Public Key Infrastructure Analysis

Controlled Substances Ordering System

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 13, 2000

Prepared by
PEC Solutions, Inc.

Section 1 — Introduction

1.1 Overview and Background

Under the authority of the Controlled Substances Act of 1970, the Drug Enforcement Administration, 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 controlled substances into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. Chapter 21, Code of Federal Regulations, Parts 1300-1316 sets forth in detail the authority and responsibilities of DEA in this area. It is further intended that these control systems prevent the introduction of contraband controlled substances into the legal distribution channels.

The Controlled Substances Ordering System (CSOS) Public Key Infrastructure (PKI) is designed to bring to this regulatory process the advantages of PKI. CSOS will: (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) *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; (b) *integrity of communications*- it will be possible for the recipient of a message to determine if the message content was altered in transit; (c) *technical non-repudiation*- the originator of a message can not convincingly deny to a third party that the originator sent it. Confidentiality of communications will not be included initially but remains an option for the future.

1.2 Objectives of the CSOS POC PKI

The Federal Code of Regulations Title 21, Parts 1300-1399 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, for examples, manufacturing, distributing, dispensing, research, etc., are required to register with the DEA unless otherwise exempted from registration as described in sections 1301.22, 1301.23, or 1301.24.

Registrants fall into two categories, labeled Type A and Type B, as shown in Table 1–1.

Type A	Type B
Retail Pharmacy	Manufacturers
Hospital/Clinic	Distributors
Practitioner	Researcher
Teaching Institution	Analytical Lab
Mid-Level Practitioner	Importer
	Exporter
	Narcotic Treatment Program

Table 1–1. Registrant Categories

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 CSOS PKI project:

- ❑ implements a PKI for use by industry electronic ordering systems involving the transfer of controlled substances between manufacturers, distributors, retail pharmacies, hospitals and other dispensing registrants;
- ❑ focuses on high volume registrants, Manufacturers, Distributors and Retail Pharmacies;
- ❑ and enhances the regulatory process through the use of PKI.

1.3 General Information

This document—the *Controlled Substances Ordering System Concept of Operations* – has been prepared by PEC Solutions (PECS) for the Drug Enforcement Administration's Office of Diversion Control (OD).

Prior documentation produced in support of this task is identified below. It should be noted that previous documents use the term "MADI" to identify this project. However, to be more descriptive of the scope of the project, the term MADI has evolved into the acronym "CSOS," for Controlled Substances Ordering System. For purposes of understanding this project's history, from now on the terms MADI/CSOS should be considered synonymous.

Previous documents delivered are:

CSOS PKI Analysis and Design Program Plan dated 7/9/99 established the project goals and requirements and defined the approach that would be used to accomplish the CSOS project.

- *CSOS PKI Certificate Policy Requirements Analysis* dated 2/3/00 examined industry security practices, identified stakeholder security requirements, and analyzed issues that will affect the level of assurance upon which the CSOS PKI will be implemented.

- *CSOS PKI Existing Network Infrastructure Analysis* dated 2/3/00 examined industry business processes, network and application infrastructures to determine the extent to which existing infrastructures could be utilized in the CSOS PKI.

This CONOPS provides a conceptual overview of how the Public Key Encryption Infrastructure (PKI) will be implemented to bring the security services of authenticity, integrity and non-repudiation to the controlled substances ordering process. It defines how the system can be operated from both Industry and DEA's perspective. This CONOPS provides the following:

- A single high level CSOS PKI reference document for DEA decision-makers, representatives of the regulated industry, potential users and relying parties of the CSOS PKI.

- A comprehensive approach for establishment of the CSOS PKI Proof of Concept (POC).

- Serves as the basis for detailed implementation, planning, development, and direction for the operations of the CSOS.

1.4 Document Organization

The document is organized into the following sections:

Section 1 Introduction: The introduction provides a description of CSOS and provides an overview of the goals and objectives of CSOS.

Section 2 Current Environment: This section provides an overview of the current environment- stakeholders, current processes and security requirements.

Section 3 PKI Overview: This section provides an overview of PKI- benefits, and the fundamental components that make up PKI.

Section 4 Design Concept of the Controlled Substances Ordering Process PKI: This section describes the design concept of the new electronic ordering process- roles, responsibilities, assurances, how requirements are met and how the new ordering process will work.

Section 5 PKI Operations: This section provides detail level descriptions of procedures and operations for the CSOS PKI.

Section 6 Implementation Procedures: This section describes the implementation procedures for the CSOS PKI and the new electronic ordering process.

Section 7 Control and Management of the CSOS PKI: This section describes the control and management structure of the CSOS PKI.

Section 8 Compliance With Federal Standards and Requirements: This section describes the various Federal standards and requirements that the CSOS PKI adheres to and reasons for any variance from those standards.

Appendix A – Fundamentals of Making an Application PKI Aware

Appendix B – Data Requirements for Ordering Applications

Appendix C – List of Acronyms

Section 2 — Current Environment

2.1 Introduction

This section provides an overview of the current environment; who are the stakeholders in the process, what are the current processes, processing volumes (transaction volumes), and impact of the paper process, network architectures and security requirements.

2.2 Current Controlled Substances Distribution Environment

2.1.1. Stakeholders in Controlled Substances Distribution

Stakeholder groups that are directly or indirectly involved in the controlled substances handling process are organized and defined here into high level groups for the purposes of this project. Each stakeholder's specific role in the current paper process is defined.

DEA uses the terms "supplier" and "customer" to describe the roles of Registrants that use DEA 222 Forms to order controlled substances. The customer fills out a DEA 222 Form and sends it to the supplier.

Industry uses the term "***inbound*** DEA 222 Form" to describe a DEA 222 Form coming in to a supplier. The term "***outbound*** DEA 222 Form" is used to describe a DEA 222 Form sent out by a customer. The terms inbound and outbound indicate a perspective on the flow of the process. Each DEA 222 Form is inbound to the supplier and outbound from the customer.

❑ **Manufacturers**

Manufacturers are suppliers. They process ***inbound*** DEA 222 Forms that are received from their customers. Some manufacturers also transfer controlled substances internally using the DEA 222 Form.

❑ **Distributors**

Distributors are both customers and suppliers. In the customer role, they send DEA 222 Forms ***outbound*** to the manufacturer. In the supplier role, they receive DEA 222 ***inbound*** Forms from their customers (i.e. pharmacies, hospitals and other dispensing registrants).

❑ **Chain Drug Stores**

Chain Drug Store Distribution Centers act as suppliers processing ***inbound*** DEA 222 Forms from their own stores (customers). They also act as customers and process ***outbound*** DEA 222 Forms from their headquarters facility to manufacturers. Those

Chain Drug Stores that ***do not*** centrally warehouse and distribute controlled substances utilize the services of an independent distributor.

- **Pharmacies**

  Pharmacies, acting as customers, send ***outbound*** DEA 222 Forms to a distributor to be filled. Pharmacies typically have one main distributor and, in a few cases, have a back up distributor, or may order small quantities from other pharmacies.

- **Other Dispensing Registrants**

  Other dispensing registrants, such as hospitals, drug treatment centers, researchers, etc., acting as customers, process ***outbound*** DEA 222 Forms to a distributor; and, in a few cases, directly to a manufacturer to be filled.

- **Pharmacy Boards/State Regulators**

  Information contained on DEA 222's may be made available as needed to State regulators and/or Pharmacy Boards for investigative purposes.

- **DEA Headquarters and Local DEA Field Offices**

  DEA Headquarters issues DEA 222 Forms to registrants. The issued DEA 222 Forms are completed by the distributor or manufacturer in the supplier role, and the green Supplier copies are forwarded periodically to the local DEA Office. Additionally, DEA Headquarters receives "Automation of Reports and Consolidated Orders System" (ARCOS) reports which are prepared using information extracted from the Supplier's copies of the 222 Form. The ARCOS reports are sent monthly to DEA Headquarters.

2.1.2 Current Controlled Substance Ordering Process

The current paper ordering process is described in Exhibit 2–1. Current Controlled Substance Order Process.

Customer registrant first orders preprinted sets of DEA Form 222 from DEA Headquarters.

1. **Customer Creates Order–** the Customer registrant (Pharmacy Manager, Pharmacist or Purchasing Agent) fills out a DEA 222 Form at their location. It is then mailed to the Supplier or given to the Supplier's driver. In most cases, the Customer has also placed electronic orders with the Supplier which are then validated for Schedule II controlled substances using the DEA 222 Form.

2. **Supplier Receives and Validates Order–** the DEA 222 Forms are taken to the Supplier's Customer Service and quality checked. The DEA 222 Forms are entered into the distributor's computer order entry system and multiple checks are made by

the system concerning the validity of the DEA registration, the State registration and other customer profile attributes (size of order, frequency of order).

3. **Supplier Fills the Order–** the DEA 222 Forms are sent to controlled substance vault area and picking/packing lists are created. The order is picked from the vault and the DEA 222 Form is completed with order information and cross-checked with the computer entry order. The order may be cross- checked again and the order is shipped.

4. **Customer Receives and Completes DEA Form 222–** Upon the order being delivered from the Supplier, the Customer registrant (Pharmacy Manager, Pharmacist or Purchasing Agent) fills in the receiving portion of their original copy of the DEA 222 Form. Their copy of the original completed DEA 222 Form is then filed securely.

5. **Supplier Sends DEA Copies–** After it is annotated with the shipping information, one copy of the DEA 222 Form is retained at the distributor's site; and one copy is forwarded to the local DEA office.

6. **Local DEA Receives Copies–** Once the DEA 222 Forms are completed by the distributor or manufacturer when they are the suppliers, the green copies are forwarded periodically to the local DEA Office. The copies are made available to state and local governments or other regulatory authorities as needed.

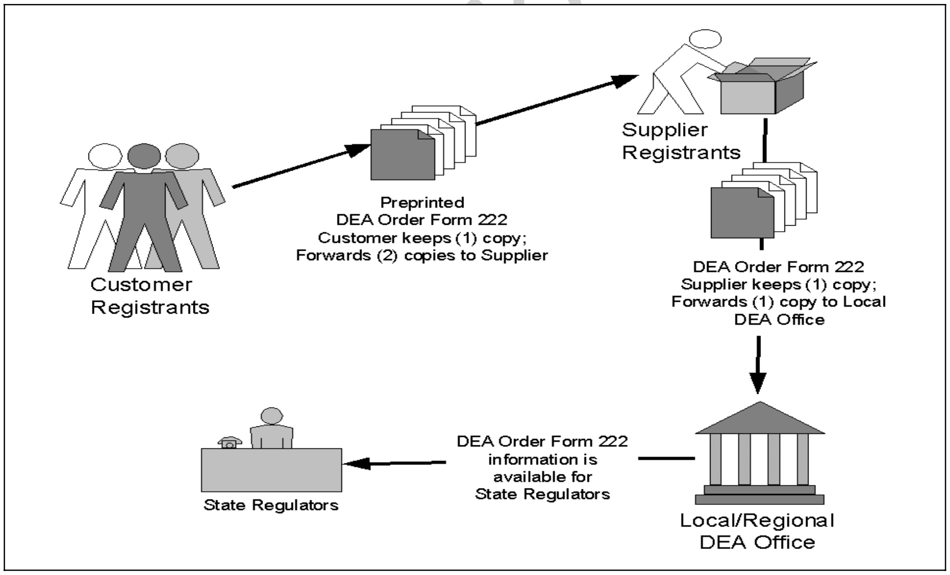


Exhibit 2–1. Current Controlled Substance Order Process

2.1.3 Current Paper Transaction Volume and Impact of the Paper Process

Dependent on their role in the supply chain, the current paper DEA 222 regulatory process impacts industry stakeholders differently. Exhibit 2–2. Yearly Volume of Controlled Substance Transactions per Type of Industry Stakeholder shows the volume of

DEA 222 forms processed on a yearly basis. As the exhibit indicates, there are two industry stakeholder groups who are impacted by the current process more substantially than all others- Distributors and Chain Drug Store Distributors that distribute their own controlled substances.

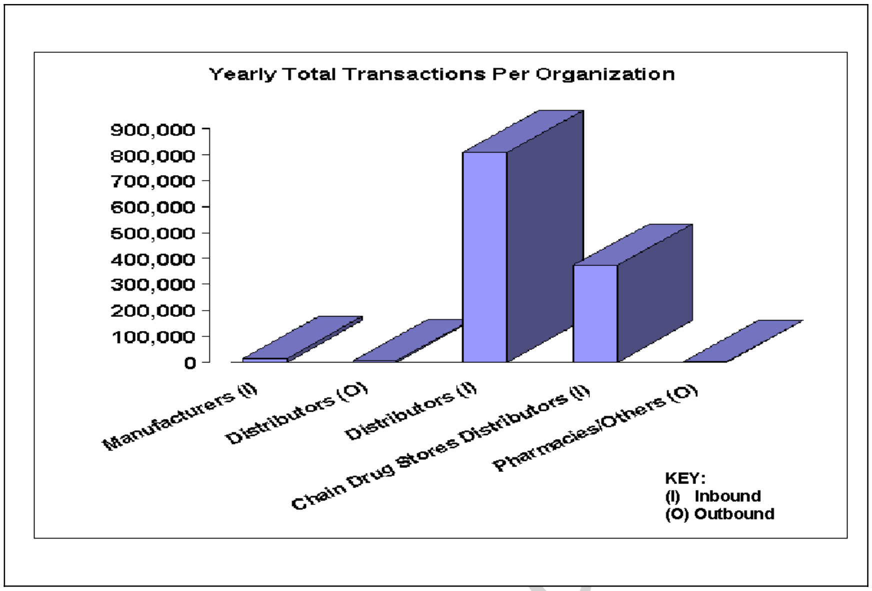


Exhibit 2–2. Yearly Volume of Controlled Substance Transactions per Type of Industry Stakeholder

2.1.4 Existing Technology Infrastructures

The next exhibit, Exhibit 2-3, shows the high level view of the current industry network architectures. There are two distinct architectures that cover the majority of all registrants: 1) a client server type architecture where the client application dials up the host server and sends data, and 2) an electronic data interchange (EDI) architecture that utilizes the X.12 standard and communicates data through a value added network.

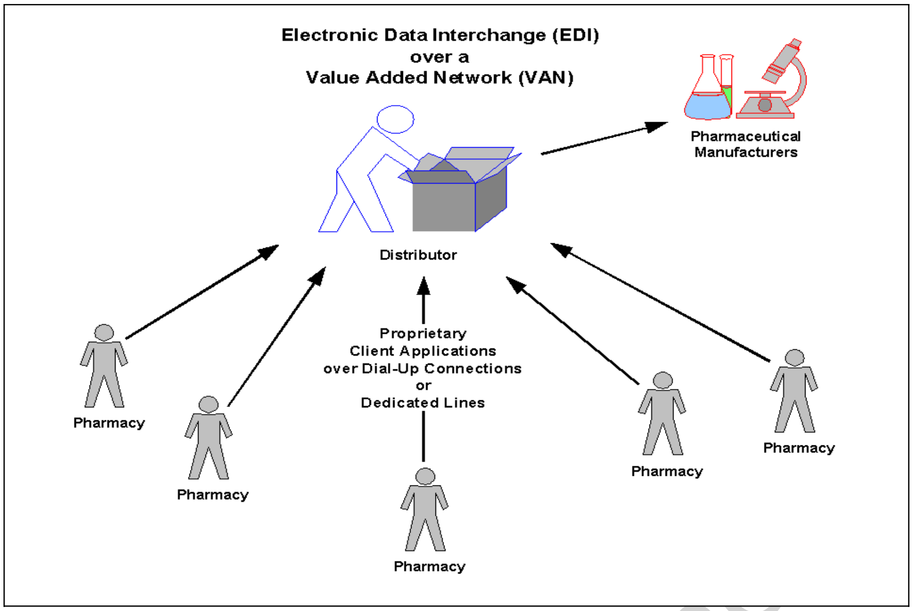


Exhibit 2–3. Current Industry Network Architecture Connections

The client server architecture is used by suppliers that provide the client application to their customers (pharmacies, hospitals) to place orders by dialing up the supplier's system and forwarding the order (same system to same system). Suppliers use the EDI architecture to place orders with manufacturers (disparate system to disparate system).

At this time only a very limited amount of business is conducted over the Internet between interested trading partners. However, in view of the Internet's potential for business opportunities, network architectures and applications are being aggressively investigated by industry for future use to replace older legacy architectures and applications.

2.1.5 Certificate Policy Requirements Analysis

The current level of security, both physical and logical, that surrounds the DEA Form 222 ordering process is adequate for the current paper process. A substantial number of manual controls, physical security controls and auditing procedures surround the current paper process. As a result, little or no diversion of controlled substances occurs involving this process. The vast majority of errors in the current paper process involve arithmetic errors, human errors and changes to registrant information. All stakeholders indicated that all of the PKI security services, with the exception of confidentiality, would be required in the new system.

- ❑ **Authentication-** Industry registrants need to know that the sender of the controlled substance order is in fact a valid registrant with the authority granted from DEA to order controlled substances.

- **Integrity-** Industry registrants need to be certain that the controlled substance order sent has not been altered in transit.

- **Technical Non-Repudiation-** Industry registrants need to be assured that the sender will be unable to convincingly deny having sent the order.

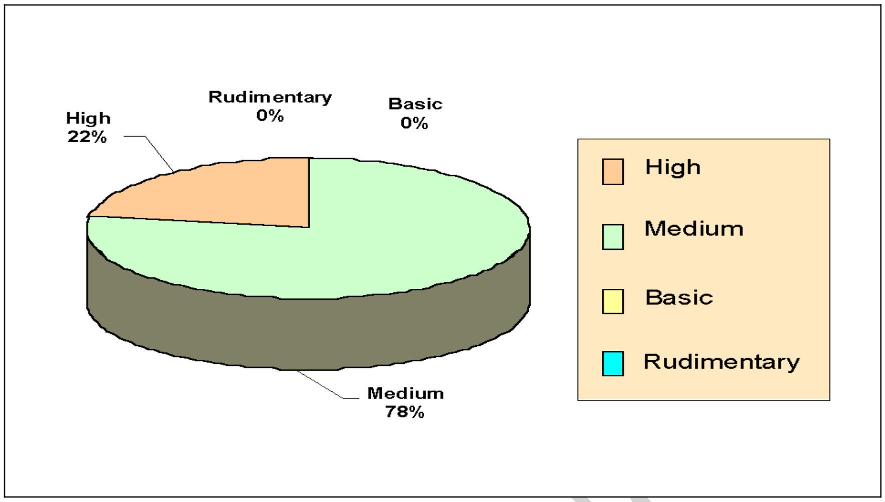


Exhibit 2–4. Required Level of Security (DEA Response)

Based upon responses received from both DEA and Industry, as shown in Exhibits 2-4 and 2-5, the CSOS PKI will be operated at a medium level of security assurance.

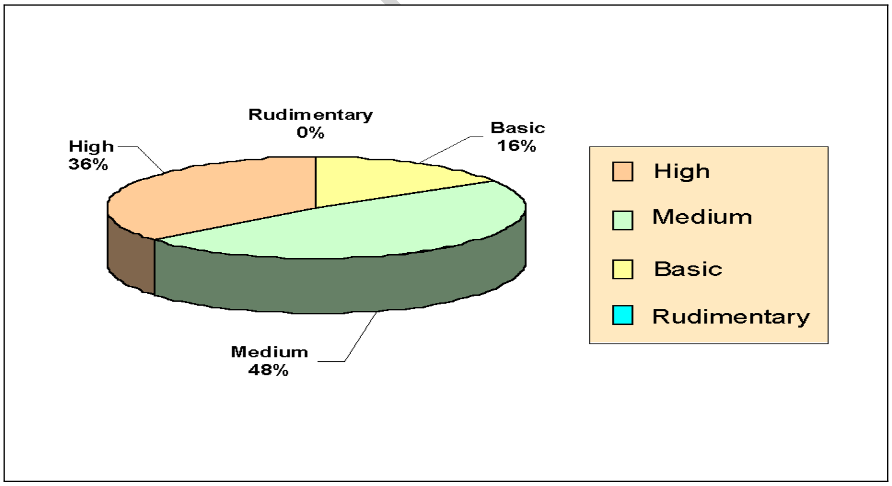


Exhibit 2–5. Required Level of Security (Industry Response)

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."

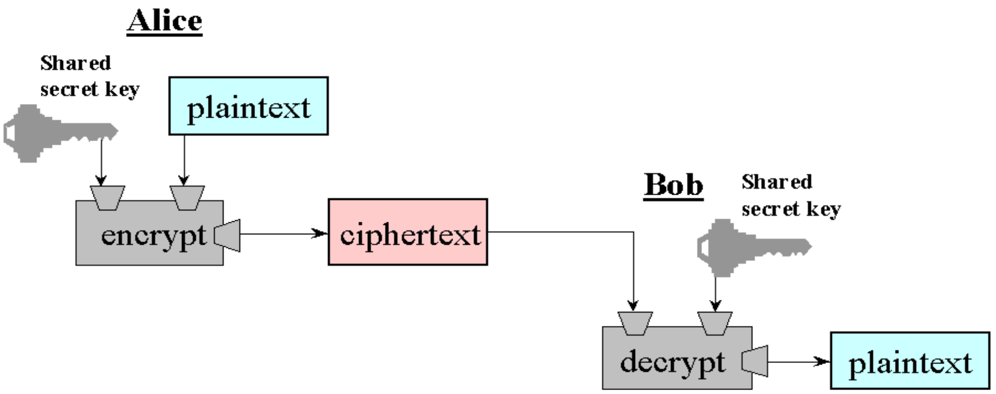
3.4.2 Public Key – The PK in PKI

- **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.



Alice and Bob both have the secret key.
The encrypt/decrypt algorithm is a standard that both have agreed on.
This same secret key is used for encryption and decryption.
This type of cryptography is relatively fast.

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 himself 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.

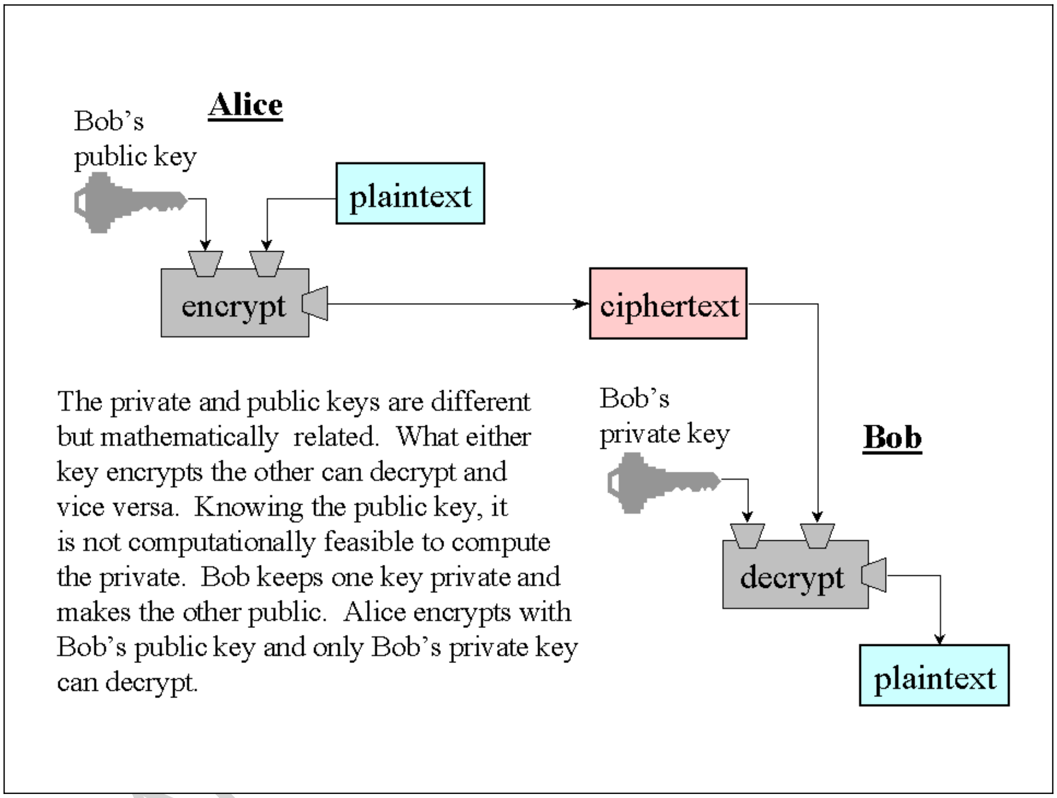
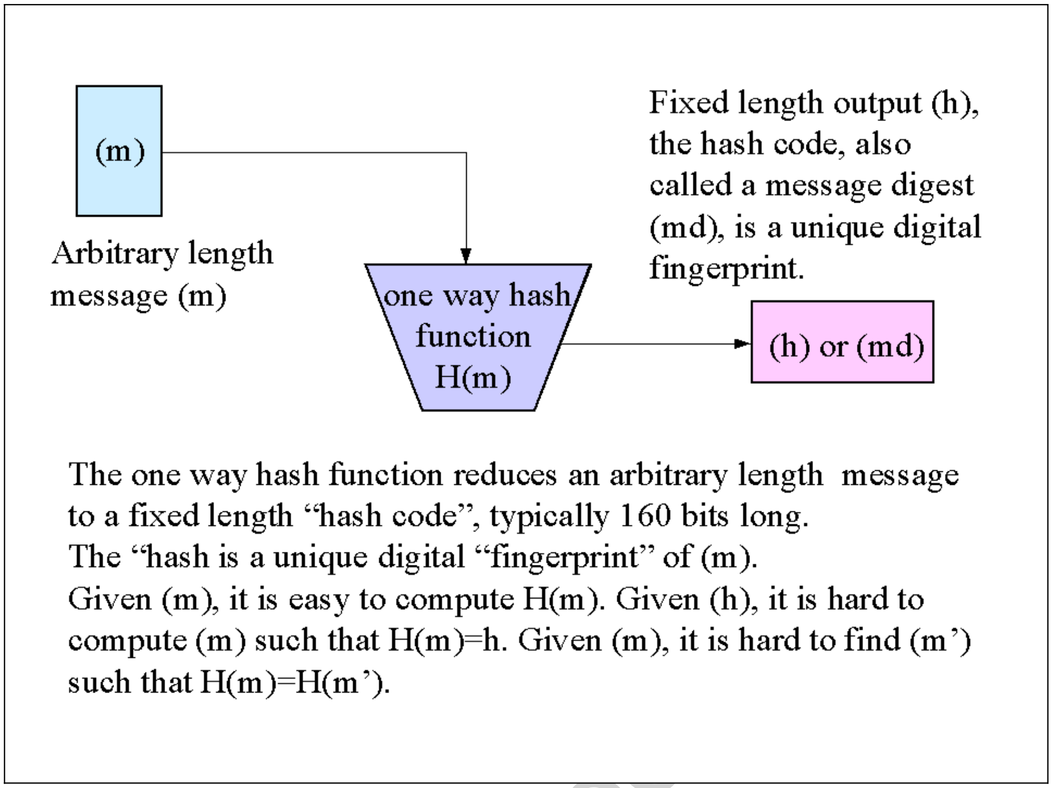

Alice
Bob's
public key
plaintext
encrypt
ciphertext
The private and public keys are different but mathematically related. What either key encrypts the other can decrypt and vice versa. Knowing the public key, it is not computationally feasible to compute the private. Bob keeps one key private and makes the other public. Alice encrypts with Bob's public key and only Bob's private key can decrypt.
Bob's
private key
Bob
decrypt
plaintext

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.


(m)
Arbitrary length message (m)
one way hash function H(m)
Fixed length output (h), the hash code, also called a message digest (md), is a unique digital fingerprint.
(h) or (md)

The one way hash function reduces an arbitrary length message to a fixed length “hash code”, typically 160 bits long.
The “hash is a unique digital “fingerprint” of (m).
Given (m), it is easy to compute H(m). Given (h), it is hard to compute (m) such that H(m)=h. Given (m), it is hard to find (m’) such that H(m)=H(m’).

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.

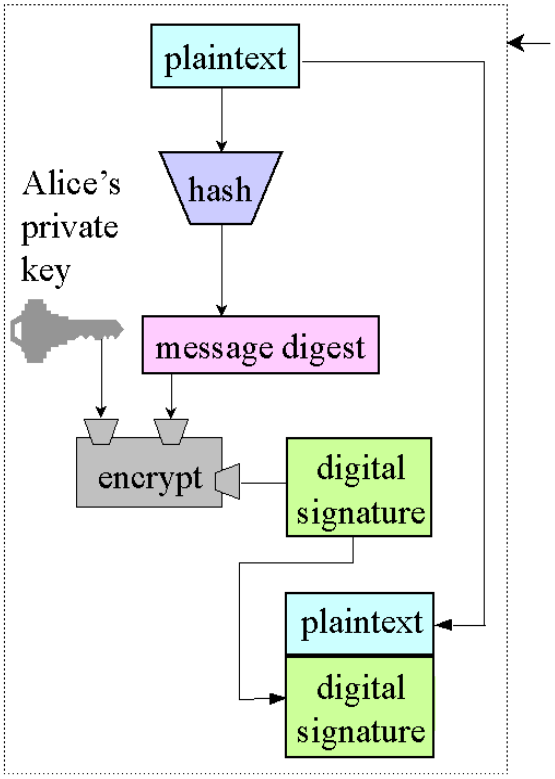
The digital signature process results in a bit string that allows a recipient of a message to verify the identity of the signer of the message and the integrity of the message. Any one of several digital signature algorithms can generate the bit string. These algorithms have the generic characteristic 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.



Digital Signature Creation: Alice "hashes" the plaintext document. Next, she encrypts the message digest with her private signing key. This encrypted digest is her digital signature, a "mark" on the document that only she could have made. The digital signature is then attached to the original plaintext document and sent to the intended recipient.

Digital Signature Verification: The recipient, Bob, "hashes" the plaintext document. He then decrypts Alice's signature with her public key. He next compares the "hash" he obtained with the "hash" in Alice's signature. If they are identical, then the digital signature is verified.

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:

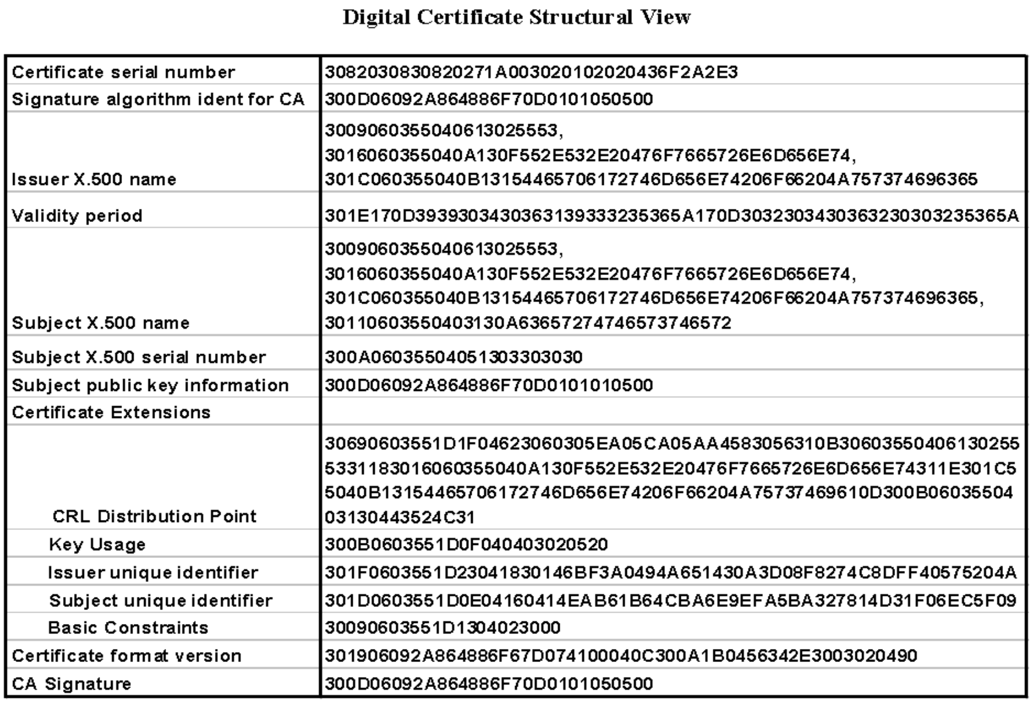
❑ Certification Authority (CA)

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	300906035504061302555З, 3016060355040A130F552E532E20476F7665726E6D656E74, 301C060355040B13154465706172746D656E74206F66204A757374696365
Validity period	301E170D3939303430363139333235365A170D3032303430363230303235365A
Subject X.500 name	3009060355040613025553, 3016060355040A130F552E532E20476F7665726E6D656E74, 301C060355040B13154465706172746D656E74206F66204A757374696365, 30110603550403130A63657274746573746572
Subject X.500 serial number	300A06035504051303303030
Subject public key information	300D06092A864886F70D0101010500
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 Server (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.

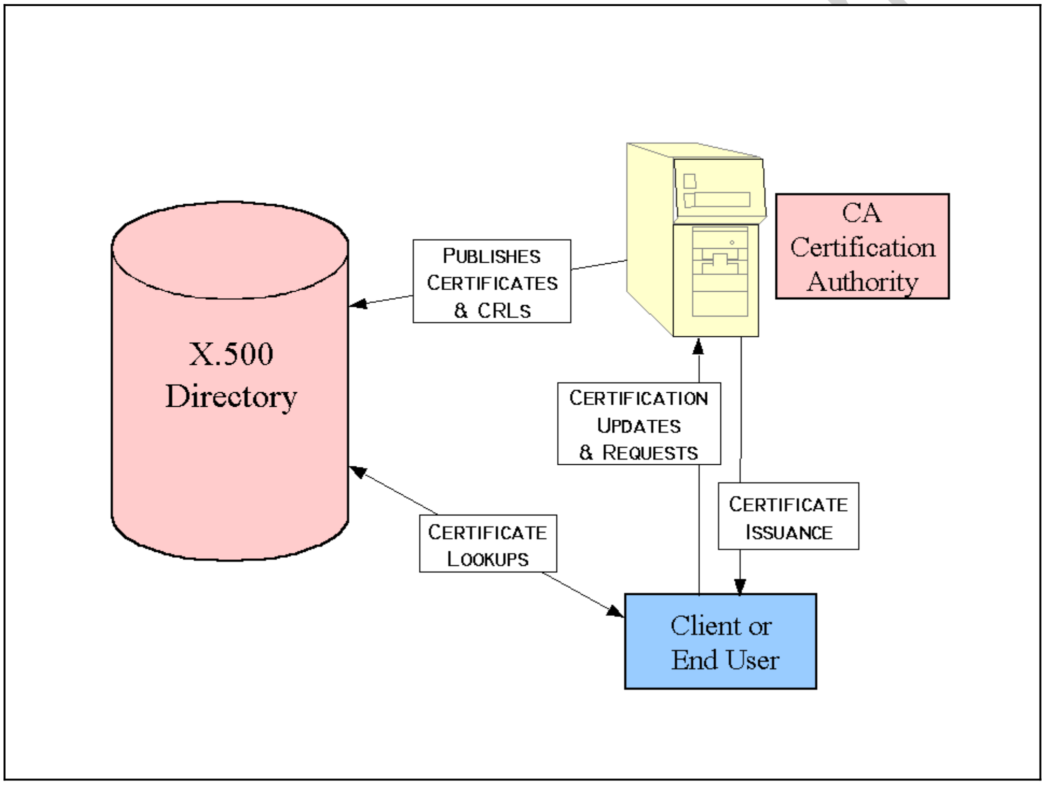


Exhibit 3–6. PKI Functions Performed

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 an 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 it's 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 CSOS 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 it's 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 untrusted 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 — CSOS PKI Design Concept

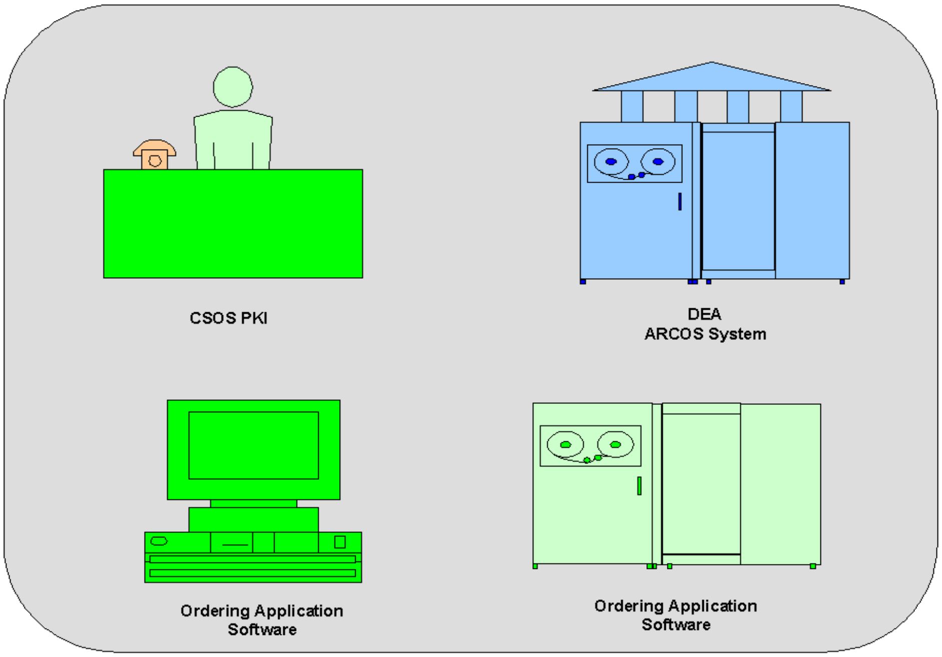


Exhibit 4–1. Controlled Substances Ordering System (CSOS)

4.1 Introduction

This section introduces the concept of operations for the CSOS PKI. It discusses information flow between PKI components from both functional and network viewpoints. This section discusses:

- ❑ *The CSOS PKI functional design concept*, presenting the concept of operations for the information flow between the DEA, the Customers, the Suppliers, and the CSOS PKI components.
- ❑ *The CSOS PKI network design concept*, presenting the concept of operations for connectivity between the DEA, the Customers, the Suppliers, and the CSOS PKI components.
- ❑ *The CSOS PKI certification authority design concept*, presenting the concept of operations for trust model for the CSOS PKI.

A result of the “Certificate Policy Requirements Analysis” and the “Existing Network Infrastructure Analysis” was discovering that the scope of the MADI PKI was broader than originally conceived by DEA and PEC. The original MADI PKI project was renamed to “Controlled Substances Ordering System,” or CSOS, a more appropriate project title which now includes the PKI, the software applications to be PKI enabled and the business processes that use these technologies.

The entire “Controlled Substances Ordering System” is composed of three major components: the PKI, the PKI enabled ordering applications, and the back end DEA reporting system (associated with ARCOS). Each component exists independent of the other, but is dependent on and integrated with the other, to supply all necessary services to accomplish the regulatory process.

4.2 Design Concept of the Controlled Substances Ordering System

4.2.1 Design Goals and Requirements

In developing a design concept for the CSOS, PEC was provided with:

1) Project Goals;

2) DEA High Level design requirements and constraints; and,

3) DEA and Industry design requirements.

The goals, constraints and design requirements were gathered from interviews, meetings and documentation from the Stakeholders in DEA and Industry. These goals, constraints and requirements have provided the guidance necessary to produce the Concept of Operations for the CSOS.

While we recognize that it may not be possible to meet all requirements in a single, universal design, the design brought forward here represents what we believe to be the synthesis of these goals, constraints and requirements.

To synopsize the most important design goals, constraints and requirements:

- The CSOS must meet all legal requirements for the current DEA 222 Form.

- Additionally, the CSOS needs to provide the security services of the current DEA 222 Form and thereby maintain the “closed system of controlled substances distribution.”

- Achieving industry consensus and providing a system with the maximum user acceptance will be an important aspect of this project.

- Utilize and leverage existing business processes and technology infrastructures to the maximum feasible extent.

- Employ standards-based technology and COTS solutions.

- The CSOS will only be an option; the current paper process will remain for those that choose to continue to use it.

In conclusion, the CSOS design presented has addressed these goals, constraints and requirements to the maximum extent possible and achieved the following project goals:

1) **Reducing the amount of paper in the process**

   Eliminates the paper DEA Form 222 entirely by utilizing existing industry electronic ordering systems, archive and technical infrastructures.

2) **Speeding transaction times**

   Transaction times for controlled substances orders will now be processed in virtually the same amount of time as any other order to a supplier.

3) **Lower the costs per transaction**

   The additional costs associated with paper processing and the manual processes around the current controlled substance ordering system will be eliminated. Certain stakeholders indicated that the savings to their organizations would be substantial, perhaps on the order of a dollar per transaction.

4) **Introducing Security Services into the process.**

   The regulatory process will be enhanced with the following additional PKI security services:

   (a) ***authentication of sending party*** – the recipient will be able to positively identify the sender of a message (order) and subsequently to demonstrate to a third party, if required, that the sender was properly identified as a valid registrant at that time;

   (b) ***integrity of communications* –** it will be possible for the recipient of an order to determine if the order content was altered in transit to make certain the order was not changed;

   (c) ***technical non-repudiation* –** the originator of an order can not convincingly deny to a third party that the originator sent the order. That is, it is provable that only the registrant originating an order could have sent the order, given that the registrant has maintained the security of their private key.

5) **Enhancing DEA’ s ability to perform law enforcement responsibilities.**

   DEA will have improved capabilities to electronically receive and process information from Industry registrants. The turnaround time to receive supplier information will be greatly improved. The ability to analyze information received to uncover trends and potential violations will also be facilitated. The on-site inspection or audit can be conducted more efficiently, using the existing electronic reporting and archiving system available at the registrant’s site.

4.2.2 Components of the CSOS Functional Architecture

The CSOS architecture includes connectivity, interaction and processing among multiple organizations and networks. The architecture incorporates existing industry electronic ordering system with new security technology to create an integrated Controlled Substances Ordering System.

The components of the CSOS architecture are:

- **CSOS Certification Authority**

  The CSOS Certification Authority (CA) will be established and operated under the auspices of the DEA. The role of the CA will be to issue certificates to entities and then manage the use of those certificates.

- **CSOS CA X.500 Directory with LDAP Access**

  CSOS will establish an X.500 Directory to be the repository of all valid registrants' certificates, CA certificate, a copy of the Certificate Policy, and a copy of the required Certificate Revocation List (CRL). The CRL must be accessed each time an order is processed by a Supplier to determine whether the Customer has a valid DEA registration. However, in order to avoid the substantial communications overhead of accessing the directory each time an order is placed, the client or local system will periodically "cache" (i.e., *temporarily store*) the Directory's CRL so this access to the CRL can be performed locally.

- **Industry Supplier PKI Enabled Applications**

  There is a requirement to PKI enable existing Industry Supplier ordering and shipping client applications, so that they will have the PKI functionality necessary under the CSOS system. Appendix A provides a brief overview of the process of making an application PKI aware. The following applications require this modification to perform the indicated functions:

  1) **Industry Supplier PKI Enabled Ordering Application**

     The existing Industry Supplier ordering application software, or that software now used to generate non-controlled substance orders, will be modified into a PKI enabled client application. The modification will permit the ordering application to utilize DEA provided digital certificates to digitally sign controlled substance orders.

  2) **Industry Supplier PKI Enabled Ordering Application Host**

     The existing Industry Supplier Customer Service host application software, that accepts orders generated from the Customer, will be modified into a PKI enabled client application. This will permit the application to access the CSOS Directory to retrieve (and "cache") the CRL to permit verification of the digital signature of the Customer prior to the order being processed by the Suppliers' system.

3) **Industry Supplier PKI Enabled Shipping Order Fulfillment Application**

The Industry Supplier shipping/order fulfillment application that processes the controlled substance orders for shipping will require integration of a client PKI application. This PKI modification will enable the shipping/order fulfillment application to digitally sign the Supplier's report to DEA. This digital signature activity is a mathematically secure process performed by the PKI enabled application to assure the order's integrity. This signing process is not equivalent to, but must be distinguished from the concept of a handwritten signature. The Supplier's electronic report of the transaction to the DEA will be known as the Controlled Substance Transaction Report (CSTR) and replaces the green copy of the 222 Form that is presently forwarded to the DEA. The existing regulations will be changed to reflect the ability of this electronic system to report the required information in a more timely and secure fashion without unduly burdening Suppliers. Therefore, in the new system each report shall be received by the DEA within a 24-hour period after each transaction occurs. Most importantly, by transitioning to this electronic process, Suppliers are no longer required to handle, store or send the DEA the paper copy of the 222 Form. Within this system, the 222 Form disappears entirely.

❑ **DEA CSOS CSTR Reporting System**

After completion of a controlled substance order, a report will be forwarded to DEA Headquarters. As stated above, this report is called the CSTR report. The CSTR report will contain the same fields as the green copy of the 222 form; there will be no new information required. For network efficiency and/or convenience, the CSTR reports may be automatically or manually batched and submitted at a time of low network utilization. The DEA CSOS Reporting System will accept the digitally signed report, validate the supplier digital signature and archive the report. It is expected that the information in the report will be made available through the Firebird System to Local DEA Field Offices.

❑ **ARCOS Reporting**

The ARCOS Report is a periodic report showing all transactions (e.g., purchases, sales, losses, and disposals) of all Schedule II substances and all transactions of Schedule III narcotics down to the retail level as reported by all manufacturers and distributors. The ARCOS report is created by the Supplier and can be submitted on paper or on electronic medium, as in the present system, but there is no provision at this time for electronic transmission to DEA. The ARCOS reporting process will remain unchanged. In the future, combining the CSTR report (i.e., all Supplier Schedule II transactions which may be batched) and the ARCOS report is planned, but initially they shall remain two distinct regulatory requirements.

4.2.3 Description of Operational Design Concept

The CSOS design incorporates existing infrastructure elements from within DEA and Industry and adds a specific security infrastructure for a complete system. Using a CSOS CA issued digital certificate, Industry registrants will be allowed to send and receive electronic controlled substances orders. Using existing PKI enabled Industry applications and communications channels, CSOS allows for electronic record keeping for controlled substances throughout the entire DEA regulatory process.

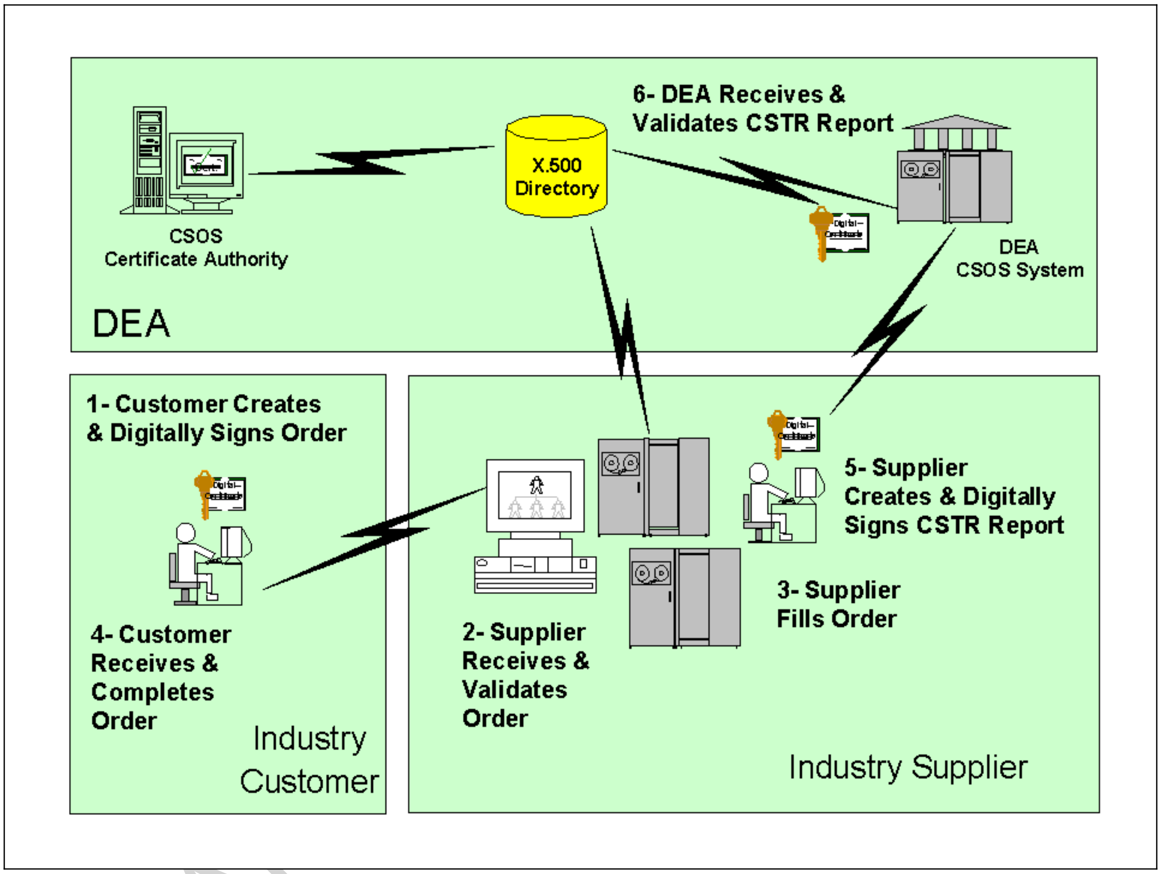


Exhibit 4–2. CSOS Operational Design

The key features of the CSOS Design include:

- **CSOS CA Issued Digital Certificates**. Industry registrants, who currently manufacture, distribute, or dispense controlled substances will be issued digital certificates to be used in placing and transacting controlled substances orders.

- **PKI- Enabling of Industry Systems.** Industry registrants that wish to use the "CSOS Option" for placing electronic controlled substances orders and regulatory reporting, will need to incorporate specific changes into their existing application software systems to allow for digital signatures and certificate handling.

- **Electronic Validation of Customer Registrant and Validity of Order.** Industry Suppliers using the CSOS will check the validity of the public certificate matching the private key used to sign the order. This will establish the identity and current DEA registration of the customer. In the CSOS system, only orders that have been signed will be sent. Upon checking the validity of the order, an order may be received as "valid" or "invalid." If received as "invalid," for example, because the order initiator was no longer a current DEA registrant, then the Customer will be informed that the order was invalid and that the order could not be processed.

- **CSOS Business Process closely matches the Current Industry Ordering and Fulfillment Process.** The CSOS regulatory process has been designed to closely follow existing business processes and practices, eliminating manual paper handling and human intervention as much as possible.

- **New Regulatory Electronic Record Keeping Process.** A new regulation and electronic process specific to the CSOS system will be developed in order to allow Industry registrants to implement the CSOS system as an option.

- **Certification of Industry Systems.** Industry registrants using the CSOS option will be required to demonstrate that their systems comply and that they are operated in the manner specified in the new regulations. A third party will periodically audit CSOS PKI enabled ordering systems. The third party audit will be similar to, but less burdensome, than the SAS-70 type audits.

- **CSOS Regulatory Option.** The CSOS is an electronic option to using the paper DEA Form 222.

4.3 CSOS PKI Network Architecture

The connectivity requirements in the CSOS functional architecture shown in Exhibit 4-3 below include both dialup lines and the Internet. All participants utilizing the CSOS PKI will need an Internet connection to the CA to perform an initial and yearly CSOS registration and to communicate on an ongoing basis with the DEA Directory. Some of the key features of this architecture are:

- The network architecture utilizes the existing connectivity between the Customers and the Suppliers.

- This network architecture will allow Customers and Suppliers to have the required connectivity to the CSOS CA and CSOS Directory (which includes the CRL) with a single connection to the Internet.

- To avoid the communications overhead of accessing the CRL directory each time an order is placed, the Customer and Supplier systems will be permitted to "cache" (i.e. *temporarily store*), the CRL information from the CSOS Directory. The caching procedure will be provided in the CSOS Design Plan.

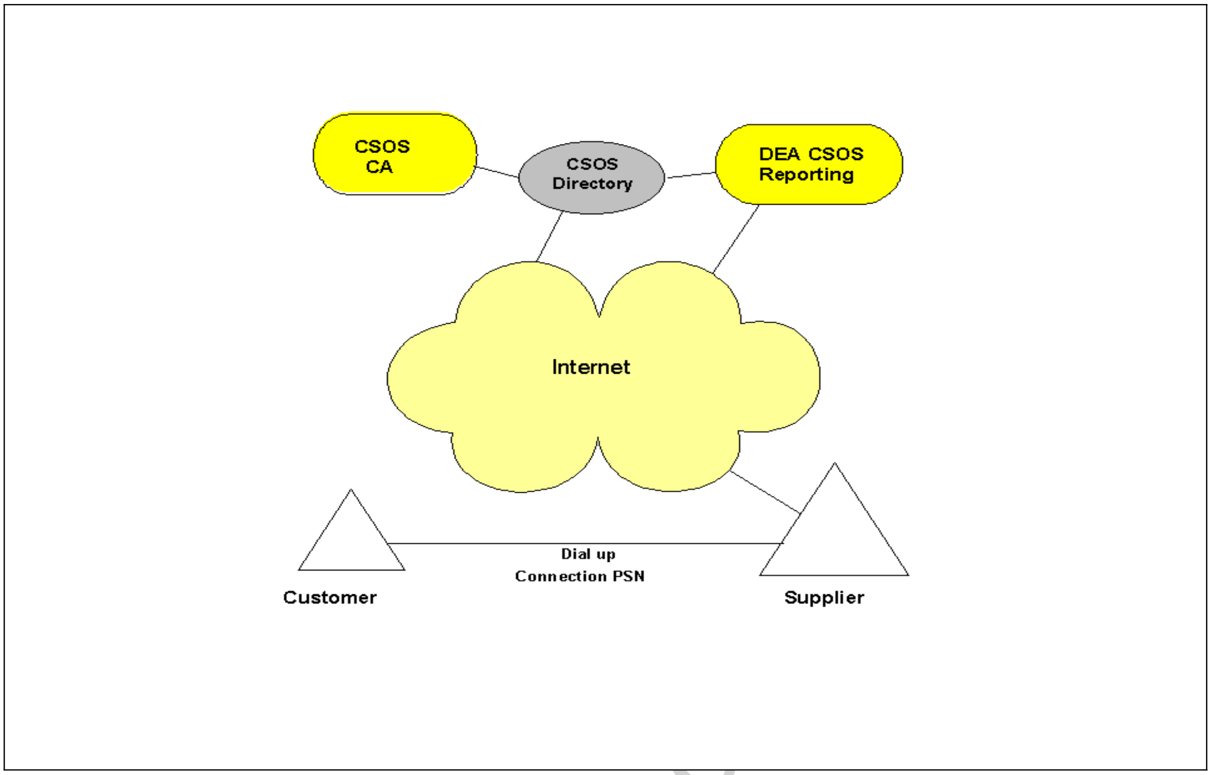


Exhibit 4-3. CSOS Network Architecture

4.4 CSOS PKI Design Concept

The CSOS PKI will exist solely for the use of DEA and DEA valid registrants and holders of power of attorney from a registrant who are authorized to handle controlled substances.

4.4.1 CSOS PKI Trust Model

The CSOS PKI will provide third party (CSOS CA) trust to enable electronic controlled substances transactions to occur securely amongst industry trading partners. The trust model will be a single CA with many users.

Level of Assurance

The CSOS PKI will be operated as a medium level assurance PKI. The CSOS CA CP will describe fully the meaning of this medium level of security.

Set forth below are details of the CP, which characterize a medium level policy implementation.

1	Overview	The CSOS PKI will be operated under the authority of the DEA Office of Diversion Control Policy Management Authority (PMA). The purpose of the CSOS PKI is to bring the security services of authenticity, integrity and non-repudiation to the DEA 222 Form 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 a CSOS PKI PMA. The PMA is responsible for setting, implementing, and managing certificate policy decisions regarding the CSOS 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 (OMA)	The PMA will establish an OMA. The OMA will carry out the policy of the PMA The OMA will direct the activities of the CSOS PKI Manager. The OMA is composed of Office of Diversion personnel. It will be at least 1 full time position.
4	The PKI Manager	The PKI Manager will run the CSOS 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 CSOS PKI is limited to DEA employees and DEA Registrants and the holders of valid power of attorney from DEA Registrants who meet all other requirements. The certificates are limited in applicability to the signing of orders by persons engaged in the manufacture, distribution, and dispensing of Controlled Substances and to the signing of official transactions to DEA.
6	Certification Authority	The CSOS Certification Authority is responsible for (1) issuing, signing, and managing through their life cycle, certificates binding subscribers with their signature verification keys (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.
7	Certification Authority obligations and warranties	The Certification Authority 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	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

	Certification Authority	with respect to any service associated with the issuance, use of, or reliance upon, a CSOS 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 CSOS 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 CSOS Certificate Policy will be published in the repository. CRLs will be published in the repository.
12	Certificates	CSOS 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. In the event there were to be cross certification between the CSOS Certification Authority and another Certification Authority, the other Certification Authority would be a relying party. Subscribers have obligations in the CSOS 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 regarding Subscribers. An OID 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 limited to subscribers or cross-certified Certification Authority's. 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.
15	Approved and prohibited applications	The Certification Authority must be satisfied that all applications that intend to use CSOS 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 3 persons.
18	Personnel security	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 CSOS 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.
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.
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.
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	CSOS 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.

4.4.2 DEA

The DEA will make available every 24 hours to the CSOS CA the names of new DEA Registrants authorized to handle controlled substances. This list will be used by the CSOS CA in the registration process to identify authorized applicants.

Every 24 hours the DEA will make available to the CSOS CA a list of persons whose DEA registration has been revoked. The CSOS CA will use this list in the preparation of CRLs.

4.4.3 Certification Authority

The CSOS Certification Authority (CA) will be operated under a policy that emphasizes reliability and availability to subscribers 24 hours a day 7 days a week. The CSOS CA will:

- ❑ Issue X.509 version 3 certificates to authorized registrants, their Power of Attorney (POA) holders and selected DEA personnel.
- ❑ Maintain a certificate revocation list (CRL).
- ❑ Maintain a repository of public certificates.

X.509 version 3 Certificate Standard

The CSOS Certification Authority will issue certificates to valid applicants. Certificates will only be issued to valid DEA registrants and POA holders, who are registered to handle controlled substances. The certificate will be an X.509 version 3 certificate.

X. 500 Directory

The CSOS Certification Authority will establish an X.500 directory with Lightweight Directory Access Protocol (LDAP) access. This directory will contain the certificates of all DEA registrants and POA holders allowed to manufacture and distribute controlled substances. The directory will also contain the certificates of selected DEA personnel. The Directory will contain a Certificate Revocation List (CRL) of those registrants who have had their certificate revoked or suspended. The directory will be available to be accessed through LDAP by valid CSOS PKI enrolled registrants to check the registration status of customers ordering controlled substances. The CRL will be cached.

The CSOS CA will revoke the certificates of persons under the following circumstances:

1) the DEA advises that their DEA registration status is no longer valid due to expiration or revocation;

2) the certificate holder requests revocation due to loss or compromise of private key or any other reason;

3) the certificate holder fails to comply with the obligations of users/end entities as described in the CP and expressly agreed to by user/end entity at time of registration in the CSOS PKI.

4.4.4 CSOS PKI Certificate Policy

The Certificate Policy (CP) will describe the minimum provisions for CA operation that collectively contribute to the level of assurance that DEA will mandate for CSOS transactions. These provisions include:

- The practices followed by the CA for subscriber identity proofing
- The CA's operating policy, procedures, and security controls
- The subscriber’s obligations (for example, in protecting the private key)
- The CA’s obligations (for example, warranties and limitations on liability).

4.5 Roles and Responsibilities in the CSOS

The roles and responsibilities in the CSOS closely match those that currently exist in DEA and in Industry today, both for the regulatory process and the existing business processes. This will support a faster acceptance, ease of adoption and implementation for the new system.

4.5.1 Roles and Responsibilities of DEA

- DEA will establish the CSOS Policy Management Authority (PMA), Operations Management Authority (OMA), CSOS Manager and Operations Staff.
- DEA will establish the CSOS Certification Authority and Directory.
- DEA will integrate the CSOS organization into the existing DEA organization, including training of Agents and Auditors in the processes of the new system.

4.5.2 Roles and Responsibilities of CSOS CA

- The CSOS CA will issue a Certificate Policy and Certification Practice Statement that further define the policies and procedures to be used in the CSOS PKI.
- The CSOS CA will establish guidelines for the certification of Industry PKI enabled systems.
- The CSOS CA will issue digital certificates to those industry registrants and POA holders allowed to handle controlled substances and will also issue digital certificates to selected DEA personnel.
- The CSOS CA will publish to the Directory, every 24 hours, the digital certificates of valid registrants and a Certificate Revocation List (CRL) of those registrants who have had their certificate revoked or suspended. The CA will receive information from DEA on the status of registrants.

4.5.3 Roles and Responsibilities of Industry Customers

- Industry Customers will enroll with the CSOS Certification Authority and obtain a digital certificate.

- Industry Customers will create controlled substances orders using client PKI-enabled software and digitally sign the order, archive the order, and forward the order to a Supplier.

- Upon receipt of the controlled substances product from the Supplier, Industry Customers will annotate the archived order with the receiving information, and archive the completed order. Industry Customers will create a reporting document

- Industry Customers will be responsible for the safekeeping of their private signing keys, prompt reporting of any key loss or compromise, compliance with the obligations of users as outlined in the CP, compliance with all applicable laws and regulations, and the exercise of good judgement in connection with suspicious orders.

4.5.4 Roles and Responsibilities of Industry Suppliers

- Industry Suppliers will enroll with the CSOS Certification Authority and obtain a digital certificate.

- Industry Suppliers will accept digitally signed controlled substances orders from Customers, validate the digital signature determining authenticity of the order using their PKI enabled software and check the CSOS Directory CRL that has been "cached" to determine the status of the Registrant.

- Industry Suppliers will create a CSTR reporting document from the Customer order for each filled transaction (or subset of filled transactions). Using their PKI enabled software, Suppliers will digitally sign the completed CSTR document and archive the document. Within 24 hours of having processed each order, the Supplier will forward to the DEA a copy of the digitally signed completed reporting document. These submissions may be automatically or manually batched.

- Industry Suppliers will be responsible for the safekeeping of their private signing keys, prompt reporting of any key loss or compromise, compliance with the obligations of users as outlined in the CP, compliance with all applicable laws and regulations, and the exercise of good judgement in connection with suspicious orders.

4.5.4 Roles and Responsibilities of State and Local Governments

In some states and localities, the Supplier copy of the current DEA Form 222 is made available to those state and local authorities at the local DEA OD Office. This information, in the form of the CSTR report, can be made available by DEA to state and local authorities as necessary.

Section 5 — The Controlled Substances Ordering Process Procedures and the CSOS PKI Operation

5.1 Introduction

This section describes the processes, procedures and operations of the CSOS PKI in more detail.

5.2 CSOS Ordering Process

Exhibit 5–1 below graphically illustrates the CSOS concept.

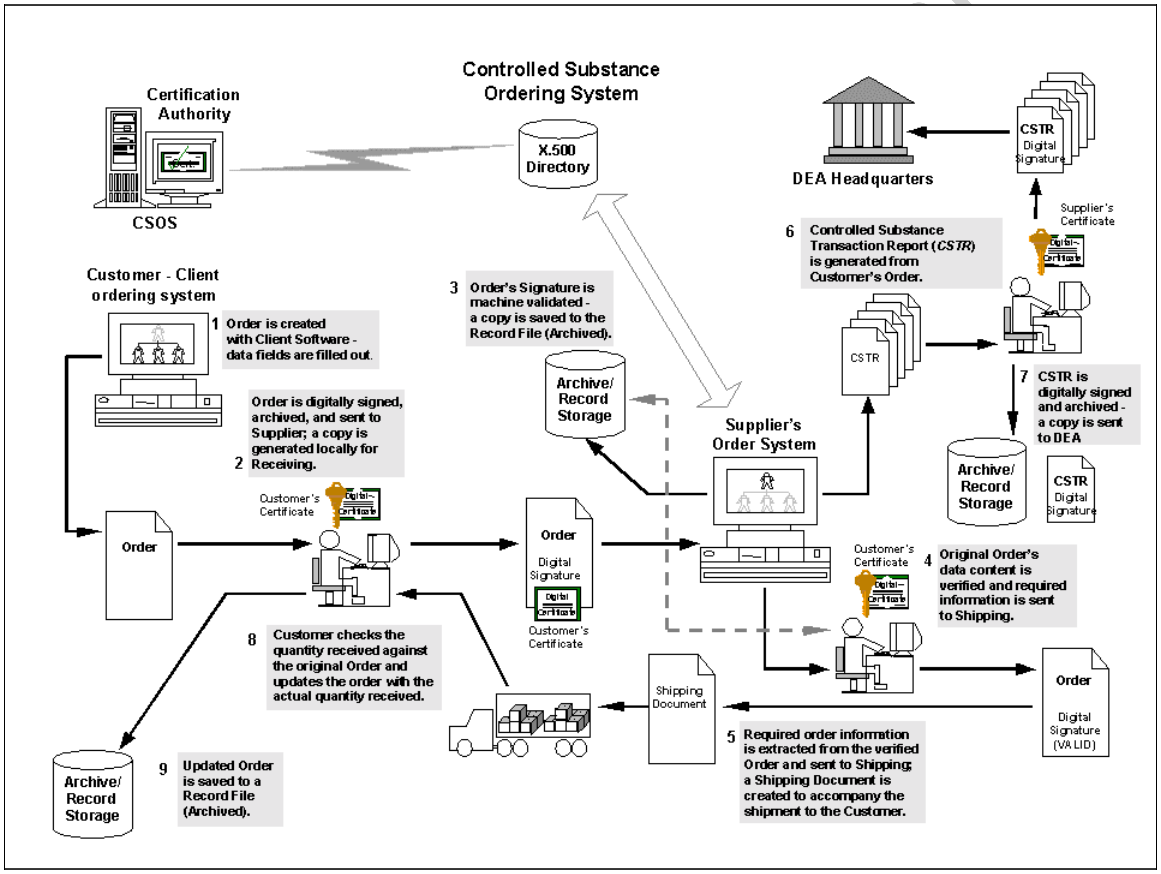

Certification Authority
CSOS
Controlled Substance Ordering System
X.500 Directory
DEA Headquarters
CSTR Digital Signature
Supplier's Certificate
6 Controlled Substance Transaction Report (CSTR) is generated from Customer's Order.
Customer - Client ordering system
1 Order is created with Client Software - data fields are filled out.
3 Order's Signature is machine validated - a copy is saved to the Record File (Archived).
CSTR
Archive/ Record Storage
2 Order is digitally signed, archived, and sent to Supplier; a copy is generated locally for Receiving.
Supplier's Order System
7 CSTR is digitally signed and archived - a copy is sent to DEA
Archive/ Record Storage
CSTR Digital Signature
Customer's Certificate
Order
Order Digital Signature
Customer's Certificate
Customer's Certificate
4 Original Order's data content is verified and required information is sent to Shipping.
8 Customer checks the quantity received against the original Order and updates the order with the actual quantity received.
Shipping Document
Order Digital Signature (VALID)
5 Required order information is extracted from the verified Order and sent to Shipping; a Shipping Document is created to accompany the shipment to the Customer.
Archive/ Record Storage
9 Updated Order is saved to a Record File (Archived).

Exhibit 5–1. CSOS Ordering Process Flow

The high level process flow shown in Exhibit 5-1 is provided as a general guideline to define how the electronic order will flow from the Customer to the Supplier, from the Supplier to the DEA, how the PKI will be used in the process and how information will be provided to DEA. This high-level process flow has been designed to closely follow the current business process, the current regulatory requirements and maintain the closed system of controlled substances distribution. It includes specific actions that must be taken with regard to document security, regulatory reporting requirements and archiving requirements.

It is possible that individual registrant situations may require minor adjustments of this process, however, the overall theme will remain.

CSOS Order Process Flow

STEP 1- CUSTOMER CREATES ORDER

1) Customer creates a unique controlled substance order by completing the required data fields 1-8 and 13-19, as shown in Appendix B, Table B–1, using the PKI enabled client software.

2) Customer digitally signs controlled substance order with Customer's private signing key. A copy of the Customer's digital certificate is attached to the order to facilitate Customer digital signature verification.

3) Customer sends digitally signed controlled substance order to Supplier.

4) Customer saves the digitally signed order to an archive, where for audit purposes, the archive is maintained for 2 years.

STEP 2- SUPPLIER RECEIVES AND VALIDATES ORDER

1) Supplier receives digitally signed controlled substance order from the Customer.

2) Supplier's PKI enabled software performs the following validity checks:

   (a) is the certificate within the validity period?

   (b) is the information contained in the certificate valid?

   (c) is the certificate listed in a CRL?

   (d) is the customer information in the order the same customer information in the now validated certificate?

3) Supplier takes the unaltered digitally signed and validated order document and places the electronic controlled substance order document in an archive. (This archive is to be maintained for 2 years at the Supplier's site)

STEP 3- SUPPLIER FILLS ORDER

1) Supplier extracts ordering data from controlled substance order document or sends controlled substance order for fulfillment.

2) Supplier creates a controlled substance shipping document, the Controlled Substance Transaction Report (CSTR) Form, from the Customer's controlled substance order document or appends the controlled substance order document with the four shipping fields.

3) Supplier digitally signs and archives the CSTR. (This archive is to be maintained for two years at Supplier's site).

4) Supplier ships the controlled substance order to the Customer.

STEP 4- CUSTOMER RECEIVES AND COMPLETES ORDER

1) Customer appends the controlled substance order document or appends the stored copy of the original controlled substance order document with the two receiving information fields.

2) One or both are stored and archived at the Customer location. (This archive to be maintained for two years at Customer's site)

STEP 5- SUPPLIER CREATES CSTR REPORT

1) Supplier creates a copy of the Supplier controlled substance shipping document or document subset, digitally signs the copy and forwards to DEA. (Within 24 hours for each filled transaction order).

STEP 6- DEA RECEIVES CSTR REPORT

1) DEA receives the Supplier created CSOS report, validates the digital signature and archives the digitally signed and validated report.

5.3 Certificates

The CSOS CA will issue public-key certificates to every user of the CSOS PKI system including DEA Registrants and POA holders who are authorized to manufacture, distribute and dispense controlled substances. The certificate will follow the format for an X.509 version 3 certificate.

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 serial number User Identification Number (UID). The address of the DEA Registrant and authorized schedules will be included in the altName field of the certificate.

5.4 Becoming a User in the CSOS PKI

The CSOS CA will accept applications to become a user from:

1) DEA Registrants who are authorized to manufacture, distribute and dispense controlled substances;

2) persons who hold Power of Attorney (POA) from DEA Registrants described above; and,

3) DEA personnel who require user status to perform their official duties.

The CSOS CA will issue public-key (digital signature) certificates to each applicant that is a qualified user. The CSOS PKI certificate holder will use the issued certificate to digitally sign and validate digital documents, such as electronic orders or electronic records, to permanently bind their identity to each signed digital document.

It should be noted that the process of becoming a DEA Registrant and receiving a DEA 223 Registration Certificate is completely separate and distinct from the process of applying to become a CSOS PKI user. The DEA Registration Unit at DEA HQ receives and processes applications to become a DEA Registrant. The CSOS CA receives and processes applications to become a CSOS PKI user. Of those Registrants who are authorized to handle controlled substances, not all will choose to become CSOS PKI users.

5.4.1 The Steps Toward Becoming a User

The steps in the process of becoming a user are set forth below.

1) The applicant will contact the CSOS CA to request an application form. The initial contact with the CSOS CA will be in person, by mail or electronically. It is anticipated that in the near future the application form will be available on a CSOS Web server.

2) The CSOS CA will, in person, electronically or by mail, provide to the applicant the “CSOS PKI Initial Application Form.”

3) The application form will:

    - ❑ Require proof of identity in the form of one Government issued photo identification card

    - ❑ Require proof of DEA Registration status by either a Form 223 DEA Registration Certificate or a Power Of Attorney (POA) letter from a DEA Registrant. POA holders must attach a copy of the 223 DEA Registration Certificate of the Registrant who gave them POA.

    - ❑ Require proof of current employment in the form of a letter, on letterhead stationary, with current work mailing address, IP address, e-mail address, and telephone number.

- ❑ Provide a statement of CSOS PKI user obligations. The applicant will sign these obligations to acknowledge understanding and acceptance.

- ❑ Provide a copy of the CSOS CA Certificate Policy (CP) for review by the applicant. The applicant will sign to acknowledge receipt and understanding of the CP.

4) The applicant will complete the application form and forward it to the CSOS CA. The form may be forwarded in person, electronically or by mail.

5) The CSOS CA will review the application form with the diligence described in the CP. The CA will have access to information previously provided to DEA by the Registrant and to DEA information on applicant's current DEA Registration status.

6) The CSOS CA will advise the applicant, within 48 hours of receipt of the application, of the status of the application. The application will be approved, denied, or placed on hold for additional information or further verification of information. The status report will be in person, electronically or by mail.

7) When an application is approved, the CSOS CA will provide to the applicant, in a trusted manner, a secret code known only to the CSOS CA and the applicant. The secret code will be provided in an Out of Band (OOB) channel; that is to say a separate means of communication than that used for other information. The OOB channel will be in person, electronically, or by mail. The secret code will enable the applicant to securely submit to the CSOS CA a request for certification of a public key. The CA will also provide such additional information as is required for the applicant to continue the application process and to participate as a user.

8) After receipt of notification of approval of application and receipt of the shared secret, the applicant will be able to electronically submit a request for certification of a public digital signature key.

9) The applicant must have access to either a Netscape or Microsoft Web browser to submit the request for certification. Both browsers have the hard coded logic to generate a private/public key pair and to submit a request in a standardized format.

10) The applicant will go to the CSOS CA Web server and follow the instructions for generating a key pair and submitting a certification request. After the shared secret has been used in the request for certification, it must be destroyed.

11) The CSOS CA will process the certification request. Requests will be approved or denied within 48 hours. The CSOS CA will advise the applicant by e-mail of the status of the request.

12) The CSOS CA will, depending on prior arrangement with the applicant;

a) e-mail the signed public key certificate and the CA’s public key certificate to the applicant, or,

b) advise the applicant to make LDAP access to the CSOS CA Directory to collect both the CA public key certificate and the applicant’s signed public-key certificate.

13) Upon receipt of the certificates the applicant is then a fully enrolled user and can sign and validate orders.

5.4.2 Key Management

Set forth below is information regarding the management of digital signature keys in the CSOS PKI.

5.4.2.1 CA Signing Key

The CA signing key will be stored in a FIPS 140-1 level 2 hardware device.

5.4.2.2 User Signing Key

Users are responsible for the secure storage of their private, signing key. The most secure storage medium for user’s private key is a secure hardware device, such as a smartcard.

5.4.2.3 Key Expiration

Public-key certificates and their associated signing (private) key will be valid for one year from date of issue and will have a set expiration date.

5.4.2.4 Re-Key

Users should note the date of expiration of their private/public key pair and prior to the expiration date should revisit the CSOS CA web server to submit a request for a new private/public key pair and public-key certificate in concert with re-registration.

5.4.2.5 Key Compromise

As is stated in the User’s Obligations and the CP, the highest obligation of the user in the CSOS PKI is to report loss or compromise of a private key. The user must notify the CSOS CA of loss or compromise of a private key within 24 hours of such an event.

5.4.2.6 Revocation

The CP and CPS will describe procedures for the user following revocation of the public-key certificate.

5.4.3 Key Handling Details

5.4.3.1 Key Generation

End entities will generate their digital signature key pair at the registrant’s location. The key generation will be performed in a FIPS 140-1 level 1 compliant module. The certification and initialization process will be handled in accordance with PKCS #10, RFC 2511 “Internet X.509 Certificate Request Message Format,” PKCS #7, RFC 2510 “Internet X.509 Public Key Infrastructure Certificate Management Protocols,” or via an equally secure manner approved by the Policy Management Authority.

Upon approval by the DEA Registration Unit, the Registration Unit will send that registrant’s information to the CA. The CA will issue a secret code (activation data) to be used in initializing the end entity registrant’s digital signing keys. This code may be delivered to the registrant via secure mail or email.

The registrant will create the digital signing keys at the registrant’s site, and utilizing a secure connection over the Internet, authenticate themselves to the CA with the CA issued code and forward the public digital verification key to the CA.

Certification Authority signing key must be stored in a dedicated FIPS 140-1 level 2 compliant hardware device, such as a smartcard; an end entity private key may be stored in either a dedicated hardware device, or in software, such as on a computer’s hard drive. All entities are responsible for the protection of private keys and activation data.

Registrant end entities must provide proof of possession of private key upon request by DEA.

5.4.3.2 Key Storage

Industry registrants will be responsible for the safe keeping of digital signing keys. Signing keys are to be stored in a secure medium or on a secured medium.

5.4.3.4. Re–Key

Users will generate a new digital signature key pair and request certification prior to the expiration of the existing key pair on the set expiration date.

5.4.3.5 Key Expiration

Certificates and associated digital signature keys will be valid for one year and will have a set expiration date.

5.4.3.6 Key Compromise

Registrant end entities will be responsible for notifying the CA upon loss or comprise of digital signature keys within 24 hours of event.

5.4.3.7 Revocation

The Certificate Policy and Certification Practice Statement will contain provisions for routine re-key and re-key after revocation.

5.4.4 CA and Directory Maintenance

5.4.4.1 Directory Updates and Directory Caching

The CSOS CA will be responsible for posting updates to the directory every 24 hours. A specific time will be set for those updates. The directory will be available 24 hours a day, seven days a week. A procedure will be established to allow registrants to copy and cache the CRLs within their own systems.

5.4.4.2 Maintenance and Support

The CSOS CA will be responsible for all maintenance of the CA, the directory, and supplementary system infrastructure, for example, backup system.

The CSOS CA will respond, by means of a CSOS Helpdesk, to requests by CSOS users to resolve any support issues pertaining to the operation of the CSOS system.

Registrant's will be responsible for providing helpdesk support for their own industry PKI enabled systems and for acting as the first level of support for these PKI-enabled systems.

5.4.4.4 Fees

CSOS 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.

Section 6 — Implementation Procedures

6.1 Introduction

This section describes the implementation procedures for the CSOS PKI, the new electronic ordering process and the associated activities that will be required prior to utilizing the CSOS.

6.2 Initial Certification of PKI Enabled Industry Systems

Existing industry software applications and systems that wish to become part of the CSOS shall meet the following requirements and have the functionality necessary to operate in the CSOS. A specific method and process for initial and on-going certifications of Industry PKI enabled systems will be developed upon completion and acceptance of the CSOS design.

It is expected that these certifications will be an attestation provided by an accredited external third party capable of performing Information Technology audits. It is understood that these could be accomplished in conjunction with other IT audits already being performed at the registrant location.

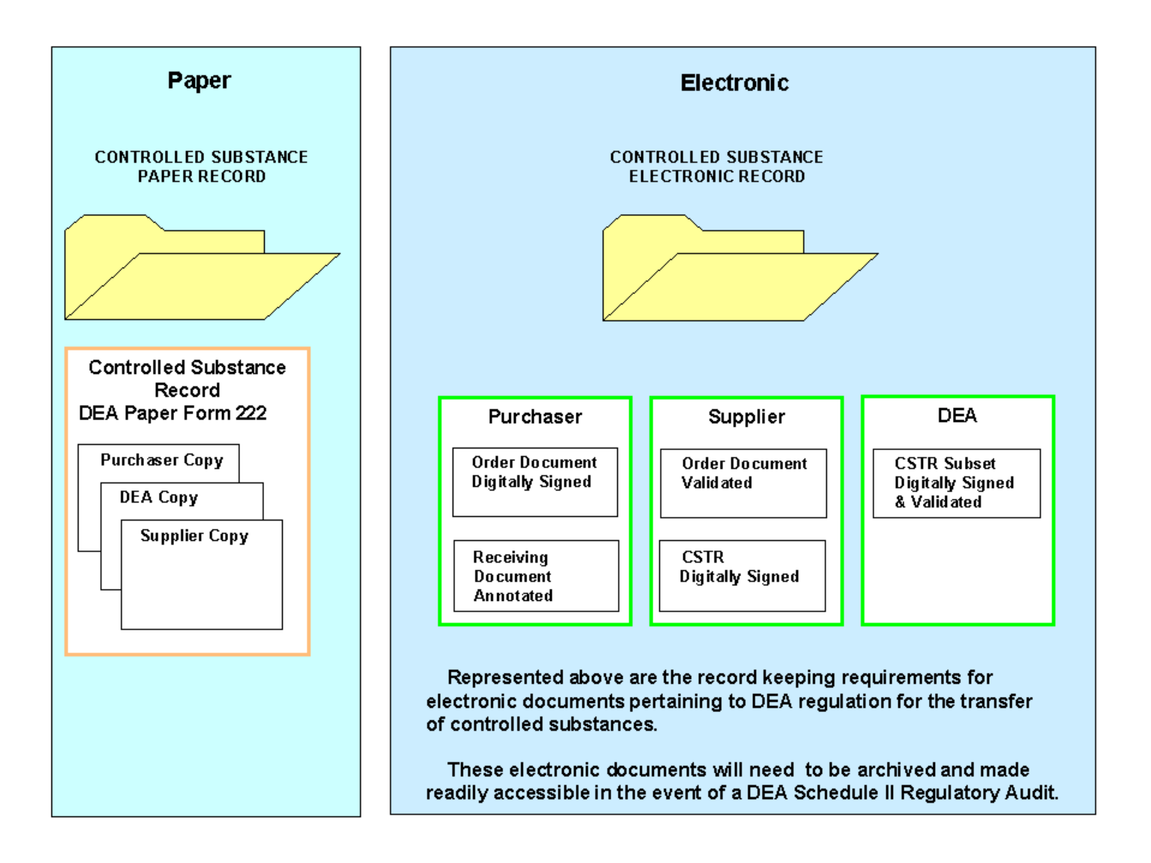
The third party auditor will be provided with DEA standards and a prepared checklist of functions, procedures and expected results that must be audited. This will be a yearly process for the on-going certifications. After initial certification, any changes to IT systems that would effect the operation of the CSOS PKI must be submitted to and approved by DEA in advance of making those changes.

6.3 Periodic Audit of CSOS Industry PKI Enabled Systems

Industry PKI enabled systems that are used in the CSOS will need to provide proof that the systems utilize the certificates and perform the required functions in the manner prescribed by the CSOS Certificate Policy.

6.4 Requirements for DEA Regulatory Audit Process

A change from the current paper based regulatory and paper based record keeping system for controlled substances will require a new definition as to what will constitute an electronic record for each controlled substance transaction. Along with that change, the way DEA inspects and audits will also require change. Illustrated below is a concept of how this new electronic record can be processed, who would process it, and where that electronic record would be stored.



Represented above are the record keeping requirements for electronic documents pertaining to DEA regulation for the transfer of controlled substances.

These electronic documents will need to be archived and made readily accessible in the event of a DEA Schedule II Regulatory Audit.

Exhibit 6–1. Controlled Substances (CS) Record Keeping

CSOS Electronic Record

The current paper based record for the transfer of controlled substances (DEA Form 222) is in three parts and requires four separate actions to complete the form and constitute a complete record of the transaction. The way that this may translate to an electronic record and the actions needed to complete the archive record are illustrated in Exhibit 6–2.

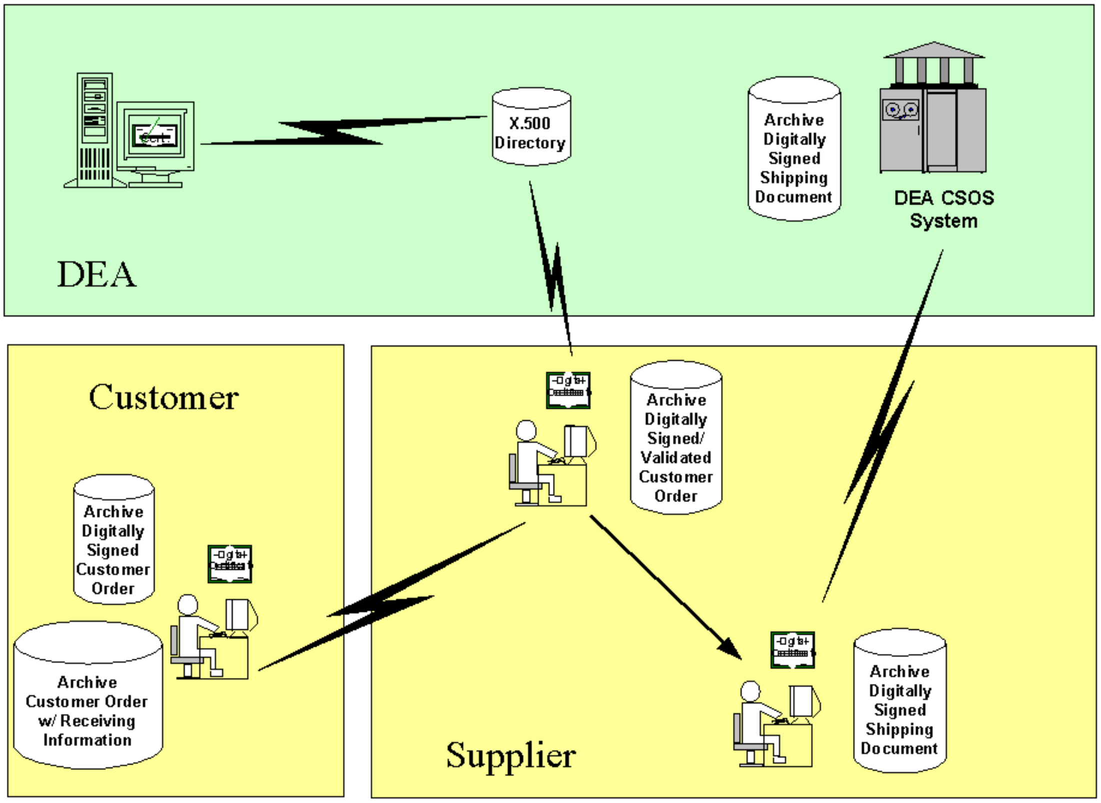


Exhibit 6-2. CSOS Transaction Archive Process

Section 7 — Control and Management Structure of CSOS PKI

7.1 Introduction

This section describes the control and management structure of the CSOS PKI as depicted in Exhibit 7-1 and the associated documents that will be produced to define the policy (Certificate Policy) and practices (Certification Practice Statement) of that structure.

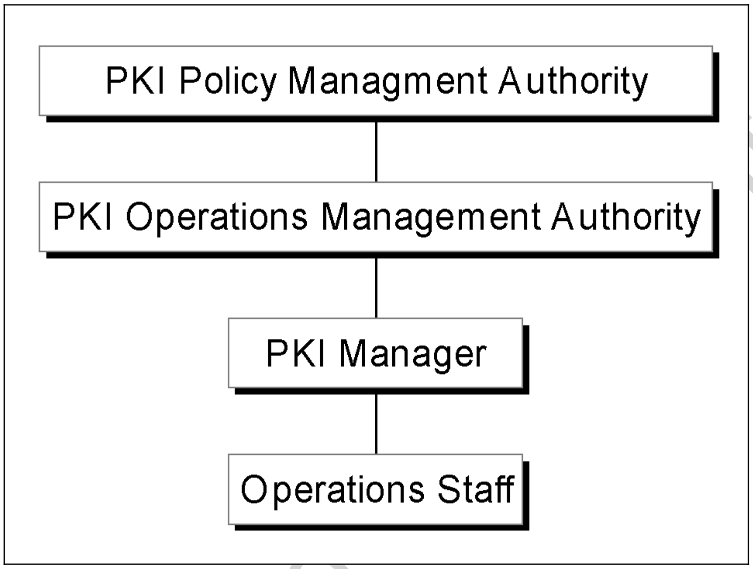

PKI Policy Managment Authority
PKI Operations Management Authority
PKI Manager
Operations Staff

Exhibit 7–1. CSOS PKI Management Structure

7.2 Policy Management Authority

The Office of Diversion Control will establish a CSOS PKI Policy Management Authority (PMA). The PMA is responsible for setting, implementing, and managing certificate policy and practices regarding the CSOS PKI. The PMA is composed of Office of Diversion Control personnel.

7.2.1 Responsibilities

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

(1) approving and revoking certificates of Registrants;

(2) ensuring appropriate use of PKI facilities throughout the CSOS PKI;

(3) maintaining and publishing the Certificate Policy and Certification Practice Statement.

The PKI Policy Management Authority commissions annual audits of PKI operations.

7.2.2 Cyclical and Routine Activity

The CSOS 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 Management Authority (OMA)
- Staffing changes within the PKI Operations Management Authority
- Pending changes to policies or other PKI management directives
- Review of PKI-related procedures and record-keeping practices
- Review matters of consideration presented by CSOS PKI participants
- 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 CSOS 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.

7.3 Operations Management Authority

The PMA will establish a 24 hours/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 CSOS PKI Manager and the PKI manager’s staff. The OMA is composed of Office of Diversion Control personnel and/or Contractor personnel.

7.3.1 Responsibilities

The OMA has overall responsibility for proper and reliable operations of the CSOS PKI 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:

- Develop revisions to, maintain currency of, and publish the Certificate Policy and Certification Practice Statement
- Oversight of PKI operations
- X.500 Directory operations
- Identify and investigate areas for PKI improvement
- Review Certification Authority operations and activity
- All technical, hardware and software aspects of the PKI
- Review 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 Policy Management Authority, and other elements of the CSOS 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 the PKI reporting requirements established or endorsed by the Policy Management Authority.

7.4 PKI Manager

The PKI Manager staffs and operates the CSOS 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, breeches of security or policy, and/or 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 Control personnel, may be contractor personnel, or may be a combination of both.

7.4.1 Responsibilities

The PKI Manager staffs and operates the Certification Authority (CA) server and it's 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 Certification Authority and the overall operation of the PKI. This includes:

- ❑ Implementing the policies and directives of the Policy Management Authority and the Operations Management Authority
- ❑ Access control of the CA server
- ❑ 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
- ❑ Providing 2nd echelon help desk assistance to end users
- ❑ Operating and maintaining the CA server
- ❑ Operating and maintaining the X.500 directory
- ❑ Maintaining official CA records and activity logs
- ❑ Evaluating new technology
- ❑ Maintaining and refreshing existing technology
- ❑ Disaster recovery procedures

7.4.2 Cyclical and Routine Activity

The PKI Manager provides availability of the Certification Authority and its associated Directory on a 24 hours/day, 7 days/week basis.

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

- ❑ Monitor Certification Authority server activity on an hourly basis
- ❑ Issue Certificate Revocation Lists (CRLs)
- ❑ Verify the physical security and integrity of the CA server 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

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

- Produce and store backup copies of Certification Authority database and journals
- 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 security, processing, or procedural anomalies or violations to the Operations Management Authority.

7.4.3 Procedural Requirements

The PKI Manager will establish and publish detailed procedures for all aspects of the Certification 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 subjects:

- Routine Certification Authority server procedures
- 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 the following requirements:

- demonstrate the integrity of the CSOS PKI;
- compliance with policy and directives issued by the Policy Management and Operational Management Authorities;

- compliance with the CSOS data processing, security, and asset management policies.

Section 8 — Compliance with Federal Standards, Commercial Standards and Requirements

8.1 Introduction

This section describes the various Federal standards, Commercial standards and requirements that the CSOS PKI adheres to and reasons for any variance from those standards.

8.1.1 Electronic Signatures in Global and National Commerce Act

The “Electronic Signatures in Global and National Commerce Act,” S.761, was signed on June 30, 2000 and becomes 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 ensures 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 Act defines this term to mean 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.

8.1.2 Government Paperwork Elimination Act (GPEA)

The 105th Congress, 2d Session, enacted the Government Paperwork Elimination Act (GPEA) 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."[1] The GPEA defines electronic signature in section 11 as a method of signing an electronic message that:

(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."[2] 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.

8.1.3 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.

ELECTRONIC RECORD- The term "electronic record" means a writing, document, or other record created, stored, generated, received, or communicated by electronic means.

[1] GPEA §9

[2] GPEA §6

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.

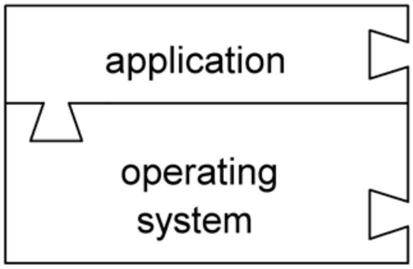


Exhibit A–1. Application and Operating System

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.

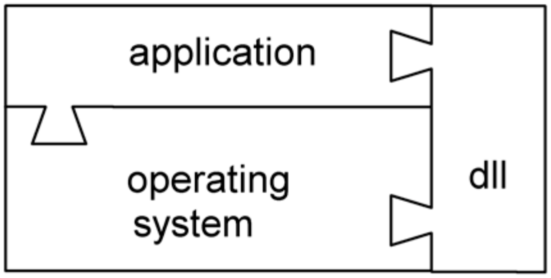


Exhibit A–2. Adding Functionality to OS using a DLL

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 principles 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.

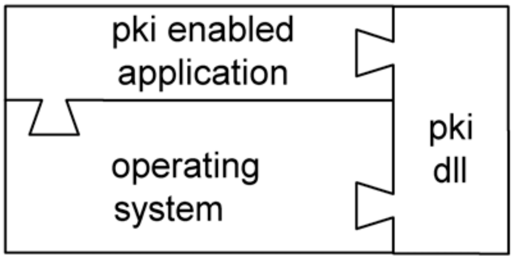


Exhibit A–3. A PKI Enabled Application

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 — Data Requirements for Ordering Applications

The following Table B–1 shows required data fields presently contained in the paper 222 order form. These fields are also required to be provided in the CSOS electronic ordering system by the Customer or Supplier in processing a Schedule II order.

Field Number	Field Data Contents	Provided by Customer	Provided by Supplier
1	To		
2	Street Address		
3	City and State		
4	Date		
5	Line Number		
6	Number of Packages		
7	Size of Package		
8	Name of Item		
9	Supplier's DEA Registration No.		
10	National Drug Code (NDC)		
11	Packages Shipped		
12	Date Shipped		
13	Number of Packages Received		
14	Date Received		
15	DEA Registration No.		
16	Schedules		
17	Registered as a		
18	Number of this Order Form		
19	Name and Address of Registrant		

Table B–1. Form 222 and CSOS Transaction Required Data Fields

The CSOS ordering process is electronic and designed to be incorporated into new and existing industry electronic ordering systems. Therefore, the design is intended to enable industry groups to incorporate their own data processing management enhancements, such as adding additional data fields to the order, as long as it does not interfere with DEA regulatory and security requirements.

It is important to note that the CSOS ordering system is authorized for all controlled substance orders, however, Schedule II orders must be stored to permit their ready retrieval distinct from any other controlled substance orders. Additionally, Schedule II order data alone is required to be reported through the CSTR report to the DEA in the CSOS reporting system.

Appendix C — List of Acronyms

CA	Certification Authority
CN	Common Name
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSTR	Controlled Substance Transaction Report
DN	Distinguished Name
DEA	Drug Enforcement Administration
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GOC	Government of Canada
GPEA	Government Paperwork Elimination Act of 1999
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MOU	Memorandum of Understanding
OID	Object Identifier
PKI	Public Key Infrastructure

RA	Registration Authority
RSA	Public key cryptographic algorithm named for it’s inventors, Rivest, Shamir, and Adleman
TCP/IP	Transmission Control Protocol/Internet Protocol
UID	Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
X.500	The standard for directory services
X.509	The standard for PKI certificates
XML	Extensible Markup Language