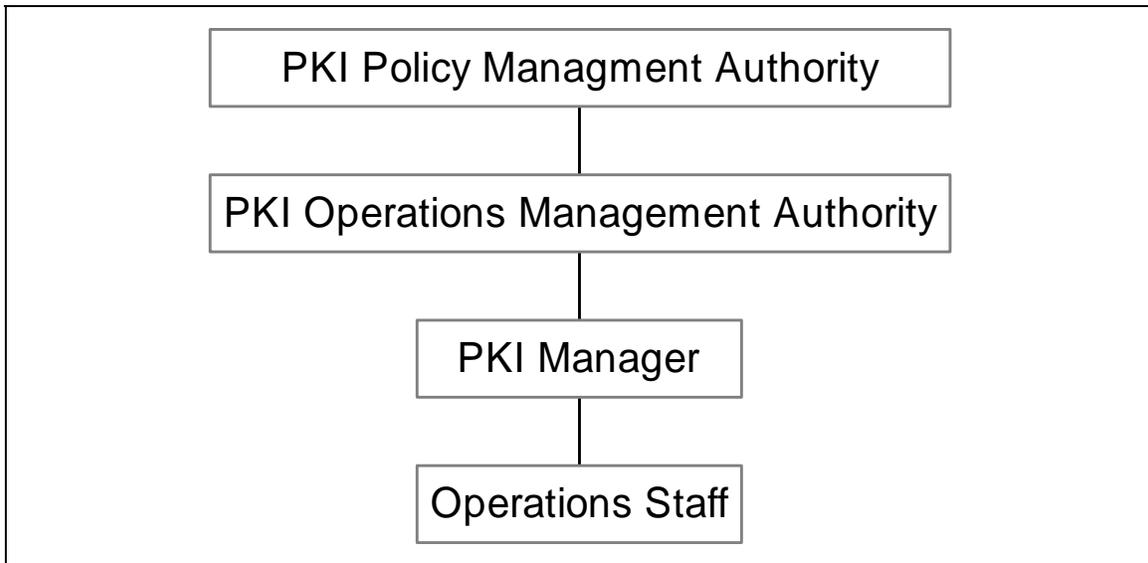
- **Retain the entire electronic prescription message.** The pharmacy must retain the certificates associated with the electronic prescription message to provide for auditing the validity of the electronic signatures at a later time.
- **Retain copies of CRLs.** The Certification Authority must retain copies of all CRLs it publishes to assist in auditing the validity of the electronic signatures.
- **Trusted time stamp.** The pharmacy must use a trusted time-stamp service so that the date and time of receipt of the electronic prescription are known in a trustworthy fashion.
- **Regular Backups.** The pharmacy must take precautions to safeguard against data loss. The pharmacy must make periodic backup copies of the archive to protect against accidental erasure or corruption.

- **Media selection.** The pharmacy must ensure that the actual storage media is sufficient to meet DEA's standards for a two-year storage period.
- **Physical safeguards.** The pharmacy must store electronic archives in a fireproof vault, possibly off-site.
- **Backwards Compatibility.** Software manufacturers must make certain that newer releases of the pharmacy software can read and validate an electronic signature made in within 2 years. This may require retaining previous versions of the software, or portions of it.

## Section 7 — Control and Management Structure of EPCS PKI

### 7.1 Introduction

This section describes the control and management structure of the EPCS PKI as depicted in Exhibit 7-1.



**Exhibit 7–1. EPCS PKI Management Structure**

### 7.2 Policy Management Authority

The Office of Diversion Control will establish an EPCS PKI Policy Management Authority (PMA). The PMA is responsible for defining, implementing, and managing certificate policy decisions regarding the EPCS PKI. The PMA is composed of Office of Diversion Control personnel, its contractor and/or a combination of both.

#### 7.2.1 Responsibilities

The PKI PMA is responsible for certification and accreditation of the overall PKI implementation and has responsibility for oversight of all PKI operations. It is responsible for maintaining and publishing the Certificate Policies for EPCS PKI. The PKI Policy Management Authority is also responsible for the following:

- (1) Approving and revoking certificates of Commercial Certification Authorities and Registrants.
- (2) Ensuring appropriate use of PKI facilities throughout the EPCS PKI.

(3) Maintaining and publishing the Certificate Policy.

The PKI PMA commissions annual audits of PKI operations.

### 7.2.2 Cyclical and Routine Activity

The EPCS PMA meets quarterly or as required to conduct routine business at a time and place announced by the Chair. An agenda is prepared in advance and distributed by the chair. Typically the agenda will include the following items:

- The *Monthly Operations Report* submitted by the PKI Operations Authority
- Staffing changes within the PKI Operations Authority and Registration Authority domain
- Pending changes to policies or other PKI management directives
- Review of PKI-related procedures and record-keeping practices
- Review of Commercial Certification Authority applications which are being considered for approval
- Review matters of consideration presented by Commercial PKI enrollees
- Changes to the PKI configuration (hardware, software, location, etc.)
- Proposed and pending enhancements and expansions.
- Incidents and non-routine events
- Interfaces with other organizations
- Changes in standards or technology.
- Acquisitions, contract performance, and budgetary issues
- Special reports and studies commissioned by the Chair

Based on these meetings, the Chair may issue directives relative to PKI policy and operations. The Chair may also direct research or planning assignments related to current or potential PKI policies and operations.

On an **annual** basis the PKI PMA will:

- Commission an independent compliance audit of the EPCS PKI: its policies, plans, procedures and operations. (The PKI PMA may suggest areas for audit attention but may not limit the scope of the audit.)

- Review the audit results and issue directives to effect improvements as necessary.
- Review the Certificate Policy and Certification Practice Statement and approve revisions as necessary.

### **7.2.3 Procedural Requirements**

The PKI PMA will adopt and publish procedures it may deem necessary to discharge its responsibilities and conduct its business efficiently.

### **7.2.4 Reporting and Record Keeping Requirements**

The PKI PMA will maintain such records as necessary to support its activities and determine the PKI reporting and record keeping requirements for Commercial Certification Authority enrollees.

## **7.3 Operations Management Authority**

The PMA will establish a 24 hour/day, 7 days/week Operations Management Authority (OMA) to carry out the policy of the PMA. The OMA provides planning guidance to, and oversight of the PKI infrastructure, and directs the activities of the EPCS PKI Manager and the PKI manager's staff. The OMA is composed of Office of Diversion personnel.

### **7.3.1 Responsibilities**

The OMA has overall responsibility for proper and reliable operations of the EPCS PKI Root CA and for seeing that the policies and directives of the Policy Management Authority are carried out. It is responsible for establishing and approving detailed operating procedures. Responsibilities of the PKI Operations Management Authority include:

- Developing, maintaining currency, and publication of the Certification Practice Statement.
- Establishing and monitoring PKI security procedures.
- Oversight of PKI operations.
- X.500 Directory operations.
- Identifying and investigating areas for PKI improvement.
- Reviewing Certification Authority operations and activity.
- All technical, hardware and software aspects of the PKI.
- Reviewing PKI functional, technical, staffing, and budgetary plans.

### **7.3.2 Cyclical and Routine Activity**

The PKI OMA meets weekly to conduct routine business at a time and place announced by the chair. Typically the agenda might include:

- Review of outstanding problems and action items reported by the PKI Manager
- Incidents and non-routine events
- The *Weekly Operations Report* prepared by the PKI Manager
- PKI usage and activity patterns
- Directory usage and activity patterns
- Changes and trends in technology
- Configuration management issues
- PKI maintenance and technology life-cycle plans
- Directory maintenance and technology life-cycle plans
- Requirements analysis of potential PKI applications
- Requirements analysis of potential Directory applications

On a **daily** basis, the Chair may receive PKI related communications from or meet with the PKI Manager, the PMA, and other elements of the EPCS PKI.

### **7.3.3 Procedural Requirements**

The PKI OMA will adopt and publish procedures it deems necessary to discharge its responsibilities and conduct its business efficiently.

### **7.3.4 Reporting and Record Keeping Requirements**

The PKI OMA will maintain such records as necessary to support its own activities and monitor the PKI reporting and record keeping of the PKI Manager. It will comply with any PKI reporting requirements established or endorsed by the Policy Management Authority.

## **7.4 PKI Manager**

The PKI Manager staffs and operates the EPCS PKI on a day-to-day basis and assures that it is functioning properly, that all procedures and safeguards are being followed, and that any operational errors, anomalies, and breaches of policy and procedure are addressed promptly and properly. Because the PKI itself is a trust-oriented service, it is

essential that the PKI Manager institute, and consistently follow, operational procedures that promote reliability and trust. The PKI Manager will be subordinate to the OMA. The PKI Manager and its staff may be Office of Diversion personnel, may be contractor personnel or may be a combination of both.

#### **7.4.1 Responsibilities**

The PKI Manager staffs and operates the Certificate Authority (CA) Workstation and its associated directories, repositories and communication facilities. The PKI Manager is responsible for developing and maintaining PKI plans, policies and procedures pertaining to operation of the Certificate Authority and the overall operation of the PKI. This includes:

- Implementing the policies and directives of the PMA and the OMA
- Physical security of the CA workstation
- Information security for the PKI
- Staffing and assignment of duties for PKI personnel
- PKI staff training
- Development of CA's operating procedures
- Liaison with vendors
- Development and operation of help desk for end users
- Operating and maintaining the CA workstation
- Operating and maintaining the X.500 directory
- Maintaining inventory records
- Maintaining official CA records and activity logs
- Evaluating new technology
- Maintaining and refreshing existing technology
- Certification of Commercial Certificate Authorities
- Disaster recovery procedures
- Acquiring, issuing, and maintaining records related to tokens and readers

## 7.4.2 Cyclical and Routine Activity

The PKI Manager provides availability of the Certificate Authority and its associated directories on a 24 hour/day, 7 days/week basis except for brief pre-announced periods as may be necessary for maintenance. The availability of the Directory is a prerequisite for end-user signature verification and encryption activity.

On a **daily** basis, the PKI Management staff will:

- Monitor Certificate Authority Workstation Activity on an hourly basis
- Issue Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs) as required
- Issue, accept, and revoke Commercial Certification Authority certificates as required
- Verify the physical security and integrity of the CA Workstation facility
- Receive new hardware and software

On a **weekly** basis, the PKI Management staff will:

- Prepare the Weekly Operations Report
- Run the weekly audit cycle and produce the weekly system audit report
- Review hardware token inventory levels and reorder as needed.

On a **monthly** basis, the PKI Management staff will:

- Produce and store backup copies of Certificate Authority database and journals off-site
- Review adequacy of PKI configuration and recommend improvements if necessary.
- Review adequacy of PKI procedures and make improvements as necessary

On an **annual** basis, the PKI Management staff will:

- Support the annual compliance audit
- Test (and replace where necessary) archival files

On an **as-required** basis, the PKI Management staff will:

Immediately report processing or procedural anomalies or violations to the Operations Authority.

### **7.4.3 Procedural Requirements**

The PKI Manager will establish and publish detailed procedures for all aspects of the Certificate Authority operations. The procedure documentation and its associated records will be sufficient to permit verification by independent auditors that the PKI Manger is fully compliant with the policies and directives of the Policy Management Authority and the Operations Management Authority. At a minimum, the PKI Manager procedure set will encompass the following:

- Routine Certification Authority Workstation procedures
- Hardware Token Inventory procedures
- Encryption Key Recovery procedures
- Disaster Recovery procedures

### **7.4.4 Reporting and Record Keeping Requirements**

The PKI Manager is responsible for developing and maintaining procedures, records, and periodic reports required to meet four requirements:

- They must demonstrate the integrity of the EPCS PKI.
- They must comply with policy and directives issued by the Policy Management and Operational Management Authorities.
- They must comply with the EPCS data processing, security, and asset management policies.

## **Section 8 — Compliance with Federal Standards and Requirements**

### **8.1 Introduction**

The following sections summarize the enacted Federal legislation that 1) supports the use of PKI for digital signature or 2) gives legal basis for the use of digital signatures.

### **8.2 Electronic Signatures in Global and National Commerce Act**

The “Electronic Signatures in Global and National Commerce Act,” S.761, was signed by the President on June 30, 2000 and will be effective on October 1, 2000.

The Act clarifies the legal validity of electronic contracts, signatures, notices, and other records, and allows contracting parties to choose the technology for authenticating their transactions without government intervention. The Act will also ensure that on-line consumers will have legal protections equivalent to those in the off-line world.

The Act does not diminish the protections offered by any Federal or State law relating to the rights of consumers, other than to eliminate requirements that contracts and other records be written and signed on paper. Consumers retain the choice to do business and receive records on paper or online. Before notices and disclosures may be sent electronically, consumers must give their consent and the firm must verify that the consumer will be able to access electronically the information that will be provided.

**ELECTRONIC SIGNATURE.** The term “electronic signature” means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

### **8.3 Government Paperwork Elimination Act (GPEA)**

The 105th Congress, 2d Session, signed the Government Paperwork Elimination Act (GPEA) into law on October 8, 1998. The Act mandates the electronic availability of Government agency forms, questionnaires and surveys. In the case that a signature is required, an electronic signature may be used as an equivalent to a “wet” (ink) signature.

The Act establishes the legal foundation for the acceptance and use of electronic signatures. Congress seems to feel that “there is no meaningful difference between contracts executed in the electronic world and contracts executed in the analog world, such contracts should be treated similarly under Federal law.”<sup>1</sup> The GPEA defines electronic signature in section 11 as a method of signing an electronic message that:

---

<sup>1</sup> GPEA §9

- (1) identifies a particular person as the source of such electronic message; and,
- (2) indicates such person's approval of the information contained in such electronic message.

“Electronic signatures shall not be denied legal effect, validity or enforceability as long as they are in accordance with set procedures and guidelines.”<sup>2</sup> The GPEA has charged the Office of Management and Budget (OMB) with the responsibility to establishing procedures and guidelines for the implementation of the GPEA.

#### **8.4 OMB Proposed Implementation of the GPEA**

The Office of Management and Budget (OMB) has issued a proposed implementation of the GPEA to the Federal Register, Vol. 64, No. 43, March 5, 1999. In their guidelines, the OMB recognizes the strength of Public/Private Key Cryptography in comparison to other electronic signature techniques, and identifies PKI as the strongest method of assuring identity. This distinction is reflected by the fact that the OMB defines digital signature in the context of Public/Private key cryptography. The OMB guidelines point out that an agency's policies and procedures for the operation and maintenance of a PKI are an essential component of trust that binds a person's identity to a digital signature.

#### **8.5 FDA, HHS 21 CFR Part 11**

The Food and Drug Administration (FDA) issued its final rule regarding the criteria for FDA's acceptance of electronic records and electronic signatures for records requirements set forth in agency regulation. The ruling was posted in the Federal Register, vol. 62, no. 54 on March 20, 1997. The ruling specifically requires the use of digital signature technology in certain cases—as opposed to the lower assurance provided by generic electronic signature. The ruling provides FDA with the discretion to decide what submissions it will accept electronically. The FDA will post in a public docket the types of submissions that it is prepared to accept electronically.

The FDA has defined controls for two types of computing environments.

- **Closed System**—“an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.”
- **Open System**—“an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.”

---

<sup>2</sup> GPEA §6

The requirements for the use of electronic records and signatures in an open system differ from those required in a closed system in two ways. First, digital signatures are required in an open system—rather than electronic signatures. Second, the confidentiality of the electronic record must be maintained along with the authenticity and integrity of the record's contents, from the instance of the record creation to the instance of the record's receipt.

## **8.6 HCFA, HHS 45 CFR Part 142**

The Health Care Financing Administration (HCFA) issued a *Notice of Proposed Rulemaking* (NPRM) for a security and electronic signature standard. The HCFA NPRM is applicable to transactions defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This ruling will effect all health care plans, providers and clearinghouses that maintain or transmit health care information electronically. The regulations define health care information as, ” (1) information received or created by health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual”.

HCFA's current proposed standard for security and electronic signature standards strongly identifies PKI as the most viable technology that will insure the proper level of protection for health care information.

"Currently there are no technically mature techniques that provide the security service of non-repudiation in an open network environment, in the absence of trusted third parties, other than digital signature- based techniques. Therefore, if electronic signatures are employed, we would require that digital signature technology be used."<sup>3</sup>

The HCFA NPRM does not mandate the use of any one type of technology over another nor are they requiring the use of electronic signature. However, they recognize the necessity for electronic signatures for a completely paperless environment. HCFA does not define the services of digital signature to include a PKI. It does state that a PKI is a required infrastructure for digital signature, “that may necessitate the expenditure of initial and recurring costs for users.”<sup>4</sup>

The strength of electronically binding a certificate to an identity is also founded on the soundness of the mathematical framework of the enabling technology. It is dependent on

---

<sup>7</sup> Vol. 63, No. 155, Federal Register pg. 43257 (Aug 12, 1998)

<sup>4</sup> Vol. 63, No. 155, Federal Register pg. 43260 (Aug 12, 1998)

the policies and procedures that are adopted in the operation and maintenance of the enabling technology. HCFA has outlined requirements that address such issues.

The need to utilize technical standards that are maintained by a recognized standards body for the enabling security technology is an integral aspect of any security system. Employing standards assures that the enabling technology survives and evolves with changes in technology.

### **8.7 National Conference of Commissioners on Uniform State Law (NCCUSL)**

States are acknowledging the need to establish uniform laws and regulations governing the legally binding nature of digital signature. The NCCUSL is a non-profit unincorporated association, comprised of state commissions on uniform laws from each state, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands. NCCUSL has put forth two uniform state acts to be adopted by state lawmakers.

- Uniform Electronic Transaction Act (UETA) 7/23-30/1999—Approved by NCCUSL
- Uniform Computer Information Transaction Act (UCITA) 7/23-30/1999—Approved by NCCUSL provides conditions for the legal acceptance of electronic signatures.

### **8.8 American Bar Association (ABA)**

The Information Security Committee (ISC) the Electronic Commerce Division of the ABA has been addressing law initiatives since the Division's formation in 1992. The ISC published digital signature guidelines in August 1, 1996. The guidelines are intended to provide a framework that will:

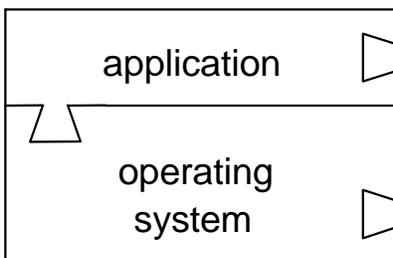
- (1) minimize the incidence of electronic forgeries
- (2) enable and foster the reliable authentication of documents in computer form
- (3) facilitate commerce by means of computerized communications, and
- (4) give legal effect to the general import of the technical standards for authentication of computerized messages.

The ISC is also currently preparing Public Key Infrastructure Assessment Guidelines (PAG). The PAG will provide guidelines for the evaluation, assessment, determining compliance with stated policies, and licensing of PKIs. The PAG is intended for two audiences' (1) those assessing PKI providers, and (2) those providing PKI products and services.

## Appendix A — Fundamentals of making an Application PKI Aware

A PKI enabled or aware application is an application that incorporates functionality, which permits the application to use the security services provided by a PKI.

The process of understanding how an application can be transformed into a PKI enabled application begins by considering the following diagram depicting an abstract view of the relationship between an application and operating system. Exhibit A-1 shows an application's executable file being supported by the underlying operating system.

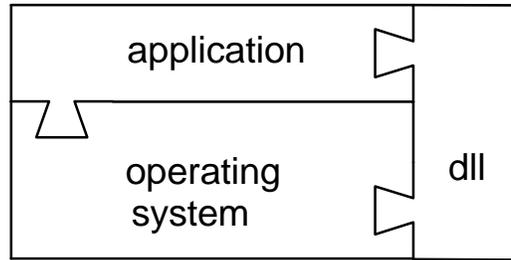


**Exhibit A-1. Application and Operating System.**

In Exhibit A-1, the interface between the two elements includes a geometric detail, illustrated as a dovetail, that suggests the “joining” of the application to the operating system. This joining aspect is accomplished by program code that “calls” and links the application executable to the operating system at runtime.

Normally, applications use their own built-in program code to perform most activities, but they also rely upon code of the underlying operating system, the kernel, to perform other basic functions. For example, an application may call operating system code to save a copy of working data to permanent storage.

An application may also need other functionality that does not exist in the application executable file or in the kernel of the operating system. If so, it can achieve this functionality by calling additional code known as *dynamically linked library* (DLL) files. The DLL file is a mechanism to extend the functionality of the operating system. This concept is illustrated in Exhibit A-2.



**Exhibit A–2. Adding Functionality Using a Dynamically Linked Library.**

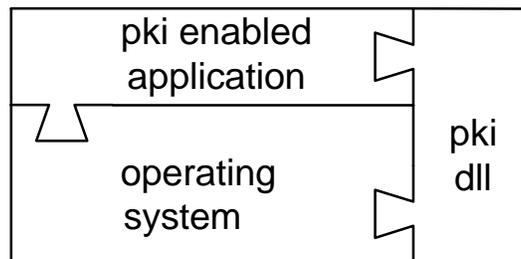
In practice an application may call many different DLL files. In Exhibit A-2 a single DLL file is shown functioning as an extension of the application and the operating system.

DLL files can be created to fulfill a need for special functionality using software development tools known as “toolkits.” The DLLs can be created to consist of multiple software modules, as many as are necessary to embody multiple functionality. As a further step, the application is modified to call the created DLL. The modification should include modifying the application user interface (GUI) to provide a means to invoke the desired functionality resident in the DLL. In this way, DLLs are incorporated into the application using standard programming procedures.

The PKI enabling process uses the above process to incorporate PKI DLL files into existing applications as follows:

1. create a PKI DLL,
2. modify the application so a user can invoke, and the application call, the DLL,
3. and incorporate the DLL into the application environment.

Exhibit A–3 shows the end result of this process.



**Exhibit A–3. PKI Enabled Application.**

As an example, the created PKI DLL may contain the following software modules: encryption and decryption algorithms, digital signing module, and validation module. Modifications to the application that would be required include: for example, adding a GUI action button to the user interface to permit a user to invoke the PKI enabled

functions, i.e., an on-screen button that is identified to initiate a digital signing action to an e-mail.

The above process is specific to the Windows 9x/NT/2000 OS environment having dynamically linked libraries; however, similar processes are applicable to other environments.

In conclusion, there exists multiple PKI toolkits for creating DLLs for various applications. PEC evaluated six of the most widely used toolkits for functionality. Using the process described above, three of the toolkits were tested by PKI enabling Internet browsers and e-mail clients. The tests were successful and demonstrated the practicality of the process.

## Appendix B – Listing of Acronyms

ACF	Access Control Facility
ASAP	American Society for Automation in Pharmacy
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CFR	Code of Federal Regulations
CN	Common Name
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
CSOS	Controlled Substance Ordering System
DEA	Drug Enforcement Administration
DN	Distinguished Name
DUR	Drug Utilization Review
EDI	Electronic Data Interchange
EDT	Electronic Data Transmission
EMR	Electronic Medical Records
EPCS	Electronic Prescriptions for Controlled Substances
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard

FPKI	Federal Public Key Infrastructure
GOC	Government Of Canada
GPEA	Government Paper Elimination Act
HCFA	Health Care Fraud Alert
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HMO	Healthcare Maintenance Act
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRM	Information Resource Management
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
LTCF	Long Term Care Facility
MCP	Multiple Copy Prescriptions
NABP	National Association of Boards of Pharmacy
NARA	National Archives and Records Administration
NCCUSL	National Conference of Commissioners on Uniform State Law
NCPDP	National Council for Prescription Drug Programs
NIST	National Institute of Standards & Technology

NPI	National Standard Health Care Provider Identifier
NPRM	Notice of Proposed Rule Making
NPS	National Provider Service
NTP	Narcotic Treatment Programs
OD	Office of Diversion Control
OMA	Operations Management Authority
OMB	Office of Management and Budget
PBM	Pharmacy Benefit Management
PEC	Performance Engineering Corporation
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMA	Policy Management Authority
POC	Proof Of Concept
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, & Adleman
Rx	Prescription
TCP/IP	Transmission Control Protocol / Internet Protocol
UCF	Universal Claims Form
UCITA	Uniform Computer Information Transaction Act
UETA	Uniform Electronic Transaction Act
UID	Unique Identifier
VA	Veterans Affairs

VPN	Virtual Private Network
X.500	The standard for directory services
X.509	The standard for PKI certificates
XML	Extensible Markup Language