Controlled Substances Ordering System

Under the authority of the Controlled Substances Act of 1970, the Drug Enforcement Administration (DEA), Office of Diversion Control (OD) regulates the manufacture and distribution of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and to ensure that there is a sufficient supply for legitimate medical uses. The DEA's regulations currently allow for the electronic transmission of controlled substance orders for Schedule II substances as long as the supporting DEA 222 Form follows the electronic order. The DEA is working to modify its regulations to allow for a secure electronic transmission of controlled substance orders without the supporting 222 Form. The Controlled Substances Ordering System (CSOS) is expected to bring numerous benefits to the manufacturing, distribution, and pharmacy community. These benefits include:

- **The number of ordering errors would be less.**

- **The customer could include more line items on a single order.**

- **With faster ordering there would be less consolidating of orders by pharmacists, and orders could be placed more frequently for fewer items.**

- **With faster ordering there would be less reason to stockpile product and less waiting to fill up an order form.**

- **Less product could be kept on the shelf and smaller orders could be placed more frequently.**

The transaction volume from pharmacies to distributors is estimated at over 800,000 per year. By industry's own accounts, incorporating an electronic ordering system would result in a substantial cost savings.

Responding to Industry's needs

The typical turnaround time for an order utilizing the DEA 222 form is 1 to 3 days from the time the order is submitted until it is delivered. The factor that influences the turnaround time is the manner in which the form is transported from customer to supplier.

- **Orders that are given directly to the distributor's drivers, or orders that are FedEx'ed or couriered are obtained more quickly.**

- **Orders that are placed in the regular mail tend to take longer- from 3 to 7 days.**

Factors that significantly contribute to slower turnaround times include:

- **US Mail**

- **Getting the paper document from point A to B.**

- **Improperly filled out 222 Form**

- **Weather**

- **Quotas and Lack of Inventory**

Error rates with the paper DEA 222 form are critical in the processing time for a controlled substance order. The following contribute to the error rate:

- **Corporate name changes, address changes due to Post Office redistricting, road construction changes that change addresses, mergers and acquisitions.**

- **Human errors such as National Drug Code (NDC) numbers that are transposed, forgetting to sign the DEA 222 Form and wrong number of line items indicated.**

Factors that lower the error rates are:

- **Corporate policy that only allows experienced employees to transact DEA 222 Forms.**

- **In-store training provided to those utilizing DEA 222 Forms.**

- **Training manuals and cheat sheets.**

- **Fear of fines from DEA audits.**

An Allowance Not a Mandate

The DEA understands that businesses must weigh the advantages of any new technology against the implementation costs, and understand the expected return

on investment. Since some DEA registrants may not wish to take advantage of the new regulations, the DEA will leave current regulations and current processes in place. The 222 paper form process will still be available. The DEA will not force registrants to use CSOS. Adoption of CSOS standards will be the only allowance for the electronic transmission of Schedule II controlled substance orders from distributors to manufacturers and from pharmacies to distributors.

How will electronic ordering of controlled substances be secured?

To guarantee a similar degree of security as found in the paper 222 system, the DEA will establish an electronic ordering system where Schedule II substance orders are digitally signed using Public Key Infrastructure (PKI) technology. This technology will bring to the process the following advantages: (1) reduce the amount of paper in the process (2) speed transaction times (3) lower costs per transaction and (4) introduce security services into the process. The following paragraphs explain the underlying security technology that makes this possible.

What is a Digital Signature?

Frequently, the last business processes to be automated are those that require a “wet signature.” In the electronic world, PKI can replace the traditional approach with a more robust method that delivers both message integrity and nonrepudiation. The solution combines a “document fingerprint” with public key cryptography. Public key cryptography is an important tool used in creating a digital signature.

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

Verifying a signature—Upon receiving the digitally signed document, the recipient uses the sender’s public key to decrypt the signature and obtain the original message digest. If the signature can be decrypted with the sender’s public key, then only the sender could have sent

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

What is a Certification Authority?

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

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

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

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

What is a Digital Certificate?

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

The Need for a Certificate Policy

While technology provides the mechanism to solve the security issues facing the electronic transmission of controlled substance orders, policy ensures that the technology is implemented correctly and managed appropriately. The policy framework is as important as the technology itself.

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

Securing the private key-For true nonrepudiation, (assurance that the order was sent from a registrant or the registrant's Power Of Attorney (POA) and no one else), the registrant or POA must not share this private key with anyone.

Accepting a signed order-Upon receipt of a digitally signed order, relying parties must ensure that the digital certificate used to digitally sign the order has not expired. Relying parties must also verify that the digital certificate is not on a CRL. If it is on the CRL, the order should be rejected. Finally, the signature must be verified to ensure that the document has not been modified. To ensure that all of the above functions are performed every time, computer systems can be programmed to perform these functions automatically.

Elements of the CSOS Framework

The CSOS framework is being designed to provide trust services to DEA registered manufacturers, distributors, pharmacies, and other 222 users. The framework will consist of commercially operated systems with integrated PKI enabled software. The CSOS framework is made up of the following elements: 1) Certification Authority (CA), 2) Directory for public access, 3) CSOS-PKI enabled Electronic Ordering Systems, 4) CSOS participating, DEA registered manufacturers, distributors, retail pharmacies, and other 222 users.

CSOS Certification Authority

The CSOS framework was developed after carefully considering a number of PKI-architecture alternatives. The architectures were evaluated with respect to a number of factors including regulatory enforceability.

The CA, Directory, and supporting infrastructure are designed to function as an alternative system that is legally equivalent to, but does not supplant, the 222 paper form for Schedule II substances.

While the DEA has the authority to take action against registrants who fail to follow DEA regulations, it was unclear how DEA would be able to enforce certificate policy if a commercial CA's certificate was utilized by DEA registrants/POA's. In the event that a registrant/POA operates in an improper manner—inconsistent with the DEA's CSOS Certificate Policy—the DEA desires the ability to revoke the CSOS certificate of that registrant/POA. By operating its own CA, the DEA would have the ability to control all functions and actions of the CA. While such a step would be drastic, it would only occur after discussions with the DEA Program Management Authority (PMA) or after some form of legal or administrative action.

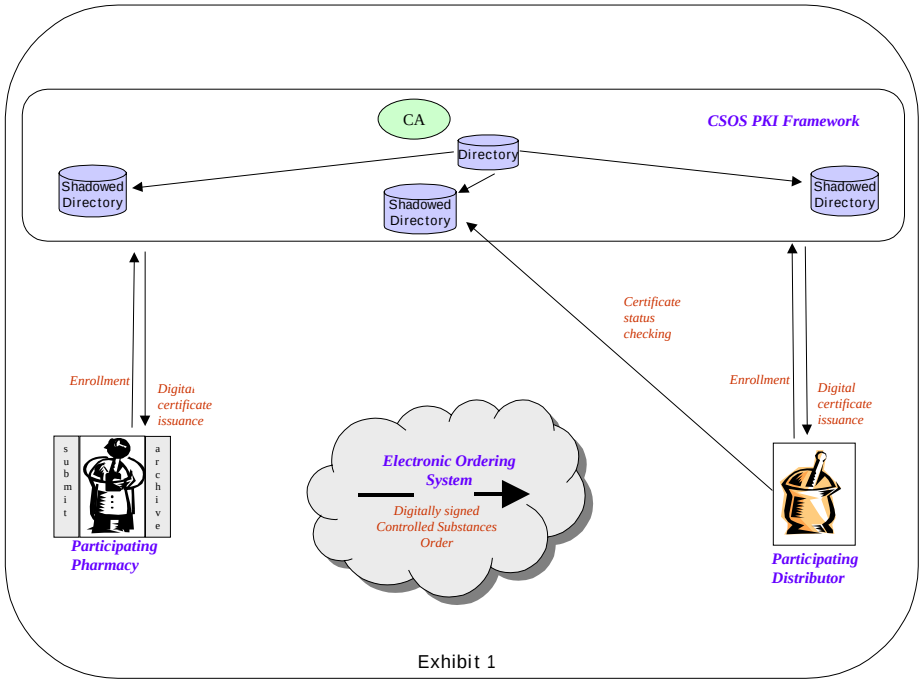

Exhibit 1

The DEA intends to establish a CSOS Certification Authority as shown in Exhibit 1. Under this framework, the

CA will be operated in accordance with the DEA's Certificate Policy and has the authority to issue and revoke CSOS Digital Certificates to DEA registrants and POA's.

Responsibilities of CSOS Certification Authority

- **Comply with the DEA's CSOS Certificate Policy**- The DEA will define the CSOS Certificate Policy (CP). The CP will set strict standards and obligations that must be met by the CSOS Certification Authority.

- **Issue CSOS Certificates to DEA registrants**- Registrants and qualified POA's will be able to apply for a CSOS certificate either in-person or on-line. It is anticipated in the case of on-line enrollment, the registrant/POA would first have to submit a signed copy of some type of a DEA application form along with proof of DEA registration.

- **Publish up-to-date Certificate Status Information** – The CA must publish a CRL on a regular basis as defined in the CSOS CP. The CRL identifies the CSOS digital certificates that have been revoked by the CA.

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

- **Perform an Annual Audit**- Participating industry ordering systems will be required to submit to a yearly third-party audit indicating that they are operating in compliance with DEA standards.

Electronic Ordering System Applications

Today, there are numerous industry systems used by manufacturers and distributors for transmission of their customer's orders electronically. Under the DEA's current regulations, these systems are prohibited from electronically transmitting Schedule II controlled substance orders without the order also being submitted on the DEA 222 Form. The DEA anticipates that once its revised regulations are in place, industry will be able to PKI-enable their ordering systems to support digitally signed electronic orders for controlled substances to comply with the newly established standards.

Industry Obligations

Electronic ordering systems will be expected to provide services between manufacturers, distributors, and

customers. Depending on the functionality provided by the ordering system, the following obligations would be pertinent to the system.

Support CSOS Digital Signatures—The system must provide the customer with the ability to digitally sign all electronically transmitted controlled substance orders using the registrant's or POA's CSOS private key. The system should automatically prompt the customer for a digital signature prior to submission of a controlled substance order. The system must transmit the registrant's or POA's CSOS public key and digital certificate along with the controlled substance order.

Support Validation of CSOS Digital Signatures— The system must provide the supplier with the ability to validate a digitally signed controlled substance order. The system should verify that the order has been digitally signed, that the user who signed the order is not on a CRL, and that the digital signature is valid which indicates that the order has not been altered. Once validation has been successfully checked, the system must archive the original order without alteration, the registrants or POA's CSOS public key and digital certificate, and the digital signature along with the controlled substance order.

Perform Audit of PKI-Enabled Ordering Systems—Suppliers who PKI-enable their ordering systems will be required to perform a yearly third-party audit of their applications to ensure that the software correctly performs the applicable obligations.

CSOS Participants

DEA registered manufacturers, distributors, pharmacies, and other users of the 222 form for Schedule II substances will be eligible to obtain CSOS digital certificates. CSOS digital certificates will be valid for one year and will allow the user to electronically transmit orders for schedule II controlled substances and eventually for schedule II-V controlled substances. Since the DEA registration-based CSOS digital certificate is structured to certify the holder's registration status to the relying party for the ordering transaction, registrants and the authorized POA's of the registrants will be allowed to obtain a DEA CSOS digital certificate according to what is required by the CONOPS, Certificate Policy, and Certificate Practice Statement policy documents.

As relying parties to the electronic ordering of controlled substances transaction, pharmacies, hospitals and other registrants who wish to participate in the CSOS program will receive CSOS certificates. The electronic ordering system they use will be required to be CSOS-compliant. This means that the software must perform the CSOS-defined relying party obligations—identified below—prior to submitting an electronic order for controlled substances.

Participant Customer Obligations

The following bullets identify some of the CSOS participants' obligations.

- **Apply for a CSOS Digital Certificate**—Before a participant can begin electronially submitting controlled substance orders, they must first submit a properly documented application to the CSOS CA. DEA registrants/POA's will be permitted to order controlled substances electronically only after the application has been approved and the CA has issued a digital certificate to the registrant/POA.

- **Safeguard the Private Key**—The participant is obligated to protect the private key on a smartcard or other physical device under the sole control of the participant.

- **Notify CA in event of lost or stolen private key**—CSOS participants are obligated to notify the CSOS Certification Authority within 24 hours of the loss of the private key.

Supplier Obligations

The following bullets identify the key CSOS supplier obligations that must be performed prior to fulfilling an electronically transmitted order for controlled substances. These obligations must be performed for every submitted order. The steps of verification and validation will be performed by the PKI enabled applications instantaneously and will be transparent to the user.

- **Order Signature Verification**—Verify that the electronic order has not been altered or that it is not a forgery. The supplier must reject fraudulent orders and orders that have been tampered with.

- **Validate Customer's Status**—Check the status of the customer's CSOS digital certificate to ensure that the signature comes from a DEA registrant or POA, verify

that the registrants/POA's CSOS digital certificate is not on the CRL, and verify that the registrant/POA is authorized to order the appropriate schedule of controlled substances. The supplier must reject the order if the customer's digital certificate has been revoked, or if the customer's digital signature is not valid.

- **Maintain an Archive for 2 years**—The supplier must maintain an electronic archive of all orders received and controlled substances shipped.

- **Electronically Sign the Reporting Information**—For all valid CSOS orders, the supplier must electronically sign the reporting information that is submitted to DEA so that the supplier is bound to the act of fulfilling the order.

- **Submit required info to DEA** — all Schedule II information is required to be submitted upon completion of the order.

DEA's Efforts to Date

– Gathering Security Requirements

Interviews were performed with a representative mix from manufacturers, distributors, and pharmacies to identify issues about the current paper 222 form and the proposed electronic process for controlled substances. The results of this effort are documented in the *MADI PKI Certificate Policy Requirements Analysis* posted on the DEA's web site at http://www.deadiversion.usdoj.gov.

– Industry IT Infrastructure Review

DEA is sensitive to the significant investment that the manufacturing, distributing, and pharmacy industry has made in Information Technology. To ensure that any electronic ordering system for controlled substances framework is consistent with industry's IT architectures and configurations, extensive interviews with industry representatives were conducted to identify how the framework could be designed to minimize the impact on industry while at the same time leveraging existing infrastructure. The results of this effort are documented in *the MADI PKI Existing Network Infrastructure Analysis* posted on the DEA's web site at http://www.deadiversion.usdoj.gov.

Future DEA Efforts

Concept of Operations - From the outset, industry opinions have been solicited on how a PKI framework would operate. As a part of this process, DEA will be provided with a Concept of Operations (CONOPS) which will define a clear picture of the CSOS PKI framework and how it will be designed and operated. The CONOPS defines the mechanisms by which the following events occur:

Design concepts -

Roles and Responsibilities of the PKI system –

System enrollment –

Auditing of PKI enabled systems –

The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov

PKI Product Review - DEA will be provided with a review of PKI products which will describe the evaluation of COTS PKI products which are currently available. The evaluation is based upon products that exhibit the capabilities and features needed to meet OD's regulatory requirements. The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov.

PKI Design Plan -DEA will be provided with a comprehensive design plan which will describe the components, software, and structure necessary to support a production PKI infrastructure. The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov.

PKI Implementation Plan -DEA will be provided with a detailed plan for additional acquisitions, installation, configuration, testing, certification, and end-user training requirements. The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov.

Certification Practice Statement (CPS) -DEA will be provided with the CPS which will describe specifically how the policy objectives are to be achieved. The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov.

Certificate Policy -DEA will be provided with a policy document which describes the level of security the CA will function at. This document will have implications that the users of the PKI system must face regarding whether or not to trust certificates issued by the CSOS CA. The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov.

PKI Management Selection and Training Plan -DEA will be provided with a description of the personnel requirements for the POC and full production staff. Included will be roles and responsibilities, training, deployment, and specific training required. The results of this effort will be documented on the DEA's web site at http://www.deadiversion.usdoj.gov.